

# STRATEGIA DEI DATI E INTELLIGENZA ARTIFICIALE

Verso un nuovo ordine giuridico del mercato

*a cura di*

**VALERIA FALCE**

*con contributi di*

**Emanuela Arezzo**

**Maria Letizia Bixio**

**Roberto Bocchini**

**Francesco Di Ciommo**

**Filippo Donati**

**Valeria Falce**

**Nicola M.F. Faraone**

**Tommaso Edoardo Frosini**

**Cesare Galli**

**Alberto M. Gambino**

**Anna Genovese**

**Gustavo Ghidini**

**Silvia Giudici**

**Marco Macchia**

**Massimo Proverbio**

**Cristina Schepisi**

**Maria Antonietta Scopelliti**

**Pasquale Stanzone**

**Guido Stazi**



**G. GIAPPICHELLI EDITORE – TORINO**



UNIVERSITÀ EUROPEA DI ROMA

*Collana del*

Dipartimento di Scienze Umane

*Fondata da* ALBERTO M. GAMBINO

*Diretta da*

EMANUELE BILOTTI - VALERIA FALCE - ALBERTO M. GAMBINO

LOREDANA GIANI - MARCO MAUGERI - FILIPPO VARI

---

*Sezione Giuridica – Materiali*

8



# STRATEGIA DEI DATI E INTELLIGENZA ARTIFICIALE

Verso un nuovo ordine giuridico del mercato

*a cura di*

VALERIA FALCE

*con contributi di*

Emanuela Arezzo	Alberto M. Gambino
Maria Letizia Bixio	Anna Genovese
Roberto Bocchini	Gustavo Ghidini
Francesco Di Ciommo	Silvia Giudici
Filippo Donati	Marco Macchia
Valeria Falce	Massimo Proverbio
Nicola M.F. Faraone	Cristina Schepisi
Tommaso Edoardo Frosini	Maria Antonietta Scopelliti
Cesare Galli	Pasquale Stanzone
	Guido Stazi



G. GIAPPICHELLI EDITORE – TORINO

© Copyright 2023 - G. GIAPPICHELLI EDITORE - TORINO

VIA PO, 21 - TEL. 011-81.53.111

<http://www.giappichelli.it>

ISBN/EAN 979-12-211-0376-2

ISBN/EAN 979-12-211-7969-9 (ebook - pdf)

*La pubblicazione di volumi nella Collana del Dipartimento di Scienze Umane dell'Università Europea di Roma è disciplinata da apposito regolamento, disponibile sul sito internet dell'Editore ([www.giappichelli.it](http://www.giappichelli.it)) e dell'Università Europea di Roma ([www.universitaeuropadiroma.it](http://www.universitaeuropadiroma.it)).*

*Composizione:* Voxel Informatica s.a.s. - Chieri (TO)

*Stampa:* Stampatre s.r.l. - Torino

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail [autorizzazioni@clearedi.org](mailto:autorizzazioni@clearedi.org) e sito web [www.clearedi.org](http://www.clearedi.org).

# Indice

	<i>pag.</i>
<b>Prefazione</b>	XI
<b>Valeria Falce</b>	
<b>Strategia dei dati. Traiettorie orizzontali e applicazioni verticali</b>	1
1. Introduzione	1
2. Dalle direttrici...	5
2.1. Agli assi cartesiani della strategia dei dati	6
3. Un'applicazione. Dalla strategia per la finanza digitale	8
3.1. Alla democratizzazione della consulenza	10
4. Conclusioni	15
<b>Tommaso Edoardo Frosini</b>	
<b>L'Ordine giuridico del digitale</b>	17
1. Ordine (e disordine) nel diritto digitale	17
2. Costituzionalismo e tecnologia	19
3. I nuovi diritti costituzionali nell'era di Internet. Il diritto di accesso	22
4. Segue: il diritto alla libertà di espressione	24
5. Segue: Il diritto alla privacy	26
6. Segue: il diritto all'oblio	29
7. Il diritto nell'intelligenza artificiale	32
8. Democrazia e società digitale	35
9. Fake news e disinformazione	40
10. Conclusioni	42
<b>Filippo Donati</b>	
<b>Quale disciplina per l'intelligenza artificiale?</b>	45
1. La rivoluzione dell'intelligenza artificiale	45
2. IA e tutela dei diritti	47
3. L'approccio risk-oriented	49

	<i>pag.</i>
4. Profili di criticità	50
5. La sfida istituzionale	51
<b>Cristina Schepisi</b>	
<b>Brevi note sulla “dimensione europea” della regolamentazione dell’intelligenza artificiale: principi, obiettivi e requisiti</b>	53
1. Introduzione	53
2. La dimensione europea, l’esigenza di non frammentare il mercato e il bilanciamento con la tutela dei diritti	56
3. Il pre-requisito per una dimensione europea: una definizione uniforme e chiara di “sistema di intelligenza artificiale”	57
4. La precisazione del rapporto tra la tutela del mercato e quella dei diritti fondamentali	60
5. La dimensione europea dei diritti, l’identificazione <i>ex ante</i> di alcuni diritti davvero fondamentali	62
6. Il necessario bilanciamento <i>ex ante</i> tra i vari diritti	67
7. L’aspetto procedurale europeo: la scelta della base giuridica e della misura da adottare	71
8. Profili conclusivi	74
<b>Alberto M. Gambino</b>	
<b>Piattaforme, IA e data sharing: premessa</b>	77
<b>Roberto Bocchini</b>	
<b>La rilevanza economica delle piattaforme digitali tra sfide ed opportunità pro-concorrenziali</b>	83
1. La ricerca	83
2. La rilevanza economica delle piattaforme	85
3. La necessità di ricorrere ad una regolazione organica delle piattaforme	86
4. Spunti di riflessione	92
<b>Guido Stazi</b>	
<b>Piattaforme e dati: una prospettiva concorrenziale</b>	93
<b>Nicola M.F. Faraone</b>	
<b>Chi prima arriva [forse non] primo alloggia: questioni aperte in tema di concorrenza e regolamentazione <i>ex-ante</i> nei mercati di-gitali</b>	107
1. Premesse introduttive	107

	<i>pag.</i>
2. Il diritto della concorrenza arranca e la regolazione è pronta a supplire: un'ultima decade di "riforme" vissuta "pericolosamente"	109
3. Il cumulo di procedimenti e sanzioni nel Digital Markets Act	117
4. Il caso di scuola del <i>ne bis in idem</i>	128
5. La novella dell'abuso di dipendenza economica nei mercati digitali introdotta dal DDL Concorrenza	141
6. Conclusioni	147
<b>Silvia Giudici</b>	
<b>Intelligenza artificiale e diritti di proprietà industriale e intellettuale. Spunti preliminari</b>	149
1. Introduzione	149
2. L'apporto creativo	150
3. La titolarità	151
4. Conclusioni	153
<b>Emanuela Arezzo</b>	
<b>La tutela dei prodotti dell'IA tramite diritto d'autore e i diritti connessi</b>	155
1. Introduzione	155
2. Possono i prodotti dell'IA considerarsi opere dell'ingegno?	157
3. I prodotti dell'IA e il requisito della creatività nelle opere dell'ingegno	160
4. Può l'IA considerarsi "autore"?	166
5. Assenza di una giustificazione a sostegno della tesi che intende concedere alla macchina intelligente le fattispecie esclusive tipiche del diritto d'autore	169
6. Può l'inventore/autore dell'IA vantare una qualche prerogativa verso i prodotti dell'IA? e in tal caso a che titolo	171
6.1. I prodotti realizzati dall'IA e le diverse tesi che giustificano l'attribuzione dei relativi diritti all'essere umano	172
6.1.1. La dottrina maggioritaria: valorizzazione dell'apporto creativo umano nella fase di strutturazione e predisposizione dell'IA	172
6.1.2. La dottrina che valorizza l'apporto creativo dell'utente	176
7. Una proposta de <i>jure condendo</i> di regolamentazione della tutela dell'IA e dei suoi prodotti tramite il diritto d'autore e i diritti connessi	178

**Maria Letizia Bixio****Applicazioni della *blockchain* nei processi di tracciabilità e certificazione, valutazioni in itinere** 181

1. Introduzione 181
2. *Blockchain* nel sistema della tracciabilità 183
  - 2.1. Tracciabilità quale leva pro-competitiva: aspetti positivi nell'impiego della *blockchain* per i consumatori e per le imprese 186
  - 2.2. Test per la verifica dei limiti nell'applicazione della tecnologia 190
3. Per un'ipotesi evolutiva della funzione: dal marchio di certificazione alle "certificazioni" *blockchain-based* 191
4. Conclusioni 195

**Marco Macchia****Il *Digital Finance Package* e l'elogio della regolazione** 197

1. La digitalizzazione nel settore finanziario 197
2. L'impiego dei big data nel settore finanziario 200
3. Le regole di funzionamento delle cripto-attività a tutela degli utenti 203
4. La concorrenza tra diversi strumenti finanziari digitali 206
5. La centralità della dimensione pubblicistica 209

**Maria Antonietta Scopelliti****È ancora possibile la neutralità della tecnologica della normativa?** 213

1. Introduzione 213
2. Ogni sistema di IA è uguale solo a sé stesso (framework OCSE) 214
3. La via Europea alla Regolamentazione dell'IA 216
4. L'Approccio sperimentale anche per i Regolatori e le pubbliche Autorità 217
5. L'approccio della CONSOB 217
  - 5.1. L'Esperimento KID 218
  - 5.2. L'Esperimento Abusi di Mercato 218
  - 5.3. Nuovi progetti 220

**Anna Genovese****La circolazione dei valori mobiliari su *blockchain*** 223

1. Introduzione 223
2. Le condizioni per la circolazione dei valori mobiliari su *blockchain* 226
3. Dalla dematerializzazione alla tokenizzazione dei valori mobiliari 231
4. Le scelte di regolazione di rilievo gius-commercialistico 232
5. Note conclusive 234

pag.

**Francesco Di Ciommo****Smart Contract, robo advisor e mercati finanziari** 237

1. Trading algoritmico ed Internet of Things: fenomenologia del mondo che cambia 237
2. Gli Smart Contract: una categoria (non giuridica) alla moda 241
3. La Blockchain a servizio degli Smart Contract 245
4. I mercati finanziari dall'Algorithmic Trading (AT) all'High Frequency Trading (HFT) 250
  - 4.1. Velocità e intensità delle negoziazioni come fattori concorrenziali 255
  - 4.2. HFT e rischi di market abuse 257
  - 4.3. I primi tentativi di regolare gli HFT 261
  - 4.4. Gli AT e gli HFT alla luce delle direttive MIFID I e II 263
5. La consulenza finanziaria e la c.d. robo advisor 266

**Massimo Proverbio****Strategia dei dati e Digital Finance Package in Intesa Sanpaolo** 273

1. Strategia dei Dati e Piano industriale di Intesa Sanpaolo 273
2. DORA e Cloud 276
3. Dati e Intelligenza Artificiale 279
4. Pagamenti Istantanei 283
5. Mondo Digitale 288
6. Prossime sfide e conclusioni preliminari 289

**Cesare Galli****Il futuro delle piattaforme tra *blockchain*, NFT, metaversi e gestione dei dati** 291

1. La necessità di un approccio sistematico nella disciplina delle nuove tecnologie 291
2. Il rapporto tra metaversi e *blockchain* e le esigenze di corretta contrattualizzazione dei relativi rapporti giuridici 293
3. Token e Non Fungible Token e il loro rapporto con *blockchain* e metaverso 296
4. Metaversi e diritto dei marchi 297
5. Metaversi, nuove tecnologie e gestione dei dati 303

	<i>pag.</i>
<b>Pasquale Stanzone</b>	
<b>Verso la società della simulazione? Il metaverso e le sue sfide</b>	305
<b>Gustavo Ghidini</b>	
<b>Di diverso avviso</b>	311
<b>Gli Autori</b>	315

## Prefazione

L'intelligenza artificiale (IA) esprime la cifra distintiva della quarta rivoluzione industriale<sup>1</sup>: si alimenta di dati (big data), ricorre a tecnologie avanzate, utilizza linguaggi e tecniche predittive, per centrare obiettivi che, pur fissati dall'uomo, da questi non potrebbero essere conseguiti individualmente<sup>196</sup>. I benefici sono evidenti in ogni industria, settore e attività. L'efficienza nelle scelte gestionali e la ottimizzazione dei processi, la riduzione dei costi, la creazione di nuovi prodotti e la personalizzazione di quelli esistenti sono effetti tipici dell'IA<sup>198F</sup>, come pure l'avvicinamento e la contaminazione tra settori tradizionalmente diversi e tra prodotti e servizi comunemente separati.

Il mercato finanziario non fa eccezione, anzi.

Il ricorso all'IA ha accelerato il ricorso al trading algoritmico, alle nuove tecniche di gestione del rischio e di monitoraggio di eventuali frodi, nonché a nuove modalità per la gestione della esecuzione degli ordini e di nuove tecniche per la valutazione del merito creditizio (i.e. *credit scoring*). Tutte operazioni, queste, che si collocano nel più ampio fenomeno del FinTech e che comportano, inevitabilmente, lo smantellamento dei tradizionali modelli di riferimento, incluso l'accentramento dei rapporti, innestando nel mercato finanziario nuovi operatori e rapporti disintermediati e spersonalizzati, prodotti e servizi combinati, integrati e polifunzionali, nonché processi disgre-

---

<sup>1</sup> In argomenti, e sui diversi fronti aperti, mi si permetta di rinviare a V. Falce, *Data strategy e intelligenza artificiale*, in *Diritti e mercati nella transizione ecologica e digitale*, a cura di Passalacqua, CEDAM, 2021; V. Falce, J. Cannataci, O. Pollicino, *Legal Challenges of Big data*, EE Int., 2020; V. Falce, *Le regole sulle banche dati nella strategia europea: (molti) diritti e (poche) responsabilità*, in *Intelligenza artificiale e diritto: una rivoluzione?*, a cura di A. Pajno, F. Donati, A. Perrucci, Il Mulino, 2022; *Intelligenza artificiale e Fintech. Consulenza decentrata tra algogovernance ed elemento fiduciario*, in *Intelligenza artificiale e diritto: una rivoluzione?*, a cura di A. Pajno, F. Donati, A. Perrucci, Il Mulino, 2022; V. Falce, *Financial Innovation tra Disintermediazione e Mercato*, Giappichelli, 2021; V. Falce, A. Genovese, *La portabilità dei dati in ambito finanziario*, Quaderno FinTech, CONSOB, 2021; V. Falce, G. Finocchiaro, *Fintech: Diritti, Concorrenza, Regole*, Zanichelli Ed., 2019; V. Falce, G. Ghidini, G. Olivieri, *Informazione e Big Data tra Innovazione e Mercato*, Quaderni Romani di Diritto Commerciale, Giuffrè Ed., 2018.

gati, in cui il rilascio ininterrotto di dati contribuisce a definire nuove politiche commerciali.

La rilevanza dei predetti effetti positivi non può prescindere dalla valutazione degli eventuali rischi a essa correlati: l'esperienza insegna che l'attenta analisi dei rischi costituisce presupposto indefettibile per rispondere al "se" e al "come" regolamentare i nuovi fenomeni digitali in generale e i sistemi IA in particolare, verificando la tenuta delle regole nelle diverse prospettive del mercato, della vigilanza e della supervisione.

Non è dunque un caso che in risposta alla discontinuità in corso l'Unione Europea abbia riconosciuto nell'intelligenza artificiale il perno innanzitutto della Strategia sul mercato unico digitale, né che a ciò sia pervenuta attraverso un percorso evolutivo, transitato per la promozione di un approccio di soft law (con la pubblicazione di Linee guida etiche per un'IA affidabile e di Raccomandazioni politiche e di investimento) e poi (con la Comunicazione sulla promozione di un approccio europeo all'IA), per poi imboccare il binario regolatorio. Con la Proposta di Regolamento sull'IA l'Unione si dota di una cornice di regole certe e di qui favorire lo sviluppo, l'immissione sul mercato e l'utilizzo di sistemi di IA nell'Unione. Assi cardine della Proposta sono:

- riconoscere che le tecnologie IA sono un mezzo e non un fine, sono cioè uno strumento al servizio dell'uomo e dei cittadini dell'Unione. Si rinforza così la visione cosiddetta umanocentrica del sistema valoriale europeo;

- definire regole comuni e uniformi, da applicare orizzontalmente senza distinzione di settore o di attività per garantire sicurezza, affidabilità ed eticità dei sistemi di IA all'interno dell'Unione;

- identificare i soggetti a cui si applica il Regolamento, per il fatto di contribuire a vario titolo alla immissione in commercio di sistema IA nell'Unione;

- escludere alcune aree dal perimetro di applicazione del Regolamento (come la sicurezza e la ricerca), come pure alcuni specifici ambiti soggettivi (autorità pubbliche di paesi terzi o organizzazioni internazionali);

- graduare i sistemi IA, in relazione al livello di pericolosità che sono in grado di esprimere per i diritti fondamentali;

- prevedere un regime modulare di oneri e responsabilità, introducendo obblighi di certificazione e autocertificazione, di valutazione della conformità del prodotto e del rischio, di trasparenza e informativi, di sicurezza e affidabilità, nonché obblighi di monitoraggio anche post-market, attraverso i quali si verifichi nel tempo se siano state introdotte modifiche significative, non prevedibili rispetto alla funzione originariamente certificata;

- identificare un sistema istituzionale e di governance, accentrato nella Commissione Europea dal punto di vista della classificazione dei sistemi di IA e dell’adeguamento di obblighi e divieti;

- riservare alle autorità nazionali di vigilanza del mercato competenti la supervisione dell’applicazione delle regole, mentre rimette ad un comitato europeo per l’intelligenza artificiale – cui il Board europeo della privacy partecipa di diritto – un ruolo consultivo, di coordinamento delle autorità nazionali, di ausilio all’attività della Commissione e di assistenza sia alla Commissione sia alle autorità nazionali per lo sviluppo delle norme per l’IA;

- accreditare il modello multistakeholder, favorendo i codici di condotta volontari per i sistemi di IA non ad alto rischio, e prevedendo spazi di sperimentazione normativa per facilitare un’innovazione responsabile.

Così ricostruita, risulta evidente come la Digital Finance Strategy si inserisca a pieno titolo nella Digital Single Market Strategy, aggiungendo un tassello di essenziale rilievo “verticale” al Decennio digitale sotto il profilo dei diritti (tutela degli investitori e la protezione dei consumatori) e dei mercati, delle attività e dei processi, nonché dei soggetti (in termini di integrità, innovazione, sicurezza e concorrenza) che intervengono nella catena del valore e nell’offerta dei servizi di pagamento e finanziari. Ciò, d’altra parte, non significa, né implica che la Digital Finance Strategy sia immune da interferenze ed intersezioni di tipo “orizzontale”. Al contrario, le traiettorie della Strategia, seppure diversamente articolate per modello, organizzazione e funzioni, condividono un essenziale fondamento tecnologico: il ricorso a tecniche innovative e predittive, che rimandano ma non si esauriscono in sistemi di intelligenza artificiale.

Ecco allora che la Strategia sulla finanza digitale deve essere “contestualizzata” alla luce della Strategia dei dati in generale ed in particolare della “Legge sull’Intelligenza Artificiale”, tesa ad intervenire sull’immissione in commercio di tali sistemi (guidata dai principi fondanti “new functionality – new rules” e “same risks – same supervision”), classificandoli per poi correggerli di obblighi commisurati ai rischi (inaccettabili, rischio alto, rischio basso) attesi per i diritti fondamentali (che qualificano la cifra distintiva del sistema valoriale UE). In concreto, non solo le attività specificamente connesse al credit scoring (ad esempio il targeting delle acquisizioni per il marketing, la modellazione delle riscossioni e i modelli standard di credit scoring) rientrano nel raggio di azione della Proposta, ma più ampiamente le innovazioni del settore finanziario vanno inquadrare e devono essere filtrate alla luce delle nuove regole, tenuto conto che i modelli di algo-governance e i sistemi IA sono per natura tecnologicamente neutrali e per vocazione transazionali (in chiave geografica) e inter e intra-settoriali

(in chiave merceologica). Con una doppia avvertenza. Uno: nel rapporto tra discipline verticali e orizzontali (anche) in materia di finanza digitale, rimane fermo il principio secondo cui le prime prevalgono ogniqualevolta l'interesse sotteso sia adeguatamente protetto, anche sotto il profilo dei rimedi, senza che residuino ambiti "scoperti" in termini di diritti e tutele. Due: nell'intreccio tra interventi di carattere orizzontale e di carattere verticale, attenzione crescente va riservata ai "regulatory sandboxes", sabbie che consentono la creazione di uno spazio "controllato" in cui testare forme di sperimentazione funzionali a garantire il tempestivo adeguamento delle regole alle sfide della transizione digitale all'insegna di un modello esso stesso innovativo (in quanto multistakeholder e co-regolatorio).

Fermi questi "paletti" e tenuto conto della "relazione biunivoca" tra Strategia del mercato unico digitale e Pacchetto sulla finanza digitale, obiettivo del Volume è analizzare, anzi scandagliare, le diverse dimensioni della Strategia e le politiche europee sull'intelligenza artificiale, per verificare con il contributo dei Maestri della materia e della comunità scientifica, degli addetti ai lavori e degli operatori del settore se i tempi siano maturi per l'emersione di un nuovo ordinamento giuridico, quello del digitale, ovvero se categorie e strumentario tradizionali siano (ancora) in grado di cogliere e intercettare la discontinuità, offrendo soluzioni adeguate e soddisfacenti al nuovo che avanza.

V.F.

Roma, 27 aprile 2023

Si ringraziano l'Erasmus+ Programme dell'Unione Europea, la Cattedra Jean Monnet in Digital Transformation and AI Policy, la Banca d'Italia e il PRIN2020 E-Agorà: Online Contracts Platform, nonché il Dipartimento in Scienze Umane dell'Università Europea di Roma per il contributo e sostegno alle attività di ricerca e alla pubblicazione del Volume.

Il sostegno della Commissione Europea e dell'Erasmus+ Programme dell'Unione Europea non costituisce approvazione del contenuto, che riflette esclusivamente il punto di vista degli Autori. La Commissione Europea non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni ivi contenute.

Valeria Falce

# Strategia dei dati. Traiettorie orizzontali e applicazioni verticali

SOMMARIO: 1. Introduzione. – 2. Dalle direttrici ... – 2.1. Agli assi cartesiani della strategia dei dati. – 3. Un'applicazione. Dalla strategia per la finanza digitale. – 3.1. Alla democratizzazione della consulenza. – 4. Conclusioni.

## 1. Introduzione

La transizione digitale mette in crisi i paradigmi classici, sancendo il primato della disintermediazione e del decentramento nei rapporti, la contaminazione e conseguente integrazione tra attività, prodotti e servizi, l'emersione di nuovi protagonisti e la riqualificazione dell'utente-consumatore, che, rilasciando dati ogni volta che è connesso, contribuisce a definire i contenuti e a produrre i servizi di cui fruisce, divenendo corresponsabile delle esperienze che gli si presentano<sup>1</sup>.

In questo contesto, sono oggetto di profonda riflessione (se non di eventuale ripensamento) le categorie giuridiche rilevanti, i soggetti (*tech*<sup>2</sup>),

---

<sup>1</sup>In argomento, mi si permetta di rinviare a V. FALCE, G. GHIDINI, G. OLIVIERI, *Informazione e Big Data tra Innovazione e Mercato*, in *Quad. romani dir. comm.*, 2018; V. FALCE, *Financial Innovation tra disintermediazione e mercato*, Torino, 2021; V. FALCE, A. GENOVESE, *La portabilità dei dati in ambito finanziario*, in *Quaderno FinTech*, Consob, 2021; V. FALCE, J. CANNATA, O. POLLICINO, *Legal Challenges of Big data*, Cheltenham, UK, 2020; V. FALCE, G. FINOCCHIARO, *FINTECH: Diritti, Concorrenza, Regole*, Bologna, 2019; V. FALCE, *Intelligenza artificiale e Fintech. Consulenza decentrata tra algo-governance ed elemento fiduciario*, in *Intelligenza artificiale e diritto: una rivoluzione?*, a cura di A. Pajno, F. Donati, A. Perrucci, Il Mulino, Bologna, 2022.

<sup>2</sup>Per una disamina delle peculiarità che hanno portato alla nascita delle Techfin e delle loro caratteristiche si veda D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, J.N. BARBERIS, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, in *EBI Working Paper Series*, n. 6, 2017.

i processi e i servizi (*unbundled*), i mercati (disintermediati), i modelli (*market place model*) e i rapporti (non più fiduciari)<sup>3</sup>.

La transizione a cui si assiste è di tipo intersettoriale<sup>4</sup>, si caratterizza per processi di *fintegration*<sup>5</sup> e promuove una nuova economia fondata sui dati (personali, anonimizzati e commerciali), il cui valore è certo e le cui implicazioni sono strettamente legate agli usi attuali e potenziali a cui il singolo dato è o può essere destinato attraverso il ricorso a tecniche digitali estremamente sofisticate<sup>6</sup>.

A partire da una embrionale funzione di interconnessione decentralizzata e diffusa, la rete assume oggi una rilevanza diversa, che non si limita ad incidere le strutture economiche specialistiche (mercati e intermediari finanziari, *in primis*). Il processo di digitalizzazione delle relazioni economico-sociali dovuto all'uso estensivo dell'ICT (*Information and Communication Technology*) e dell'IOT (*Internet Of Things*) innesca, insomma, trasformazioni inattese sia a livello imprenditoriale – favorendo l'integrazione tra diversi settori industriali, aprendo nuovi mercati e trasformando i modelli di *business* e l'organizzazione del lavoro aziendale – sia a livello con-

---

<sup>3</sup> C. SCHENA, A. TANDA, C. ARLOTTA, G. POTENZA, *Lo Sviluppo del Fintech – Opportunità e Rischi per l'Industria Finanziaria nell'Era Digitale*, Consob, Milano, 2018; BANCA D'ITALIA, *Fintech in Italia – Indagine Conoscitiva sull'Adozione delle Innovazioni Tecnologiche Applicate ai Servizi Finanziari*, Banca d'Italia, Roma, 2017; R. LENER, *Fintech, Diritto, Tecnologia e Finanza*, Roma, 2018; A. JANCZUK, GORYWODA, *Evolution of EU Retail Payments Law*, in *European Law Review*, 2015, 40, 858; R. FERRARI, *L'era del Fintech. La Rivoluzione Digitale nei Servizi Finanziari*, Milano, 2016; M. ZACHARIADIS, P. OZCAN, *The API economy and digital transformation in financial services: the case of open banking*, in *SWIFT Institute Working Paper n. 2016-001*, 2016; D. ZAOTTINI, L. LO PRATO, *La centralità dell'Unione Europea nei Settori Bancario, Finanziario ed Assicurativo*, Servizio Studi del Senato, 2018; D. MILANESI, *A new banking paradigm: the state of open banking in Europe, the United Kingdom and the United States*, in *TTLF Working Papers n. 29*, 2017; ISO/TC 307 – Blockchain and Distributed Ledger Technologies.

<sup>4</sup> «*Fintech*» is an umbrella term encompassing a wide variety of business models» in ECB, *Guide to Assessments of Fintech Credit Institution Licence Applications*, September 2017.

<sup>5</sup> In cui operatori tradizionali e operatori specializzati nella raccolta e analisi massiva di dati vengono sottoposti a controllo unitario così integrando servizi e attività tradizionalmente distanti, aprendo nuovi mercati e trasformando i modelli di business e l'organizzazione del lavoro.

<sup>6</sup> Si rinvia allo studio promosso dalla Committee on Payments and Market Infrastructures (CPMI), 2014, che ha distinto le diverse categorie di enti non bancari che operano attualmente nel mercato finanziario (Provider di *front-end* – ovvero sia fornitori di servizi di interfaccia tra gli utenti finali dei servizi di pagamento e il tradizionale processo di compensazione e regolamento; Provider di *back-end* – enti non bancari che forniscono servizi, esternalizzati dalle banche, collegati a determinate fasi della catena di pagamento, quali ad es. servizi di sicurezza dei dati, di data center, di audit, ecc.; Operatori di infrastrutture di pagamento al dettaglio – operatori che offrono, spesso collaborando con le banche, servizi specifici di compensazione e elaborazione per le transazioni con carta; Provider *end-to-end* – quale categoria composta da una combinazione delle precedenti).

sumeristico, incidendo l'organizzazione imprenditoriale e sociale.

In linea con la c.d. *open innovation*, il nuovo ecosistema è caratterizzato da una rete aperta di servizi modulari per imprese, individui, intermediari bancari, finanziari e assicurativi in una logica di cooperazione-concorrenza. La sinergia fra innovazione tecnologia ed *expertise* finanziaria<sup>7</sup> si traduce in una rinnovata offerta di prodotti e servizi, caratterizzati appunto dalla digitalizzazione, dalla disintermediazione e dalla decentralizzazione, nonché dall'allargamento dei soggetti che partecipano al sistema.

L'utilizzo dei Big Data<sup>8</sup>, delle tecniche di profilazione degli utenti ed il ricorso ai sistemi di intelligenza artificiale<sup>9</sup>, costituiscono delle leve offerte

---

<sup>7</sup> Il lessema Fintech descrive, in particolare, il fenomeno in base al quale si assiste ad una offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica. Tale innovazione finanziaria, resa possibile dalla tecnologia, riverbera i suoi effetti sia nel campo dei servizi finanziari sia bancari, modificandone la struttura. Il termine Fintech nasce, infatti, dalla crasi delle parole "finanza" e "tecnologia" ed è traducibile nella formulazione generica "tecnologia applicata alla finanza", in *Lo sviluppo del Fintech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderni Fintech CONSOB*, n. 1, marzo 2018, VIII.

<sup>8</sup> EUROPEAN SUPERVISORY AUTHORITIES, *Joint Committee Final Report on Big Data*, 2018; V. FALCE, G. OLIVIERI (a cura di), *Big Data e Concorrenza nei mercati dell'innovazione*, Milano, 2018.

<sup>9</sup> La Proposta di regolamento sull'approccio europeo all'Intelligenza Artificiale (COM(2021) 206 final) ha un chiaro obiettivo: delineare una cornice giuridica alta e armonizzata. Alta perché l'ambizione è di promuovere lo sviluppo dell'IA, per un verso affrontando i rischi per la sicurezza e i diritti fondamentali e per altro verso garantendo la certezza giuridica necessaria per facilitare investimenti, innovazione e concorrenza nel settore dell'intelligenza artificiale. Armonizzata perché lo sforzo è di definire regole uniformi da applicare centralmente a livello UE. L'ambizione si scontra però con un ambito di intervento limitato. Il regolamento, infatti, non intende esaurire i profili di interesse giuridico dell'IA; intende piuttosto inserirsi in un quadro normativo più ampio, definendo un decalogo di divieti e obblighi modulati e scalari sulla base del rischio che il sistema IA solleva rispetto ai valori dell'Unione. Da questo punto di vista, ferma (ma con assoluta) è la risposta della Commissione nei confronti dei sistemi che creano un rischio inaccettabile rispetto ai valori dell'Unione. Vengono così vietati, con eccezioni e deroghe, i sistemi che utilizzano tecniche subliminali in grado di manipolare il comportamento di un soggetto con probabili conseguenze fisiche o psicologiche a danno di quel soggetto o di altri soggetti; quelli che sfruttano le debolezze di un gruppo specifico di soggetti vulnerabili come l'età, la disabilità fisica o mentale al fine di manipolare il comportamento di un soggetto appartenente a tale gruppo, con probabili conseguenze fisiche o psicologiche a danno di quel soggetto o di altri soggetti; quelli utilizzati dalle pubbliche autorità (o per conto di pubbliche autorità) al fine di valutare e classificare l'affidabilità delle persone fisiche sulla base del loro comportamento sociale; o ancora quelli che consentono l'identificazione biometrica a distanza "in tempo reale" a meno che l'uso di questi sistemi non sia strettamente necessario a finalità ritenute prevalenti. Meno rigido è l'approccio proposto nei confronti dei sistemi classificati ad alto rischio, definiti tali sulla base della possibile incidenza sulla salute e sui diritti fondamentali delle persone fisiche, nonché sul godimento dei valori fondamentali così come riconosciuti e sanciti dalla normativa primaria dell'Unione europea. In questi casi, scattano obblighi a carico del provider

ai nuovi protagonisti del sistema finanziario per competere sul mercato. Invero, grazie all'utilizzo delle informazioni ricavate attraverso tali tecnologie, gli attori sono capaci di ridisegnare il mercato finanziario (ad es. nei servizi di pagamento), configurando prodotti e servizi finanziari *ad hoc* per i clienti estremamente vantaggiosi e, talvolta, persino gratuiti<sup>10</sup>.

Sul fronte delle dinamiche interne all'impresa, le ripercussioni sono di pari "distruzione creativa". In punto di tecnologie, si assiste ad una imprevista escalation, in cui campeggiano la Behavioural Biometrics insieme ai processi di Intelligence Business Management. In punto di obiettivi, si registra un cambio di registro senza precedenti. Dall'automazione attraverso programmi e software che compiono più velocemente operazioni note, si passa alla predizione e all'orientamento dei comportamenti attraverso l'acquisizione e poi l'elaborazione di dati e soluzioni, che si correggono da sole valutando in tempo reale rischi ed opportunità. In punto di modello organizzativo, le potenzialità sono notevolissime. Dalla struttura piramidale e a silos si passa al decentramento delle decisioni, al bazar, e di qui dalla *platform governance* alla *community-driven governance*, con una integrazione sempre maggiore di professionalità diverse all'interno della compagine societaria grazie al ricorso a strumenti e tecnologie abilitanti che assicurano la partecipazione a livello diffuso e capillare. In punto di metodo, le implicazioni sono a raggera. Dalla c.d. delega discendente, in cui all'algoritmo viene assegnato un ruolo all'interno del processo operativo con funzione

---

e del produttore. Di valutazione e autovalutazione della conformità del prodotto e del rischio, di informazione e trasparenza, nonché di sicurezza e affidabilità. Decisamente più morbida è la proposta nei confronti degli altri sistemi, quelli che risultano pericolosi per il sistema valoriale UE e che vengono lasciati all'autodeterminazione del mercato, nel rispetto di taluni limiti: il rispetto della *fairness* e della correttezza. La Proposta è lontana dall'essere legge europea e molte sono gli snodi e le questioni aperte, soprattutto nella prospettiva di garantire un giusto equilibrio tra le ragioni dell'innovazioni e del mercato. Punto fermo è però l'impianto: la scelta della graduazione delle regole sulla base dei rischi, infatti, non è nuova, ma riflette indirizzi di *policy* che già si sono affermati con successo in settori affini, se non contigui (dispositivi medicali). Né deve sorprendere la direttrice imboccata dal punto di vista istituzionale e di *governance*, perché la centralizzazione dei poteri è propria dell'evoluzione del diritto europeo, si accompagna alle fasi di svolta delle politiche europee in cui l'uniformità di indirizzi e di soluzioni è imprescindibile. Né infine deve meravigliare lo stampo impresso al regolamento, di raccordo con i diritti fondamentali, perché il sistema valoriale dell'Unione ne è la cifra distintiva da consolidare a livello interno e auspicabilmente esportare a livello internazionale. In argomento, mi si permetta di rinviare a V. FALCE, V. PANZIRONE, *L'intelligenza artificiale spiana la strada a organizzazioni a rete*, in *Il Sole24Ore*, 16 marzo 2021; V. FALCE, *Intelligenza artificiale, regole a tenuta dei valori UE*, in *Il Sole24Ore*, 6 ottobre 2021.

<sup>10</sup> Si veda sul punto, *inter alia*, EUROPEAN BANKING AUTHORITY, *EBA Report on the impact of fintech on incumbent credit institutions' business models*, 2018; ESMA, EBA, EIOPA, *Joint Committee Final Report on Big Data*, 15 March 2018, JC/2018/04.

consultiva, a quella c.d. ascendente ed integrata, in cui ruolo e funzioni tendono ad essere autonome dal contributo umano<sup>11</sup>.

## 2. Dalle direttrici ...

In questa tempesta perfetta c'è un punto fermo: il dato nella sua veste multiforme. Quello personale (oggi disciplinata dal regolamento (UE) 2016/679), che si erge ad input essenziale per la realizzazione di prodotti e servizi sempre più rispondenti ai bisogni di ciascuno; quello non personale (definito per differenza dalla regolazione) capace di traghettare il dato personale nell'arena commerciale (disciplinato dal regolamento n. 1807/2018) che soggiace al principio della libera regolazione; quello confidenziale e riservato (regolato dalla direttiva n. 943/2016), perché la sua circolazione entro una cerchia ristretta di soggetti è funzionale alla promozione di forme di cooperazione inter- e intra-settoriale; quello pubblico (oggetto della Regolazione open data) e quello pubblicamente disponibile, accessibile grazie e attraverso la rete, che diventa parte di raccolte digitali, mobili, interattive e dinamiche (disciplinate dalla direttiva 96/9/CE), che risultano utili a migliorare prodotti e servizi, generare efficienze e innescare processi innovativi.

---

<sup>11</sup> Il fermento è vulcanico, le traiettorie sono numerosissime. Eppure, in punto di trasparenza e *accountability*, e di qui di diritti e responsabilità, l'elaborazione è ancora inadeguata. Sul fronte dei diritti, l'Europa ha stabilito che le regole di proprietà intellettuale sono sufficienti. Dal punto di vista delle responsabilità, mentre nel 2017 il Parlamento UE aveva gettato le basi per riconoscere la soggettività giuridica dell'IA, a fine 2020 ha negato ogni possibile reinterpretazione "creativa" dei principi internazionali della materia, a partire dalla Convenzione di Berna. Ma allora se l'IA non è un soggetto di diritto, chi deve rispondere degli inevitabili falsi, degli eventuali errori e delle conseguenze che da queste possono scaturire? Possono valere le regole di responsabilità oggettiva che si sono affermate per l'ipotesi di prodotto difettoso, o invece si deve ragionare sulla responsabilità del suo titolare/proprietario ovvero dell'utilizzatore che se ne giova, o ancora va invocata la teoria dell'estensione della soggettività del suo creatore? Il dibattito è acceso e numerose le proposte. E allora, nell'attesa di una nuova Data Governance, la strada da seguire rimane quella tratteggiata da Luigi Einaudi nelle Prediche inutili: mappare, conoscere e solo infine indicare una nuova policy. Se così è, si tratta di rafforzare la "cultura dell'IA" dentro e fuori l'impresa. Innanzitutto, attraverso Commissioni CorpTech che sappiano favorire la comprensione delle tecnologie smart a livello intra-aziendale e il dialogo al di fuori dell'azienda, nei rapporti con regolatori e autorità, che a loro volta stanno inaugurando la stagione della RegTech. In argomento, mi si permetta di rinviare a V. FALCE, V. PANZIRONE, *L'intelligenza artificiale spiana la strada a organizzazioni a rete*, in *Il Sole24Ore*, 16 marzo 2021; V. FALCE, *Intelligenza artificiale, regole a tenuta dei valori UE*, in *Il Sole24Ore*, 6 ottobre 2021.

Senonché, l'eterogeneità del dato solo apparente, perché indipendentemente da forma e natura, tecniche e sistemi di intelligenza artificiale consentono di scomporre e ininterrottamente riaggregare ogni bit con altre informazioni, anche apparentemente scollegate, ora per essere oggetto di studio, simulazione e sperimentazione, ora per essere catalogato in cluster orientati alla profilatura e alla commercializzazione.

Nel nuovo ecosistema, insomma, i dati, filtrati attraverso le nuove tecnologie, si impongono per la valenza mutante e acquisiscono un valore che, dipendendo dalla combinazione e dall'uso a cui sono destinati, diventa sempre più fluido e mobile. Così decodificati, i dati si svelano come coesenziali alla definizione della cornice di riferimento e poi al funzionamento e allo sviluppo dell'economia liquida, con implicazioni importanti sul fronte istituzionale e di governo (tese a rivendicare la necessità di un'autorità europea IA).

## 2.1. Agli assi cartesiani della strategia dei dati

Si è appena detto che i dati sono pilastri e fondamenta della nuova strategia europea. Si può ora precisare che questa si snoda lungo due direttrici essenziali: l'una (1) centripeta ed interna – volta al rafforzamento dell'autonomia strategica, l'altra (2) centrifuga ed esterna – tesa all'exportazione del modello europeo su scala globale. L'una (la forza esterna) si va delineando attraverso una dichiarazione di principi e un atto non vincolante, un'alleanza che raccolga e sintetizzi indirizzi e posizioni codificate a livello UE. L'altra (la forza interna) è modellata dalla e nella *single market strategy*, con implicazioni a raggiera, che possono essere così sintetizzate.

In particolare, in punto di sistema, la scelta di indirizzo è univoca, tendendo verso regolazioni umanocentriche nell'*imprimatur*, neutrali e orizzontali nell'applicazione con rafforzati raccordi e coordinamenti con regolazioni verticali e settoriali. In termini di tecnica, si afferma il modello *multistakeholder* in cui l'armonizzazione massima delle regole è completata attraverso forme di autoregolamentazione e codici di condotta. In chiave istituzionale e di *governance*, la direzione è quella dell'accentramento dei poteri di definizione, attuazione ed *enforcement*, rafforzamento dei profili di coordinamento con autorità nazionali e *favor* nei confronti di scambi di informazioni. Quanto ai contenuti, questi si incastonano in una cornice ampia, i cui tasselli sono i mercati e i servizi digitali, il governo dei dati, pub-

blici e privati, l'intelligenza, l'identità digitale e la sicurezza digitale, a tendere il mercato dei dati.

Entro la cornice ora tratteggiata si gettano le basi per il consolidamento del mercato europeo dei dati: aperto, libero, contendibile e come tale fair e competitivo.

A tal fine, si opta per una architettura alta e comune, informata da regole orizzontali. Non per imbrigliare l'innovazione, ma per riportarla entro guide sicure, dando corpo a quella autonomia strategica cui si accennava. Due i binari di riferimento, che rimandano ad altrettanti principi fondanti.

Il primo sposta il fuoco dal soggetto all'attività: "stessa attività, stesso rischio, stesse regole e supervisione". Le attività insomma vengono graduate sulla base dei rischi che sollevano rispetto a beni omogenei, indipendentemente da chi e attraverso quali modalità i servizi vengano offerti. Questo è vero in ogni settore e si applica ad ogni attività. Per i mercati e i servizi digitali (oggetto di regolazioni europee: DMA e DSA) vale la regola secondo cui quel che è lecito off line, lo è on line e quel che è illecito offline, lo è pure on line, perché alle medesime attività che sollecitano il medesimo rischio devono seguire le medesime regole<sup>12</sup>.

Il secondo allarga il campo delle attività senza spostare l'asse delle responsabilità: "esternalizzazione sì, impunità no"<sup>13</sup>. L'esternalizzazione è una chance differenziale per allargare il mercato, mai uno schermo dalle responsabilità. Indipendentemente dal ricorso ad un soggetto tecnologico in affiancamento o in sostituzione nella creazione e fornitura di servizi, insomma, ferma è l'imputazione dei rapporti e la responsabilità delle azioni. Anche sotto forma di corresponsabilità.

L'effetto è l'innalzamento dei nuovi protagonisti tecnologici a soggetti di diritto in ragione e sulla base dell'attività prestata, e di qui la loro responsabilizzazione in quanto operatori di mercato.

Le implicazioni sono rassicuranti. A prescindere dalla affermazione di reti organizzative, dal ricorso a contratti *smart* e a tecnologie avanzate, sono l'attività e il servizio proposto a dover orientare il regolatore.

---

<sup>12</sup> Da ultimo, in tema, S. ARAMONTE, W. HUANG, A. SCHRIMPF, *DeFi risks and the decentralisation illusion*, accessibile a [https://www.bis.org/publ/qtrpdf/r\\_qt2112b.pdf](https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf).

<sup>13</sup> EBA, *Orientamenti in materia di esternalizzazione*, EBA/GL/2019/02, accessibile a [https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/1c9aaefc-e10d-45a6-8a51-1fb450814a29/EBA%20revised%20Guidelines%20on%20outsourcing\\_IT.pdf?retry=1](https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/1c9aaefc-e10d-45a6-8a51-1fb450814a29/EBA%20revised%20Guidelines%20on%20outsourcing_IT.pdf?retry=1).

### 3. Un'applicazione. Dalla strategia per la finanza digitale

Se è vero che quelli ora accennati sono gli assi cartesiani della strategia dei dati, è altrettanto vero che transizione digitale, algoritmi e intelligenza artificiale<sup>14</sup> sono al centro *anche* (e non a caso) della Strategia per la finanza digitale (Digital Finance Strategy – DFS 2020), che si propone di dare impulso e sostegno allo sviluppo della finanza *data driven* nell'UE<sup>15</sup>.

Tra le misure più rilevanti previste dalla strategia sulla finanza digitale campeggiano i tre Regolamenti rispettivamente sui mercati in cripto-attività (“Regulation on Markets in Crypto-assets – MiCAR”), sulla resilienza operativa digitale nel settore finanziario (“Regulation on digital operational resilience for the financial sector – DORA”) e su un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (“Regulation on a pilot regime for market infrastructures based on distributed ledger technology – PILOT”).

Quanto alla tematica delle cripto-attività, è pacifico che la Commissione europea ha promosso una molteplicità di iniziative normative in materia di Fintech volte sia a valutare l'eventuale applicazione di norme esistenti e ancora vigenti ad attività innovative ma funzionalmente simili e comparabili (in ossequio al principio “*same business, same risks, same rules*”) sia ad introdurre, ove opportuno, nuovi presidi regolamentari (secondo il bro-

---

<sup>14</sup> Fra queste si ricordano in particolare l'Agenda europea 2019-2024; la nuova strategia per la sicurezza informatica (*The EU's Cybersecurity Strategy for the Digital Decade*); la strategia globale per la cooperazione in materia digitale (*Global Digital Cooperation Strategy*) e le iniziative rientranti nel quadro delle relazioni bilaterali con paesi terzi e contesti multilaterali; l'azione di sostegno alla trasformazione digitale delle economie in via di sviluppo (Digital4Development Hub); il Libro Bianco sull'Intelligenza Artificiale; il *Digital Services and Markets Act* package; la proposta di regolamento *New Competition Tool*; la Comunicazione sulla strategia europea per i dati (*Data Act*); il programma *NextGenerationEU*; il *Digital Compass*. Da ultimo, la proposta *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*, presentato come «*the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally*» e che mira a istituire un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale in conformità ai valori dell'Unione. Cfr., anche, D.A. ZETZSCHE, A.W. DOUGLAS, R.P. BUCKLEY, B. TANG, *Artificial Intelligence in Finance: Putting the Human in the Loop*, in *CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship*, n. 1, University of Hong Kong Faculty of Law Research Paper No. 2020/006, 2020, disponibile all'indirizzo web [www.ssrn.com](http://www.ssrn.com).

<sup>15</sup> Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito, COM/2020/594 final.

cardo “*new functionality, new rules*”). Il MiCAR, dunque, favorisce un quadro armonizzato a livello europeo per l’emissione di cripto-attività e la prestazione di servizi che le hanno ad oggetto, introducendo una disciplina *bespoke* del mercato dei *crypto-asset* diversi dagli strumenti finanziari. Gli aspetti fondamentali sono: i) una definizione comune di *crypto-asset*, con un approccio, per così dire, “*catch-all*”, anche in funzione antielusiva; ii) la “passaportazione” delle offerte previa notifica di un *white paper*, nonché un regime di autorizzazione dei service provider (MiFID-like); iii) regole per l’integrità del mercato (MAR-like); iv) una disciplina più stringente degli *stablecoins*, ossia, in gergo europeo, degli *asset reference token* (ART), e degli *e-money token*, con una vigilanza dell’EBA su quelli significativi e un coinvolgimento forte della BCE; v) una disciplina unica delle esenzioni, ossia di ciò che non rientra nella proposta MiCAR.

Con DORA, invece, il Legislatore europeo definisce norme uniformi e trasversali in materia di sicurezza ICT per tutti gli operatori del settore finanziario (banche, istituti di pagamento e di moneta elettronica, imprese di investimento, gestori del risparmio, assicurazioni, fornitori di servizi in *crypto-asset* e relativi emittenti, ecc.). Il regolamento introduce, inoltre, requisiti di *governance* e gestione del rischio ICT, nonché un sistema armonizzato delle notifiche dei c.d. *major ICT-related incident*. È prevista una responsabilizzazione dei soggetti nella definizione delle misure e del grado di sicurezza desiderato, così dando impulso ad un’attività di *compliance* (non di tipo *box ticking*, ma) orientata al risultato che si combina con un c.d. *penetration test*, reso obbligatorio e supervisionato dalla autorità di settore.

Il regolamento Pilot ambisce a stabilire un “regime pilota” (sul modello *sandbox*) caratterizzato da requisiti uniformi per gli operatori di mercato che desiderano gestire un’infrastruttura di mercato DLT. Le autorizzazioni concesse a norma di tale regolamento consentiranno agli operatori di mercato di gestire un’infrastruttura di mercato DLT e di prestare i loro servizi in tutti gli Stati membri. Tramite il regime Pilot, e nell’ottica della *sandbox* regolatoria, si potranno perciò testare nuovi modelli di business “disintermediati”, svolgere su un’unica piattaforma le funzioni di *trading* e *post-trading* e adeguare le attuali norme alle caratteristiche delle infrastrutture distribuite, permettendo l’emissione di strumenti finanziari tramite DLT e l’introduzione di un regime per le infrastrutture di mercato in base al quale le autorità nazionali, in coordinamento con l’ESMA, potranno accordare deroghe mirate alla disciplina UE (CSDR in materia di depositari centrali e MiFID) e, conseguentemente la nascita di un mercato secondario degli strumenti finanziari emessi in forma di *token*.

A completare la c.d. Digital Finance Strategy, contribuisce la c.d. “Retail payments strategy”.

### 3.1. Alla democratizzazione della consulenza

Rispetto alle predette linee di indirizzo perseguite nell’ambito della finanza digitale, la consulenza automatizzata, resa attraverso piattaforme digitali e grazie all’uso di algoritmi che consentono il rilascio di raccomandazioni di investimento, ben sintetizza le nuove frontiere<sup>16</sup>.

Specificamente rivolto ad operazioni relative a strumenti finanziari (o portafogli di strumenti finanziari) da offrire su base personalizzata, il *roboadvising* identifica, infatti, un servizio attraverso cui si possono apprezzare le intersezioni ed interferenze tra il *quid novi* impresso dalle nuove tecnologie (attraverso le quali si supera l’elemento fiduciario proprio della relazione tra intermediario e cliente), il *modus operandi* dell’IA (grazie alla quale il supera la confine tra dati ed informazioni acquisiti dalle banche dati interne ed esterne alle aziende), e la risposta della regolazione (che in tema di consulenza automatizzata non è rimasta indietro).

Ma procediamo con ordine. La consulenza finanziaria tradizionale rimette all’intermediario la definizione di profili essenziali, dalla profilatura del cliente alla definizione di un’*asset allocation* confacente alle caratteristiche dell’investitore, dalla selezione delle *asset class*, al monitoraggio periodico del portafoglio ed al suo ribilanciamento. Con il *roboadvising*, invece, si innesca con gradazioni via via crescenti: a) l’automazione delle diverse fasi del processo di investimento attraverso il ricorso ad algoritmi di *asset allocation* e *risk management*; b) la “democratizzazione” dei processi, consentendo a persone fisiche, imprese ed organizzazioni private di comunicare ed eseguire transazioni in modo agevole, in tempi rapidi e a costi estre-

---

<sup>16</sup>Secondo le proiezioni di crescita del fenomeno (dati disponibili su <https://learnbonds.com/news/robo-advisors-to-become-1.4trn-worth-industry-this-year>), le attività di gestione dei *roboadvisor* ammontano a circa 1.600 miliardi di dollari nel 2020, con un bacino complessivo di 60 milioni di utenti. Negli Stati Uniti, vi è la più alta quota di utilizzo di tali piattaforme, tenuto conto di un totale di AuM (Asset under Management) gestito dai consulenti robotizzati, pari a quasi 1.000 miliardi di dollari, rappresentativi del 75% del mercato globale. Negli ultimi anni, anche nel continente asiatico il servizio ha registrato una importante crescita, grazie alla sua diffusione tra numerosissimi utenti della categoria mass markets. La Cina, infatti, risulta essere, ad oggi, il secondo paese al mondo per volume di AuM gestito da consulenti robotici. Regno Unito, Germania e Canada occupano, rispettivamente, terzo, quarto e quinto posto.

mamente ridotti; c) l'allargamento della platea dei soggetti, determinando l'ingresso delle piattaforme digitali, che intermediano l'offerta online di servizi di natura finanziaria<sup>17</sup>; d) la spinta all'emancipazione del risparmiatore ed al superamento del requisito fiduciario come tratto proprio e distintivo della consulenza.

All'acquisita autonomia di scelta rispetto alle controparti finanziarie tradizionali<sup>18</sup> corrisponde insomma un mutato identikit del risparmiatore, che si avvale di c.d. *digital tools* per accedere alla gestione e distribuzione di servizi e prodotti finanziari, ormai non più prerogativa esclusiva di investitori di alto profilo<sup>19</sup>.

Se questa è la tendenza, d'altra parte, il c.d. *Hibryd-robo-advice*<sup>20</sup> si pone a mezza strada, esaltando la professionalità dell'*advisor* tradizionale, il quale contempera le potenzialità di calcolo e previsione dell'algoritmo con le esigenze di tutela e di assicurazione dell'investitore<sup>21</sup>.

L'effetto è misto. Le dinamiche di integrazione a cui si sta assistendo segnalano (i) per un verso, la volontà degli operatori tradizionali di voler recuperare il divario tecnologico, intercettando le innovazioni tecniche delle piattaforme digitali per metterle a vantaggio della propria offerta, (ii) per altro verso, la preminenza delle c.d. Platform Companies, le cui capacità di occupare diversi settori di mercato, grazie ai propri canali di *costumer experience*, ben possono degenerare in autentici *gate keeper*, con conseguenze preoccupanti per l'innovazione e la concorrenza.

Ebbene, in questo “caos calmo”, la regolazione tenta una di definire un equilibrio tra rischi e benefici del progresso tecnologico, valutando l'impatto dei sistemi di intelligenza artificiale sulla stabilità, la trasparenza, la

---

<sup>17</sup> Ciò grazie alla facilità di comunicazione e di accesso ai mercati di scambio da parte degli utenti, assicurata, per un verso, dall'utilizzo di risorse infrastrutturali sempre più potenti ed elastiche e, per altro verso, dalle capacità di ricerca, elaborazione, stoccaggio e celere trasmissione delle informazioni (Artificial Intelligence, Machine Learning, Application Program Interface, Distribute Ledger Technology, ecc.).

<sup>18</sup> M. PANEBIANCO, *L'industria dell'Asset Management nel 2020*, Pwc, giugno 2017.

<sup>19</sup> Sulle implicazioni rilevanti si rinvia, inter alia, a C. CASTELLUCCIA, D. LE MÈTAYER, *Study on 'Understanding algorithmic decision making: Opportunities and challenges'*, Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament, 2019, disponibile all'indirizzo web [www.europarl.europa.eu](http://www.europarl.europa.eu).

<sup>20</sup> PWC, *Robo Advisory Human Advisory, Indagine aprile 2015*, accessibile all'indirizzo <https://www.pwc.com/it/it/industries/asset-management/assets/docs/robo-advisory.pdf>.

<sup>21</sup> J.E. FISCH, J.A. TURNER, *Robo Advisers vs. Humans: Which Make the Better Financial Advisers?*, University of Pennsylvania Law School-Institute for Law and Economics, Philadelphia, March 2017.

tutela degli investitori e, soprattutto, sulla fiducia nel sistema finanziario<sup>22-23</sup>.

Con la direttiva 2004/39/CE (Market in Financial Instruments Directive – MiFID), e la relativa direttiva di attuazione 2006/73/CE, il servizio di consulenza è stato incluso tra i servizi di investimento, assumendo così la prerogativa di attività riservata, sottoposta a specifiche norme di comportamento, che può essere prestata solo da particolari categorie di soggetti, quali – nel caso specifico – banche, SIM, SGR, nonché da consulenti finanziari e società di consulenza finanziaria (rispettivamente persone fisiche e giuridiche *ex artt.* 18 *bis* e 18 *ter* TUF). Con il pacchetto MiFID II/MiFIR (direttiva 2014/65/UE, regolamento delegato UE 2017/565 e relativi atti di esecuzione), è stata introdotta la nozione di consulenza proposta su base indipendente. Con le linee guida in materia di valutazione di adeguatezza della European Securities and Markets Authority (ESMA, 2018)<sup>24-25</sup> si è inteso favorire l'armonizzazione delle *policies* di supervisione, in tema di requisiti di adeguatezza che devono essere garantiti da tutti i soggetti attivi nel mercato dei servizi di consulenza in materia di investimenti. In altri termini, la scelta è di includere nell'eterogeneo *genus* dei *robo advice* ogni

---

<sup>22</sup> Con riferimento sul piano dell'ordinamento italiano, un cenno merita la recente sottoscrizione di un Protocollo d'intesa per l'istituzione del Comitato di coordinamento per il *fintech* promosso dal Ministero dell'Economia e delle Finanze, cui hanno aderito anche la Banca d'Italia, Consob, IVASS, Garante per la Protezione dei dati personali, AGID e Agenzia dell'Entrate. Il Comitato favorisce l'elaborazione di una visione complessiva e condivisa del *Fintech* e l'individuazione degli aspetti di sistema ed operativi più rilevanti per il Paese attraverso la cooperazione e lo scambio di informazioni tra le Amministrazioni che aderiscono al presente Protocollo. Esso, tra le altre cose è deputato all'approfondimento degli aspetti regolamentari e funzionali, al fine di formulare eventuali proposte di intervento normativo, garantendo così adeguati livelli di tutela dei consumatori e della concorrenza.

<sup>23</sup> P. MAUME, *Regulating Robo advisory*, in *Texas Journal of International Law*, April 2018; R.P. BUCKLEY, D.W. ARNER, D.A. ZETZSCHE, E. SELGA, *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*, in *UNSW Law Research Paper No. 19-89*, *European Banking Institute Working Paper 2019/54*, *University of Luxembourg Law Working Paper 2019-009*, *University of Hong Kong Faculty of Law Research Paper No. 2019/112*, disponibile all'indirizzo web [www.ssrn.com](http://www.ssrn.com); M. KOVAC, *Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework*, in *European Journal of Risk Regulation*, 2021, 1-20. Per un approccio comparato con il Regno Unito si veda anche: E. BRAVO, *Views across the channel on digital regulation*, disponibile all'indirizzo web <https://www.biicl.org/blog/15/views-across-the-channel-on-digital-regulation>.

<sup>24</sup> ESMA, *Final Report. Guidelines on certain aspects of MIFID II suitability requirements*, 28 May 2018.

<sup>25</sup> Il 13 luglio 2017, l'ESMA ha pubblicato un documento di consultazione sul progetto delle *guidelines* su alcuni aspetti dei requisiti di adeguatezza MIFID II al fine di rendere esplicite la proposta, le relative motivazioni e raccogliere i contributi delle parti interessate. La consultazione è stata chiusa il 13 ottobre 2017, a cui hanno partecipato 53 interventi.

fattispecie, senza distinzione tra le varie tipologie di sviluppo tecnico. Di conseguenza, anche i sistemi consulenziali che adottino modalità operative che prescindono dalla necessità di contatti diretti con la clientela, sono soggetti alle norme tecniche stabilite dall'Autorità di settore.

Sulle imprese di investimento ricade, insomma, la responsabilità dello svolgimento delle valutazioni di idoneità dei servizi prestati, anche nei casi in cui le attività di consulenza siano eseguite, in tutto o in parte, attraverso sistemi automatizzati o semi automatizzati<sup>26</sup>. La soluzione prospettata conduce ad una *algo-governance*<sup>27</sup>. Minimo comune denominatore di tali interventi disciplinari è quello di richiedere che le modalità di configurazione e di governo degli applicativi tecnologici, siano tali da assicurare: (i) sostenibilità sociale ed ambientale (deve apportare benefici nei confronti della società in generale e delle generazioni a venire); (ii) *accountability*, (possibilità di individuare un processo per l'adozione di tecniche di intelligenza artificiale e soggetti che ne rispondano e lo guidino); (iii) equità (nella duplice accezione di giustizia e non discriminazione); (iv) trasparenza (che include un concetto di comprensibilità proporzionata al soggetto nei cui confronti va garantita)<sup>28</sup>; (v) sicurezza tecnologica e protezione dei dati personali (inclusa la possibilità di garantire al proprietario di avere accesso ai propri dati)<sup>29</sup>.

L'effetto è duplice (e si coglie in una serie di interventi<sup>30-31</sup>, anche in

---

<sup>26</sup> In questo contesto, il principio di proporzionalità potrebbe fungere da agevole parametro applicativo delle norme tecniche di settore, in particolar modo nei riguardi dei c.d. *robo for advice*. In applicazione di tale principio, infatti, si potrebbe giungere ad una più compiuta verifica e conseguente attribuzione dei profili di responsabilità tra componente umana e digitale, allorché l'utilizzo dello strumento digitale da parte del professionista comporti una valutazione di adeguatezza con possibili ricadute nei rapporti con la clientela. M.T. PARACAMPO, *L'adeguatezza della consulenza finanziaria automatizzata nelle linee guida dell'ESMA tra algo-governance e nuovi poteri di supervisione*, in *Riv. dir. banc.*, accessibile su [www.dirittobancario.it](http://www.dirittobancario.it), 52, 2018, 2.

<sup>27</sup> M.T. PARACAMPO, *op. cit.*, 56.

<sup>28</sup> C. CATH, *Governing artificial intelligence: ethical, legal and technical opportunities and challengers*, in *Philos Trans A Math Phys Eng Sci.*, 2018 October 15, 376.

<sup>29</sup> D. CAPONE, *La governance dell'Artificial Intelligence nel settore assicurativo tra principi etici, responsabilità del board e cultura aziendale*, in *Quaderno IVASS* n. 16, febbraio 2021.

<sup>30</sup> Direttiva 2014/65/UE del Parlamento Europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE. La MIFID II valorizza la relazione tra cliente e consulente, così come le competenze specialistiche e professionali del consulente, da sempre elementi fondanti della nostra proposta di consulenza specializzata. Inoltre, all'interno di questo nuovo quadro normativo, il cliente avrà la possibilità di fare affidamento su informazioni più approfondite in merito al proprio portafoglio di investimento e di contare su meccanismi ancora più evoluti di valutazione dell'adeguatezza delle operazioni effettuate.

<sup>31</sup> Regolamento UE n. 600/2014 del Parlamento Europeo e del Consiglio del 15 maggio

ambito assicurativo<sup>32-33</sup>). Per un verso, si assiste allo sdoganamento della c.d. *suitability rule*, tesa a rafforzare la tutela dell'investitore per il tramite di principi cardine e regole di condotta – tra cui gli assodati postulati di *know your customer* e *know your product* – con valorizzazione dell'importanza del valore del patrimonio informativo a disposizione del *manufacturer/distributor*, quale strumento in grado di proporre una maggiore tutela degli interessi della clientela<sup>34</sup>. Per altro verso, si avverte la necessità di rendere trasparente il complesso mondo degli algoritmi, da sempre tacciati come *black boxes*<sup>35</sup>, a causa di criticità intrinseche e dei profili di opacità che li contraddistinguono. Si tratteggia così un quadro disciplinare, che, con l'intento di offrire agli investitori un elevato livello di protezione, cerca di promuovere il miglioramento della qualità del servizio, per il tramite di misure atte a garantire trasparenza dei costi di gestione, nonché indipendenza da conflitti di interesse. Tuttavia, i non ancora sufficienti livelli di inclusione e cultura finanziaria<sup>36</sup> determinano nella domanda della consuevole un velo di diffidenza rispetto ai *robo advisor*<sup>37</sup>, tenuto conto dell'accentuarsi di rischi, sia endogeni che esogeni, al procedimento di investimento digitale, a causa di mancanze relative ai profili di *cybersecurity*, nonché in ragione dello sfruttamento sempre più intensivo, e non di rado, improprio, dei *Big Data*<sup>38</sup>, da cui possono derivare ricadute sulla trasparenza

---

2014 sui mercati degli strumenti finanziari e che modifica il regolamento UE n. 684/2012.

<sup>32</sup> Direttiva 2016/97 del Parlamento Europeo e del Consiglio del 20 gennaio 2016 sulla distribuzione assicurativa.

<sup>33</sup> Regolamento UE n. 1286/2014 del Parlamento Europeo e del Consiglio del 26 dicembre 2014, relativo ai documenti contenenti le informazioni per i prodotti d'investimento al dettaglio e assicurativi preassemblati.

<sup>34</sup> Considerando n. 78, Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio ed assicurativo, direttiva 2014/65/UE (c.d. Mifid II).

<sup>35</sup> ESMA, *Guidelines on MiFID II suitability requirements*, 28 May 2018.

<sup>36</sup> N. LINCIANO, P. SOCCORSO, *Le sfide dell'educazione finanziaria. La rivelazione di conoscenze e bisogni formativi, l'individuazione dei destinatari delle iniziative, la definizione di una comunicazione efficace*, in *Quaderni di finanza Consob*, ottobre 2017.

<sup>37</sup> Consob, *Le scelte di investimento delle famiglie italiane, rapporto 2020*. Si legge nel Rapporto che, con riferimento a specifici ambiti dell'innovazione finanziaria concernenti i *robo advisor*, emerge un livello di attività molto contenuto. Tra i fattori che potrebbero stimolare l'interesse emergono la possibilità di investire piccole somme e, nel caso specifico delle valute virtuali, la possibilità di guadagnare velocemente. Tra i deterrenti, invece, si citano più di frequente il timore di subire truffe e di non avere sufficienti competenze finanziarie e digitali.

<sup>38</sup> F. MATTASSOGLIO, *La profilazione dell'investitore nell'era dei Big Data. I rischi dell'estremizzazione della regola del "Know your Customer"*, in *Riv. trim. dir. econ.*, 4/2016 supplemento n. 1, 233.

e correttezza dell'utilizzo dei dati personali degli utenti<sup>39</sup>. Detto diversamente, sono la *governance* dei processi automatizzati, nonché una più compiuta ed efficiente organizzazione aziendale le leve che nelle sedi tecniche si è ritenuto di valorizzare. E ciò al fine di evitare che l'innovazione digitale possa compromettere la già precaria relazione fiduciaria tra istituzioni finanziarie e clientela.

Se *literacy gap* e *digital divide*<sup>40</sup> continuano a frenare l'emancipazione dell'investitore e del risparmiatore, a rafforzare l'elemento fiduciario contribuisce il piano delle responsabilità, che si regge su due principi fondamentali.

Il primo, che, come si è detto, è incentrato sull'attività svolta indipendentemente dalla democraticizzazione dei processi, prevede che le attività vengano graduate sulla base dei rischi che sollevano rispetto a beni omogenei, a prescindere da chi e attraverso quali modalità i servizi vengano offerti.

Il secondo, nel favorire l'allargamento delle collaborazioni e partnership anche strategiche con soggetti terzi, ribadisce che l'esternalizzazione sia una chance differenziale di penetrazione dei mercati, ma non anche uno schermo dalle responsabilità, mantenendo ferma l'imputazione dei rapporti e la responsabilità delle azioni. Anche sotto forma di corresponsabilità.

Attraverso questa doppia direttrice, a prescindere dall'*algo-governance*, sono l'attività e il servizio proposto ad orientare il regolatore e a sancire il regime delle responsabilità, dando così impulso a innovazione e mercato, senza vuoti di controllo e supervisione, e soprattutto senza rinunciare ad un sistema di diritto.

## 4. Conclusioni

Alcune considerazioni conclusive.

L'*excursus*, che precede, conferma che Strategia europea dei dati e Pacchetto sulla finanza digitale condividono la medesima finalità: cogliere ed

---

<sup>39</sup>A. SORO, Intervento del Presidente del Garante per la protezione dei dati personali all'inaugurazione del Corso di Alta formazione "Fintech e Diritto" organizzato dall'ABI, Roma 10 maggio 2018.

<sup>40</sup>Secondo i dati dell'*Un Report World Population Ageing 1950-2050*, accessibile all'indirizzo <http://www.un.org/esa/population/publications/worldageing19502050/>, la percentuale di anziani (persone oltre i 64 anni di età) sul totale della popolazione in età lavorativa (individui compresi tra i 15 e i 64 anni) raggiungerà il 25,4% nel 2050, rispetto all'11,7% registrato nel 2010.

inquadrare la discontinuità innescata dalla quarta rivoluzione industriale in chiave geo-politica, di sistema e di valori.

La distinzione, dunque, non è genetica ma di latitudine: la prima propone una cornice di tipo orizzontale e tecnologicamente neutra, mentre la seconda si focalizza verticalmente sul settore finanziario, la cui componente tecnologica è spiccata (indipendentemente dalla nuova rivoluzione industriale).

La consulenza automatizzata, nel promuovere un modello decentrato dei rapporti, è figlia della nuova rivoluzione industriale e propria del settore finanziario, schiudendo notevoli opportunità commerciali e scontando alcuni limiti. Gli uni e gli altri risultano congeniti e propri della trasformazione digitale e non specifici del settore finanziario. Così potendosi risolvere con le categorie e le soluzioni offerte dal modello generale (incentrate sui rischi e sulle responsabilità).

**Tommaso Edoardo Frosini**  
**L'Ordine giuridico del digitale**

SOMMARIO: 1. Ordine (e disordine) nel diritto digitale. – 2. Costituzionalismo e tecnologia. – 3. I nuovi diritti costituzionali nell'era di Internet. Il diritto di accesso. – 4. Segue: il diritto alla libertà di espressione. – 5. Segue: Il diritto alla privacy. – 6. Segue: il diritto all'oblio. – 7. Il diritto nell'intelligenza artificiale. – 8. Democrazia e società digitale. – 9. Fake news e disinformazione. – 10. Conclusioni.

## **1. Ordine (e disordine) nel diritto digitale**

Il titolo di questo scritto prende, volutamente, spunto da una formulazione, *l'ordine giuridico del mercato*, presentata diversi anni fa, la cui teorizzazione ha suscitato consensi e perplessità<sup>1</sup>: si affermava, tra l'altro, il luogo del mercato come statuto di norme, la cui decisione finale regolatoria spetta alla politica e quindi alla scelta legislativa, piuttosto che ai tribunali o alle dottrine giuridiche. Quella formula intendo qui trasferirla a uno tra i più rilevanti settori del mercato odierno, che è quello digitale. Dove però lo statuto di norme, inteso come strutturata regolazione e codificazione, appare quale metodo meno indicato per provare a dare un ordine giuridico: se non altro, quantomeno, a causa della tendenziale obsolescenza delle stesse norme, tenuto conto della rapidità con la quale si evolve e progredisce il digitale nella sua produzione industriale. Certo, ci dovrà pur essere un ordine giuridico che regola il sistema del digitale ma, a mio avviso, dovrebbe organizzarsi sulla base di norme di principio anziché di dettaglio, su norme a prevalenza promozionali anziché sanzionatorie. Come invece sembra essersi avviata l'Unione europea, attraverso una continua produzione di regolamenti, con i quali ha iniziato a normare il mercato e i

---

<sup>1</sup> N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, 1998, che ha dato luogo a un dibattito; AA.VV., *Il dibattito sull'ordine giuridico del mercato*, Roma-Bari, 1999.

servizi delle piattaforme digitali e financo a contenere l'espansione dell'intelligenza artificiale. Nell'illusione di volere "plasmare il futuro digitale dell'Europa", per dirla con uno *slogan* coniato dalla stessa UE, mentre invece rischia di determinare un disordine giuridico del mercato digitale, generato da un eccesso farraginoso di norme, che complicano il quadro regolatorio e rendono assai difficile l'applicazione delle stesse, sia da parte del cittadino-consumatore-utente delle piattaforme digitali, sia da parte delle aziende che operano nel settore della tecnologia industriale. Una prova di ciò è già verificabile nei regolamenti che sono stati varati dalla UE, che si distribuiscono per numerosi articoli e paragrafi<sup>2</sup>: si prenda, a esempio, il regolamento sull'intelligenza artificiale (d'ora in poi: IA), che si spalma su 89 "considerando", 85 articoli (di cui, almeno uno, il 4, di 44 paragrafi) e 9 allegati<sup>3</sup>. Non è facile districarsi nella boscaglia normativa nemmeno per l'intelligenza umana, anche quella di un giurista avvezzo alla interpretazione delle norme. Invece: un regolamento su una materia davvero strategica per la UE e non solo (posto che la IA si andrà a usare e applicare, da cittadini e imprese europee, in giro per il mondo, quindi oltre la perimetrazione normativa eurounitaria) dovrebbe, a mio avviso, essere sorretto da una disciplina normativa "sostenibile", con l'intento di riuscire a bilanciare interessi e concezioni diversificate, ponendosi quale primario obiettivo quello di non inibire la ricerca e lo sviluppo della IA, tenuto conto della sua importanza per la crescita economica e per l'implementazione della ricerca scientifica, a cominciare da quella medica, dove l'impatto della IA si sta rivelando determinante per la diagnosi e la terapia di una serie di patologie. La normativa europea dovrebbe essere altresì flessibile e adattabile ai cambiamenti; con l'obiettivo di creare e formare un diritto della IA *stable but not still*.

In tal modo, si potrà giungere a una sorta di ordine giuridico del digitale: ordine da intendersi non come comando piuttosto come precetto, che dispone di compiere (o di non compiere) un certo tipo di azioni. Pertanto, il problema va impostato e risolto sul terreno pratico dell'esperienza giuridica; si deve cioè esaminare, se si tratta o no di un fatto, che si verifica nel mondo delle azioni degli uomini in società, dove è dato constatare l'esistenza del diritto, quello costituzionale in particolare.

---

<sup>2</sup> Da ultimo: regolamento sul *Digital Market Act* 2022/1925/UE; regolamento sul *Digital Service Act* 2022/2065/UE. Su cui, specialmente sul primo, cfr. V. FALCE (a cura di), *Competition law enforcement in digital markets*, Torino, 2021.

<sup>3</sup> Su cui, v. il vol. C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale*, Padova, 2022.

## 2. Costituzionalismo e tecnologia

Del problema relativo all'ipertrofia normativa europea tratterò (anche) in questo scritto, dopo avere prima presentato e rappresentato la questione dell'ordine giuridico del digitale, sia pure costituzionalmente orientato<sup>4</sup>. Inizialmente, però, vorrei provare a mettere un punto fermo, oggettivo, sul sistema digitale e le sue applicazioni, tramite le piattaforme, nella società globale di oggi. Per fare ciò, è opportuno dare i numeri, per così dire, al fine di rendersi ben conto del problema, e quindi di ciò che siamo e di ciò che non vogliamo. Ebbene, con riferimento ai (più diffusi) *social network*, i numeri sono questi: iniziamo con *Facebook*, che ha 2,80 miliardi di utenti attivi mensili, 1,8 miliardi di utenti attivi giornalieri; il 59% degli utenti di internet, 58,5 minuti al giorno vengono trascorsi a “navigare” sul *social*; poi, *Whatsapp*, che ha 2 miliardi di utenti attivi mensili, ogni giorno vengono inviati più di 100 miliardi di messaggi, l'utente medio trascorre 38 minuti al giorno a mandare e leggere messaggi; infine, *Twitter*, che ha 353 milioni di utenti attivi al mese con un accesso quotidiano da parte di 187 milioni di persone, che trascorrono 158,2 minuti al mese usando la piattaforma per “cinguettare”<sup>5</sup>. È questa, piaccia oppure no, la società digitale, nella quale le nuove generazioni sono già perfettamente integrate. Si può davvero pensare di tornare indietro o pretendere di mettere un bavaglio a tutto ciò? Piuttosto bisogna lavorare per il futuro, ormai davvero prossimo, anche attraverso forme regolative del sistema digitale, che siano – insisto, ma lo dirò meglio appresso – elaborate attraverso principi e con norme promozionali anziché complesse, eccessivamente analitiche e sanzionatorie. Inoltre, con riferimento più nello specifico al diritto nella società digitale, si pensi anche a quanti atti e fatti giuridici si compiono attraverso i *social*, e più in generale nelle piattaforme digitali, in maniera davvero planetaria, senza confini e senza frontiere, potendo, per esempio, acquistare un appartamento a Miami, stando seduto in poltrona, davanti a un *personal computer* connesso a un *wi-fi*, nella propria abitazione nella piccola isola siciliana di Filicudi. E così pure quanti diritti costituzionali, ovvero dal “tono costituzionale”, si possono esercitare attraverso la rete internet: dal

---

<sup>4</sup>Ho anticipato la discussione su questi temi in. T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 2020, 465 ss.; v. ora, adesivamente, A. IANNOTTI DELLA VALLE, *Il Digital Markets Act e il ruolo dell'Unione Europea verso un costituzionalismo digitale*, in *Giur. cost.*, n. 3, 2022, 1867 ss.

<sup>5</sup>Si tratta di dati e statistiche facilmente reperibili sulle tante piattaforme digitali, attraverso i motori di ricerca, che non si ritiene necessario indicare una precisa fonte di riferimento.

diritto di manifestazione del pensiero al diritto di associazione e riunione, e altri ancora<sup>6</sup>.

Non torno qui su temi che mi sono cari, penso, fra gli altri, al diritto di accesso a internet, e sui quali pertanto rimando a quanto già scritto altrove<sup>7</sup>. Qui mi proverò ad ampliare l'orizzonte giuridico dell'internet, cercando di scrutare il paesaggio giuridico che si sta venendo a delineare nelle piattaforme digitali, soprattutto con l'avvento della IA<sup>8</sup>. Quale disciplina che studia *se e in che modo* si riproducono i processi mentali più complessi mediante l'uso di un *computer*, attraverso due percorsi complementari: da un lato la IA cerca di avvicinare il funzionamento dei *computer* alle capacità della intelligenza umana, dall'altro usa le simulazioni informatiche per fare ipotesi sui meccanismi utilizzati dalla mente umana. Da qui, la definizione, già utilizzata, del *computer* come *simia hominis*<sup>9</sup>.

La sfida che nel XXI secolo attende il costituzionalismo è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica e i suoi derivati in punto di diritto<sup>10</sup>. Si è parlato altresì di un «nuovo costituzionalismo, che porta in primo piano la materialità delle situazioni e dei bisogni, che individua nuove forme dei legami tra le persone e le proietta su una scala diversa da quelle che finora abbiamo conosciuto»<sup>11</sup>. Sebbene costituzionalismo non sia sinonimo di costituzione, perché quest'ultime possono essere, come ce ne sono, antitetici ai principi del costituzionalismo, bisogna comunque porsi un problema, che lo si può riassumere con la seguente domanda: da un punto di vista del diritto costituzionale, le tecnologie determinano nuove forme di diritti di libertà oppure possono essere incardinate e quindi riconosciute

<sup>6</sup> Su questi aspetti, rimando a T.E. FROSINI, *Apocalittici o integrati. La dimensione costituzionale della società digitale*, Modena, 2021.

<sup>7</sup> Del diritto di accesso a Internet me ne sono occupato già tredici anni fa: T.E. FROSINI, *Il diritto costituzionale di accesso a Internet*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Napoli, 2011, 23 ss. (ora in ID., *Liberté Egalité Internet*, 3<sup>a</sup> ed., Napoli, 2023).

<sup>8</sup> V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Dir. inf.*, 2000, 271 ss.; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. Inf.*, 2022, 5 ss.

<sup>9</sup> Cfr. V. FROSINI, *Cibernetica diritto e società*, Milano, 1968.

<sup>10</sup> Ragiona di un "costituzionalismo tecnologico", dopo quello liberale e democratico, P. COSTANZO, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in *Rass. parl.*, n. 4, 2012, spec. 852; di un "costituzionalismo digitale" scrive e argomenta M. BETZU, *I baroni del digitale*, Napoli, 2022, 92 ss.

<sup>11</sup> Così, S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 7.

nell'alveo delle tradizionali libertà costituzionali? Ovvero, è necessario riscrivere nuove norme costituzionali per definire le libertà che si sono venute a determinare a seguito dell'avvento della tecnologia, oppure si possono interpretare le vigenti norme costituzionali ricavandone da esse le nuove figure giuridiche dei nuovi diritti di libertà?

Non credo che sia da ritenersi ancora del tutto superato l'esercizio ermeneutico di volere applicare le libertà costituzionali statali ai fenomeni della tecnologia informatica<sup>12</sup>, anche al fine di evitare il rischio di finire in una sorta di *constitution-free zone*. Quindi, mantiene ancora oggi una sua validità rileggere la libertà di informazione, come diritto a essere informati oltretutto a informare, la libertà di comunicazione, la libertà di associazione, la libertà di riunione, la libertà di iniziativa economica privata, e le libertà politiche, alla luce degli sviluppi della tecnologia, al fine così di individuare le forme di tutela delle nuove situazioni giuridiche soggettive. Vi è stata, altresì, l'epifania di una nuova forma di libertà, che è stata concettualizzata in dottrina, fin dagli anni Ottanta, e che si è venuta a determinare con l'avvento della società tecnologica. Si tratta della dottrina della c.d. "libertà informatica", che soprattutto con internet è diventata una pretesa di libertà in senso attivo, non libertà *da* ma libertà *di*, che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di ogni genere<sup>13</sup>. Ci troviamo di fronte, indubbiamente, a una nuova forma di libertà, che è quella di comunicare con chi si vuole, diffondendo le proprie opinioni, i propri pensieri e i propri materiali, e la libertà di ricevere. Libertà di comunicare, quindi, come libertà di trasmettere e di ricevere. Non è più soltanto l'esercizio della libera manifestazione del pensiero dell'individuo, ma piuttosto la facoltà di questi di costituire un rapporto, di trasmettere e richiedere informazioni, di poter disporre senza limitazioni del nuovo potere di conoscenza conferito dalla telematica. Si viene così a dare piena attuazione all'art. 19 della Dichiarazione universale dei diritti dell'uomo dell'Onu, che così ha chiaramente precisato il diritto di libertà di manifestazione del pensiero: «cercare, ricevere, diffondere con qualunque mezzo di espressione, senza considerazione di frontiere, le informazioni e le idee». Formulazione perfetta, anche e soprattutto nell'era di Internet.

---

<sup>12</sup> Problema esaminato con tratti chiaroscuri da P. COSTANZO, *Il fattore tecnologico e il suo impatto sulle libertà fondamentali*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), *Diritti e libertà in internet*, Milano, 2017, 3 ss. e anche, da ultimo, M. BETZU, *op. cit.*, 15 ss.

<sup>13</sup> La dottrina della *libertà informatica* venne elaborata da V. FROSINI, *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI (a cura di), *Privacy e banche dei dati*, Bologna, 1981, 37 ss. (ora in ID., *Informatica diritto e società*, 2<sup>a</sup> ed., Milano, 1992, 173 ss.).

Allora, la libertà costituzionale di manifestazione del pensiero consiste oggi in quello che prevede e prescrive l'articolo 19 prima citato, anche quando l'informazione che viaggia *on line* su internet può agitare i governi nazionali, disturbare le relazioni diplomatiche fra Stati e, specialmente, svelare gli *arcana imperii*. Potrà non piacere, e soprattutto si potrà ridimensionare la portata e l'effetto e negarne la validità giuridica, ma resta il fatto che anche attraverso questa opera di *cercare, ricevere, diffondere* si viene a mettere al centro il diritto di sapere e la libertà di informare, che rappresenta altresì un nuovo modo di essere della separazione dei poteri, in una rinnovata concezione del costituzionalismo<sup>14</sup>. Una volta erano i governanti che controllavano i cittadini attraverso il controllo dell'informazione; ora è diventato più difficile controllare quello che il cittadino "legge-vedesente", "cerca-riceve-diffonde". Internet, allora, sta generando, come è stato scritto, «una coscienza costituzionalistica globale, animata dai *media* internazionali e dai *social networks* quali strutture critiche di una sfera pubblica sovranazionale, con effetti di "apertura" su contesti sociali bloccati e persino di catalizzazioni di rivoluzioni culturali e politiche»<sup>15</sup>.

Quali sono i (nuovi) diritti da prendere sul serio nel costituzionalismo della società tecnologica? Qui di seguito mi provo a fare un'elencazione con sintetiche riflessioni, in punto di attuazione e tutela. Non si vuole così fare l'apologia del costituzionalismo tecnologico ma piuttosto ripensare e rielaborare le categorie del costituzionalismo, per mettere "vino nuovo in otri nuovi". Declinare il costituzionalismo alla luce dei cambiamenti prodotti dall'erompere della tecnologia nelle nostre vite e nelle nostre comunità, in quella che è stata definita "la nuova civiltà digitale"<sup>16</sup>.

### 3. I nuovi diritti costituzionali nell'era di Internet. Il diritto di accesso

Le traiettorie del costituzionalismo tecnologico sono già emerse, diversi anni fa, in un paio di pronunce giurisprudenziali: in particolare, della Cor-

---

<sup>14</sup> Riprendo qui toni e termini già utilizzati in T.E. FROSINI, *Tecnologie e libertà costituzionali*, in *Dir. inf.*, 2000, 489 ss., che sono stati sottoposti a garbata ma netta critica da A. PACE, M. MANETTI, *Commento all'art. 21 Cost.*, in *Commentario della Costituzione*, fondato da G. Branca e continuato da A. Pizzorusso, Bologna-Roma, 2006, 160.

<sup>15</sup> Così, P. COSTANZO, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, cit., 839.

<sup>16</sup> Cfr. G. GHIDINI, D. MANCA, A. MASSOLO, *La nuova civiltà digitale. L'anima doppia della tecnologia*, Milano, 2020; da ultimo, V. CODELUPPI, *Mondo digitale*, Roma-Bari, 2022.

te Suprema Usa prima e del *Conseil Constitutionnel* francese poi<sup>17</sup>, che hanno riconosciuto e affermato il diritto di accesso a internet, da declinare quale libertà di espressione. È significativo che proprio nei due Paesi dove è sorto il costituzionalismo, seppure inizialmente muovendosi su due opposti sentieri, si registra un nuovo metodo interpretativo di ri-leggere e applicare due antiche norme – il I Emendamento della Costituzione Usa (1787) e l'art. 11 della Dichiarazione del 1789 – pensate, scritte e approvate più di due secoli fa per affermare e tutelare la libertà di informazione: quella di ieri, di oggi e di domani, è davvero il caso di dire. Infatti, da queste norme, da quei chiari e limpidi orizzonti del costituzionalismo, che si aprivano alla modernità, oggi si cerca e si trova il nucleo fondante costituzionale per riconoscere e garantire le nuove forme espressive di comunicazione elettronica, con particolare riguardo a internet. Si sta formando, grazie a un'accorta opera d'interpretazione costituzionale, un *diritto costituzionale di accesso a internet*: perché nel contesto di una diffusione generalizzata di internet, la libertà di comunicazione e di espressione presuppone necessariamente la libertà di accedere a tali servizi di comunicazione *on line*. Ed è compito degli Stati rimuovere gli ostacoli che impediscono di fatto l'esercizio di questo servizio universale a tutti i cittadini, che invece deve essere garantito attraverso investimenti statali, politiche sociali ed educative, scelte di spesa pubblica. Quindi, il diritto di accesso a internet, da intendersi come libertà informatica, è da considerarsi *una pretesa soggettiva a prestazioni pubbliche*<sup>18</sup>. Infatti: sempre di più l'accesso alla rete internet, e lo svolgimento su di essa di attività, costituisce il modo con il quale il soggetto si relaziona con i pubblici poteri, e quindi esercita i suoi diritti di cittadinanza. Anche perché, «lo sviluppo di Internet e la crescita dell'esigenza della trasparenza [amministrativa] rappresentano, nelle società occidentali, due fenomeni concomitanti»<sup>19</sup>.

Il diritto di accesso è strumentale all'esercizio di altri diritti e libertà costituzionali: non solo la libertà di manifestazione del pensiero, ma anche il diritto al pieno sviluppo della persona umana e all'effettiva partecipazione

---

<sup>17</sup> Per la giurisprudenza statunitense: *American Civil Liberties Union v. Reno* [E.D. Pa 1996], (tr. it. in *Dir. inf.*, n. 4/5, 1996); con sviluppi in Corte Suprema 521 US 844 (1997), (tr. it. in *Foro it.*, IV-2, 1998, 23 ss.). Per la giurisprudenza francese: *Conseil Constitutionnel* n. 2009-580 DC del 10 giugno 2009 (tr. it. in *Dir. inf.*, n. 3, 2009, 524 ss.).

<sup>18</sup> Per questa tesi, rinvio a T.E. FROSINI, *Liberté Egalité Internet*, cit., 60 ss.

<sup>19</sup> A. LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'internet*, Paris, 2002, 61; v. anche, nella dottrina latinoamericana, O.D. PULVIRENTI, *Derechos Humanos e Internet*, Buenos Aires, 2013.

di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese, o piuttosto la libertà di impresa. Oggi, nella società dell'informazione o, se si preferisce, nell'era dell'accesso<sup>20</sup>, non avere la possibilità di accedere a internet significa vedersi precluso l'esercizio della più parte dei diritti di cittadinanza, soprattutto nei rapporti con la pubblica amministrazione. Il diritto di accesso si declina sotto due diversi ma collegati profili: *a) diritto di accesso al contenuto*, e quindi come strumento necessario per la realizzazione della libertà di manifestazione del pensiero. Se questa libertà diciamo *on line* è esercitabile se e in quanto si accede alla Rete, l'accesso non è solo strumento indispensabile ma diventa momento indefettibile dell'esercizio della libertà, senza il quale essa verrebbe snaturata, cancellata; *b) il secondo profilo*, invece, si riferisce al *diritto di accesso a Internet quale diritto sociale*, o meglio *una pretesa soggettiva a prestazioni pubbliche*, al pari dell'istruzione, della sanità e della previdenza<sup>21</sup>. Ancora: il diritto di accesso, come è stato sostenuto, «si presenta ormai come sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete»<sup>22</sup>. Quindi, non tanto e non solo come diritto a essere tecnicamente connessi alla rete internet piuttosto come diverso modo d'essere della persona nel mondo e come effetto di una nuova e diversa distribuzione del potere sociale.

#### 4. Segue: il diritto alla libertà di espressione

Come è cambiato il senso e il significato della libertà di manifestazione del pensiero nell'era di internet? In maniera assai significativa, anche perché ha consentito il recupero della nozione di manifestazione del pensiero

<sup>20</sup>J. RIFKIN, *L'era dell'accesso*, tr. it., Milano, 2000.

<sup>21</sup>Da ultimo, riguardo al problema dell'accesso a Internet, e con riferimento alla situazione italiana, può essere utile citare qualche dato empirico. Secondo la Relazione del 2022 della Commissione europea sullo "Indice di digitalizzazione dell'economia e della società" (DESI), l'Italia è al 18° posto in Europa per quanto riguarda la connettività. Mentre il 19% della popolazione italiana non ha mai navigato sul *web*, un dato ben al di sotto della media UE, e il 46% della popolazione non possiede competenze digitali di base. Poi, per quanto riguarda i servizi pubblici digitali, l'Italia si posiziona al 19° posto tra gli Stati membri della UE, con uno scarso livello di interazione *online* fra le autorità pubbliche e l'utenza. Buono il risultato sui servizi di sanità digitale, che pone l'Italia all'ottavo posto nella UE. L'Italia non va meglio in termini di velocità di banda, un'altra variabile che ci porta in fondo alla classifica europea.

<sup>22</sup>Così, S. RODOTÀ, *Il diritto di avere diritti*, cit., 384. Sul diritto di accesso, rimando a T.E. FROSINI, *Liberté Egalité Internet*, cit., 49 ss.; ID., *Il diritto di accesso a internet*, in *Diritti e libertà in internet*, cit., 41 ss.

come libertà individuale, cioè senza “filtri”, ovvero senza mediazioni di sorta, davvero un *open network*. Infatti: basta creare un sito internet, ovvero entrare in un sito: senza vincoli amministrativi e con una diffusione planetaria, accessibile a tutti (a condizione di avere un *computer* o un *tablet* e una connessione), immediato nella esecuzione, in grado di racchiudere in sé audio, scritto e video, con uno spazio illimitato di memoria e con il pieno e vario utilizzo di strumenti automatici di reperimento di quel che si cerca. Quindi, con internet, chiunque può rendere pubbliche idee e opinioni attraverso la creazione e la gestione di un proprio *server*, ovvero attraverso l'apertura di un proprio sito *web*. In tal modo, ognuno può essere stampatore, direttore e editore di sé stesso, diffondendo notizie in rete senza appartenere ad alcun ordine professionale. Tutto un agire individuale, insomma; un uso concreto ed effettivo da parte di milioni di persone. Quindi, per dirla con la giurisprudenza statunitense: «[internet], la forma di comunicazione di massa più partecipativa che sia stata finora realizzata». Anche perché – grazie a internet – oggi tutti possono essere al tempo stesso comunicatori e diffusori. E questo lo sarà sempre più a partire dalla prossima generazione, che sta crescendo e formandosi alimentata da *Facebook*, *Twitter*, *You Tube*, *web communities*, *sms*, *skype*, *blogs* e continue evoluzioni. Questo determinerà una concezione assolutamente nuova e diversa dell'identità, che si articolerà in forma mutevole a seconda dei luoghi, dei contesti, degli interlocutori e delle scelte identitarie che si compiono. L'identità digitale, quindi, si articola sulla base di un flusso continuo di informazioni, che vanno nelle più diverse direzioni e che sono affidate a una molteplicità di soggetti, che costruisce, modifica e fa circolare immagini di identità altrui, o addirittura genera una seconda vita sulla rete, una *Second Life* virtuale<sup>23</sup>. Insomma, una situazione di sicuro progresso in termini di libertà individuale ma anche di iniziativa economica privata. È stato argutamente detto, che «solo chi è rimasto alla preistoria del diritto e si aggira ancora armato di clava cercando di inventare la ruota, non si rende conto del passaggio epocale che si è verificato nelle società evolute in questi anni: la possibilità di accedere sempre, dovunque a tutta la conoscenza racchiusa in testi digitali; la possibilità di comunicare sempre dovunque e a costi minimi con tutti; la possibilità di diffondere sempre e dovunque a tutto il mondo il proprio pensiero. E solo i cavernicoli non si accorgono del circuito inarrestabile fra accesso alle fonti di conoscenza, creazione di forme di scambio di esperienze, diffusione di nuove idee, e creazione di nuova co-

---

<sup>23</sup> Sul punto, v. E. BASSOLI, *La disciplina giuridica della seconda vita in Internet: l'esperienza Second Life*, in *Inf. dir.*, n. 1, 2009, 165 ss.

noscenza»<sup>24</sup>. Certo, non è mera apologia della libertà di espressione in internet; si è ben consapevoli anche degli effetti distorsivi che può produrre l'informazione tramite i *social media*, i quali «possono anche essere uno strumento a favore della democrazia, ma il fatto che siano nelle mani di un numero troppo ristretto di soggetti fa sì che questi, per la loro posizione siano portati a dominare “how public opinion is organized and governed”»<sup>25</sup>. Questo problema evoca il tema della posizione dominante e dipendenza economica delle aziende dell'internet, c.d. “baroni del digitale” e definiti con l'acronimo (GAFAM: *Google, Amazon, Facebook, Apple e Microsoft*), e riconduce al tema del diritto costituzionale della concorrenza<sup>26</sup> e alla sua corretta applicazione nel mercato delle piattaforme digitali. Di sicuro interesse è, tra l'altro, il caso di Google e la sua capacità di raccogliere e utilizzare i dati dei suoi utenti per il tramite dei numerosi servizi che essa stessa, quale piattaforma digitale, mette a disposizione: dalla posta elettronica alle mappe *online*, dal suo motore di ricerca sul *web* alla gestione dei pagamenti *online* e molto altro ancora. Sviluppando ed esercitando, in tal modo, quella che è stata definita una “sovranità.com”<sup>27</sup>.

## 5. Segue: Il diritto alla privacy

Un altro diritto da prendere sul serio, nel costituzionalismo della società tecnologica, è quello della *privacy*. Un diritto che nasce come una nuova esigenza di libertà personale, laddove si invocava «il diritto di godere della vita, ovvero il diritto di starsene soli (*right to be let alone*)»: un diritto individuale di libertà da esercitare e tutelare specialmente nei confronti delle intrusioni, allora, della stampa nel riportare in pubblico fatti o elementi strettamente personali, la cui conoscenza avrebbe comportato disdoro e imbarazzo nella persona interessata. Non si chiedeva però di esaltare la difesa della solitudine fisica, ma piuttosto di ricondurre la *privacy* alla tutela

---

<sup>24</sup> V. ZENO ZENCOVICH, *Perché occorre rifondare il significato della libertà di manifestazione del pensiero*, in *Percorsi Cost.*, n. 1, 2010, 71.

<sup>25</sup> Così M. BETZU, *I baroni del digitale*, cit., 34.

<sup>26</sup> In tema, v. M. MANETTI, *I fondamenti costituzionali della concorrenza*, in *Quad. cost.*, n. 2, 2019; A. IANNOTTI DELLA VALLE, *La tutela della concorrenza ai tempi di Google Android tra fondamenti costituzionali e analisi tecnologica*, in *Dir. inf.*, 2021, 283 ss. In giurisprudenza, v. la sent. Tribunale della UE, IX sez. ampliata, del 10 novembre 2021, causa T-612/17, che ha riconosciuto il ruolo “superdominante” di Google e il suo carattere anticoncorrenziale.

<sup>27</sup> S. MANNONI e G. STAZI, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli, 2021.

dei valori di autonomia e dignità dell'individuo, che comprendono anche la protezione della sua cerchia familiare e persino di quella societaria, in cui egli ha scelto di collocarsi.

La concezione della *privacy* si è evoluta nel tempo, non più e non tanto come “diritto a essere lasciati soli”, e quindi una forma passiva di tutela, ma piuttosto anche come “diritto a disporre dei propri dati”, assumendo pertanto una forma attiva di partecipazione informativa<sup>28</sup>. Infatti, e soprattutto con l'avvento dei *computer* prima e di internet dopo, la problematica riguarda non tanto il controllo delle informazioni individuali in difesa di un diritto del soggetto alla riservatezza, quanto piuttosto il metodo adottato per la raccolta dei dati, ossia la possibilità di raccogliere le informazioni in una “banca dati” elettronica. Da qui, la nuova esigenza di tutelare la riservatezza dei dati personali, ovvero di impedire che notizie riguardanti la sfera intima della persona possano essere divulgate e conosciute da terzi, con il rischio che questo possa procurare forme di discriminazione. Si pensi ai dati sanitari o sessuali, e quindi alla possibilità che la conoscenza di questi possa consentire un trattamento discriminatorio nei confronti di chi è affetto da una certa malattia oppure le cui scelte sessuali sono diversificate. Certo, bisogna rivedere il concetto e la concezione stessa di *privacy*, che va tutelata davvero e solo quando serve. Alcuni nostri dati sono per loro natura pubblici, anche perché siamo noi stessi che li immettiamo sulla rete, e allora occorre concentrare il controllo e la tutela solo su quelli veramente rilevanti, cioè sensibilissimi.

Il diritto alla *privacy* oggi ha una sua particolare conformazione e codificazione a livello europeo (regolamento UE 2016/679: *General Data Protection Regulation*), proprio con riferimento alle esigenze di tutela che possono prodursi attraverso la rete internet. Mi provo a fare degli esempi su *provider* o motori di ricerca a tutti noti: *Amazon* monitora le nostre preferenze d'acquisto; *Google* registra le nostre abitudini in rete; *Facebook* conosce le nostre relazioni sociali e ciò che *like*; gli operatori di telefonia mobile sanno non solo con chi parliamo, ma anche chi si trova nelle vicinanze. Lasciamo impronte elettroniche ovunque: da queste, infatti, si può risalire per sapere cosa abbiamo acquistato, in quale località siamo stati, dove e cosa abbiamo mangiato e così via.

Sul diritto alla *privacy*, quindi, c'è un prima e un dopo. Il confine è segnato dall'avvento di internet, databile a partire dal secolo Ventunesimo<sup>29</sup>.

---

<sup>28</sup> In tema di diritto alla *privacy*, con riferimento alle problematiche presenti e future, cfr. T.E. FROSINI, *Le sfide attuali del diritto ai dati personali*, in S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, 25 ss.

<sup>29</sup> Fra i primi a porre la questione giuridica di internet, v. P. COSTANZO, *Internet (diritto pubblico)*, in *Dig. disc. pubbl.*, 4<sup>a</sup> ed., agg. Torino, 2000.

Perché un conto sono i dati personali raccolti e custoditi in apposite banche dati, di cui però c'è, almeno formalmente, un responsabile della gestione delle stesse, sebbene il problema sia quello del flusso dei dati da una banca all'altra, un conto è internet e la sua capacità di diffondere, subito e in tutto il mondo, dati che si riferiscono a una singola persona ovvero a imprese pubbliche e private. È chiaro che internet consente un flusso sterminato di dati il cui controllo appare difficile regolare. La questione oggi è resa più complessa con i c.d. *big data*<sup>30</sup>: si tratta dell'accumulo enorme di dati, tale da inondare il mondo di informazioni come mai prima d'ora, con una continua e irrefrenabile crescita. Il cambiamento di dimensione ha prodotto un cambiamento di stato. Il cambiamento quantitativo ha prodotto un cambiamento qualitativo. Pertanto, si tratta delle cose che si possono fare solo su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi, e altro ancora. Si viene a materializzare un percorso digitale che le grandi (e poche) aziende di internet, possono analizzare per capire le preferenze degli utenti ed elaborare un'identità digitale da utilizzare a scopi commerciali o politici.

È nota la vicenda che ha coinvolto *Facebook* per avere ceduto a una società di ricerche, *Cambridge Analytica*, i dati dei suoi utenti per consentire un trattamento finalizzato a individuare categorie di elettori. Questo dipenderebbe dai *like* che mettiamo sui *social*, come per esempio *Facebook* o *Twitter*. Perché ogni *like* che lasciamo sui *social* sarebbe un tassello in una sorta di auto-schedatura volontaria di massa, che finirebbe con offrire opportunità e poteri a chi vuole orientare le opinioni. Studi condotti da psicologi, peraltro, sostengono che bastano sessantotto *like* di un utente *Facebook* per individuare il colore della sua pelle (con precisione pari al 95%), l'orientamento sessuale (88%) e quello politico (85%). Quindi, le opinioni politiche sono conosciute da *Facebook*; quindi, il voto potrebbe non essere più segreto, libero e personale. È chiaro che questo aspetto va a colpire un diritto costituzionale quale quello del diritto di voto. E va altresì a colpire la riservatezza del cittadino laddove si individua la sua scelta politica, che è un dato sensibile che dovrebbe essere tutelato al massimo livello<sup>31</sup>. È una nuova forma di potere, quello dei *provider* di assecondare i gusti di ciascuno sulla base di ciò che fanno di noi.

---

<sup>30</sup> Da ultimo, V. ZENO ZENCOVICH, *Big data e epistemologia giuridica* e A. STAZI, *Legal big data: prospettive applicative in ottica comparatistica*, entrambi nel vol. *Dati e algoritmi. Diritto e diritti nella società digitale*, cit., 13 ss. e 77 ss.

<sup>31</sup> Sulla questione, v. T.E. FROSINI, *Internet e democrazia*, in *Dir. Inf.*, n. 4/5, 2017 (ora in ID., *Liberté Egalité Internet*, cit., 211 ss.).

Ancora, e sempre in tema di diritto alla *privacy* e internet. Si pensi ai recenti scandali internazionali, che sono stati sollevati con riferimento alla capacità di uno Stato di gestire i dati personali di migliaia di persone influenti, che appartengono e rappresentano le istituzioni europee. Ovvero l'indisponibilità personale dei dati che viaggiano sul *cloud computing*, laddove tutto il nostro patrimonio informativo finisce per essere sottratto alla nostra indisponibilità e per risiedere in *server* posti al di fuori del nostro controllo diretto, e quindi potenzialmente esposti a violare la nostra *privacy*. Il problema, peraltro, riguarda non solo dati personali, ma soprattutto grandi banche dati di operatori telefonici, imprese, istituti di credito e di risparmio, che hanno un indubbio valore strategico.

## 6. Segue: il diritto all'oblio

Il costituzionalismo nella società tecnologica deve altresì confrontarsi con un'altra situazione giuridica che si manifesta in internet: quella del diritto all'oblio (*right to be forgotten*). Da intendersi quale reviviscenza del vecchio diritto a essere lasciati soli (*right to be alone*), ovvero come «pretesa a riappropriarsi della propria storia personale»<sup>32</sup>, e quindi una sorta di diritto all'autodeterminazione informativa, altrimenti come mezzo per ricostruire la dimensione sociale dell'individuo, evitando che la vita passata possa costituire un ostacolo per la vita presente<sup>33</sup>. Per salvaguardare il diritto del soggetto al riconoscimento e godimento della propria attuale identità personale o morale, attraverso il diritto di vietare un travisamento dell'immagine sociale di un soggetto, ovvero della propria personalità individuale, per evitare che si venga a diffondere *false light in the public eye*. Quindi, un diritto a governare la propria memoria.

Diritto all'oblio e diritto alla *privacy* possono ben rappresentare due facce di una stessa medaglia, che affondano nella dignità della persona la loro rilevanza costituzionale. Il diritto all'oblio, generato dalla giurisprudenza e consolidato dalla legislazione, ha dovuto fare i conti con internet, la "rete delle reti", dove tutto ciò che è stato inserito nel *web* rimane come una memoria illimitata e senza tempo, ovvero un deposito di dati di dimensioni globali.

---

<sup>32</sup>C. CHIOLA, *Appunti sul c.d. diritto all'oblio e la tutela dei dati personali*, in *Percorsi Cost.*, n. 1, 2010, 39.

<sup>33</sup>Maggiori dettagli in T.E. FROSINI, *La tutela dei dati e il diritto all'oblio*, in *Rass. parl.*, n. 4, 2018, 497 ss.

Certo, la notizia apparsa sul *web* non dura, al pari delle notizie sulla carta stampata, come la rosa del poeta Pierre de Ronsard, *l'espace d'un matin*, ma piuttosto assume forma durevole e incancellabile; chiunque la può leggere e rileggere, ovunque si trova nel mondo, e può utilizzarla come fonte di informazione. Ma la notizia non è un dato astratto alla *mercé* di tutti, perché riguarda la persona e la sua immagine in un dato momento storico; i dati personali, vale la pena ricordarlo, costituiscono una parte della espressione della personalità dell'individuo. Come ancora di recente, ha sostenuto la Corte di giustizia UE nella decisione c.d. *Google Spain* (2014) e poi ha ribadito e confermato nella sentenza sul caso *Safe Harbour*, o altrimenti c.d. *Schrems* (2015)<sup>34</sup>. Certo, si tratta di pronunce giurisdizionali che non si limitano solo ad affermare il diritto all'oblio ma anche, fra le altre questioni, il diritto alla *privacy* da applicare secondo il diritto europeo, anche nei confronti del mercato transnazionale dei dati, specie con gli Usa. Va senz'altro ricordata, inoltre, la pronuncia della Corte di Giustizia UE (causa C-507/17), sempre in materia di diritto all'oblio e nota come *Google vs. CNIL (Commission nationale de l'informatique et des libertés)*, dove si può riscontrare una sorta di passo indietro nella tutela del diritto all'oblio e un passo in avanti per il motore di ricerca Google. Viene, infatti, a essere delimitato territorialmente il diritto all'oblio, circoscrivendo l'obbligo di deindicizzazione alle sole versioni del motore di ricerca corrispondenti a tutti gli Stati membri dell'Unione europea, senza che la deindicizzazione avvenga in tutte le versioni del motore di ricerca a livello globale<sup>35</sup>. Ultima, per adesso, è la sentenza sempre della CGUE (causa C-18/18) riguardante *Facebook*, relativa alla pubblicazione su una pagina personale di foto e commenti ritenuti lesivi del diritto della personalità, che merita di essere qui quantomeno segnalata, anche perché presenta significativi rilievi in punto di riservatezza e diritto all'oblio<sup>36</sup>.

Un cenno, infine, alla codificazione del diritto all'oblio nel regolamento

---

<sup>34</sup> Sulle sentenze della Corte UE, v. i fascicoli monografici di *Dir. inf.*, n. 4/5, 2014 (sul caso *Google Spain*) e *Dir. inf.*, n. 4/5, 2015 (sul caso *Safe Harbour*), entrambi ospitano una raccolta di contributi che analizzano le varie problematiche derivanti dalle pronunce giurisdizionali. Con riferimento alla prima sentenza, cfr. A. RALLO, *El derecho al olvido en Internet. Google versus Espana*, Madrid, 2014.

<sup>35</sup> Sulla questione della c.d. territorialità dell'oblio, v. ora G. BEVILACQUA, *La dimensione territoriale dell'oblio in uno spazio globale e universale*, in *Federalismi*, n. 23, 2019.

<sup>36</sup> Con riferimento alla sentenza *Facebook*, ma anche alla precedente, v. O. POLLICINO, *L'“autunno caldo” della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi*, n. 19, 2019.

UE 2016/679 (*General Data Protection Regulation: GDPR*). All'art. 17 è prevista la possibilità di richiedere la cancellazione dei dati esercitando così il diritto all'oblio: nei casi in cui i dati personali non siano più necessari rispetto alla finalità per cui erano stati originariamente trattati, ovvero nel caso in cui siano stati trattati illecitamente, oppure quando l'interessato abbia revocato il consenso o si sia opposto al loro trattamento. Vi è anche l'ipotesi in cui la cancellazione costituisca un obbligo giuridico che proviene dal diritto UE ovvero degli Stati membri. Sono previsti casi in cui il titolare del trattamento può opporre rifiuto alla cancellazione, come nel caso del rispetto all'esercizio del diritto alla libertà di espressione e di informazione<sup>37</sup>. Certo, la regolamentazione europea è una significativa affermazione del diritto all'oblio, che da creazione giurisprudenziale transita alla codificazione normativa: quasi una sorta di passaggio dal *common law* al *civil law*.

Una breve riflessione conclusiva sul diritto all'oblio, al di là delle oscillanti decisioni giurisprudenziali e della normazione ancora da "rodare" in punto di effettività. Deve essere consentito alla persona, a tutela della sua identità, di esercitare il proprio diritto di libertà informatica, che consiste nel potere disporre dei propri dati, ovvero delle notizie che lo riguardano, e quindi chiedere per ottenere sia il diritto all'*oblio* su ciò che non è più parte della sua identità personale, sia il diritto alla *contestualizzazione* del dato, e quindi della notizia, perché una verità non aggiornata non è una verità. Allora, è tra i principi fondamentali che va cercato il punto archimedeo del diritto all'oblio e i suoi derivati: in particolare, nella formula costituzionale non negoziabile della dignità dell'uomo, codificata e resa intangibile nelle costituzioni di democrazia liberale (nella Legge Fondamentale tedesca all'art. 1). È il principio fondamentale della dignità, infatti, che costituisce il fondamento costituzionale di tutti i diritti strettamente connessi allo sviluppo della persona: le particolari declinazioni della personalità umana, seppure siano autonomamente giustiziabili, sono riconducibili alla più generale espressione di dignità umana. Non vi può essere tutela dell'identità personale senza tutela della dignità, che si traduce nel diritto del singolo a vedere, comunque, rispettata la propria reputazione, il proprio buon nome, a non essere discriminato a causa dei propri orientamenti e dei propri stili di vita. È nella *privacy-dignity* che acquista rilievo il rispetto dell'identità di ogni persona, che non può e non deve essere trattata come se fosse un oggetto. La tutela della dignità dell'uomo passa (anche) attraverso il diritto all'oblio, ovvero il diritto a cancellare, ovvero a contestua-

---

<sup>37</sup> Per una prima analisi, v. S. ZANINI, *Il diritto all'oblio nel regolamento europeo 679/2016: quid novi?*, in *Federalismi.it*, n. 15, 2018.

lizzare, i dati personali per vietare, come già detto, un travisamento dell'immagine sociale di un soggetto, per evitare che la vita passata possa costituire un ostacolo per la vita presente e possa ledere la propria dignità umana<sup>38</sup>.

## 7. Il diritto nell'intelligenza artificiale

Le nuove frontiere del diritto e dei diritti oggi sono rappresentate dalle potenzialità della intelligenza artificiale (IA), ovvero dalla enorme capacità di raccogliere, sistematizzare ed elaborare dati per produrre algoritmi in grado di trovare soluzioni “intelligenti” per risolvere problemi, oppure per assumere decisioni autonomamente e imparzialmente<sup>39</sup>. Dati che riguardano persone, ma anche beni, servizi, merci, capacità produttive, che possono essere scambiati, creando così un vero e proprio mercato dei dati<sup>40</sup>. E possono essere soprattutto elaborati, in tal modo finiscono con il creare situazioni ambientali, apprendere elementi conoscitivi e risolvere soluzioni a problemi, in maniera velocissima, che le capacità intellettive umane non riuscirebbero a fare altrettanto.

La IA impatta su tutte le scienze del sapere umano declinandole artificialmente. Anche il diritto, che dovrà sempre più rimodularsi nei suoi paradigmi, tenendo conto dell'uso degli algoritmi per concorrere a migliorare le pronunce giurisdizionali ovvero per elaborare neutrali atti amministrativi, per citare solo alcuni esempi<sup>41</sup>. Certo, il diritto già da tempo è entrato nella società tecnologica – ovvero cibernetica, come veniva chiamata e come ora viene opportunamente riproposta<sup>42</sup> – con tutti i suoi temi e pro-

---

<sup>38</sup> Cfr. T.E. FROSINI, *Liberté Egalité Internet*, cit., 103 ss.

<sup>39</sup> Assai numerosa è la produzione di libri e articoli dedicati alla IA, qui mi limito a citare un recente volume che inquadra il tema svelando luci e ombre: K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro della IA*, tr.it., Bologna, 2021.

<sup>40</sup> T. RAMGE e V. MAYER-SCHÖNBERGER, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, tr.it., Milano 2021.

<sup>41</sup> Per un quadro d'insieme, si v. il volume A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano 2020; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, cit.

<sup>42</sup> Ripropone l'uso del termine “cibernetica”, sottolineando l'affinità fra questa e il diritto, perché «entrambi mirano a studiare e a rendere prevedibili i modelli di comunicazione e controllo dei comportamenti collettivi»: così, A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 171.

blemi derivanti dall'applicazione delle tecniche giuridiche, sostanziali e processuali, nel vasto mondo della tecnologia e suoi derivati, in particolare la rete Internet. Pertanto, si potrebbe riformulare l'antico brocardo latino con *ubi societas tecnologica, ibi ius*. Emergono, infatti, dalla coscienza sociale, e a seguito dello sviluppo tecnologico, dei "nuovi diritti", i quali, sebbene non godano di un loro esplicito riconoscimento normativo, hanno un forte e chiaro "tono costituzionale", che li collocano, implicitamente, all'interno della costituzione, riservando all'interprete il compito di estrapolarli da essa, anche attraverso quella che ho chiamato una "interpretazione tecnologicamente orientata"<sup>43</sup>. Purtroppo bisogna essere consapevoli dei rischi di presunti vizi di incostituzionalità delle leggi, che prevedono e prescrivono l'uso della IA, eventualmente riferibili alla c.d. "discriminazione algoritmica". La quale determinerebbe un algoritmo strutturalmente incostituzionale, uno scenario cioè paragonabile alla fallacia naturalistica di Hume, con riferimento al giusnaturalismo: l'errore di derivare dall'essere (della realtà sociale, spesso ingiusta o distorta) il dover essere<sup>44</sup>. Come è stato scritto, «la vera frontiera è la sua sindacabilità. Dunque all'algoritmo deve essere possibile fare accesso, deve essere conoscibile, deve essere sindacabile per controllare sulla base di quali dati, di quali informazioni, di quale presentazione del problema è stato avviato il suo funzionamento»<sup>45</sup>. Da qui, allora, l'esigenza di elaborare una dottrina della "precauzione costituzionale", ispirata alle situazioni ambientali e così delineata: «la condizione di incertezza a riguardo dei possibili effetti negativi dell'impiego della tecnologia (inclusa l'intelligenza artificiale) non può essere utilizzata come una ragione legittima per non regolare e limitare tale sviluppo»<sup>46</sup>. Pertanto, la protezione dei beni costituzionali deve essere anticipata rispetto alla produzione stessa delle applicazioni tecnologiche. Il parametro per giudicare i fenomeni della IA è la costituzione, e più in generale il costituzionalismo, specie nella parte in cui prevede e tutela la pari dignità della persona umana (art. 3 Cost. it., art. 1 Carta dei diritti UE)<sup>47</sup>.

Tutto vero, tutto giusto. Si avverte però l'impressione, che la preoccupu-

---

<sup>43</sup> T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, cit., 465 ss.; v. anche C. CASO-NATO, *Per una intelligenza artificiale costituzionalmente orientata*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 131 ss.

<sup>44</sup> Sul punto, A. SIMONCINI, *op. cit.*, 196.

<sup>45</sup> Così B. CARAVITA DI TORITTO, *Principi costituzionali e intelligenza artificiale*, n ID., *Letture di diritto costituzionale*, Torino, 2020.

<sup>46</sup> A. SIMONCINI, *op. cit.*, 199.

<sup>47</sup> B. CARAVITA DI TORITTO, *op. cit.*

pazione dei rischi di una possibile incostituzionalità dell'algoritmo siano derivati dal volere leggere i problemi con gli occhiali del giurista domestico. La questione non è nazionale ma mondiale, anche perché la IA è già operativa in diversi Paesi dove è radicato il costituzionalismo e dove la dignità umana gode di sicura tutela. Quindi, il problema laddove emergesse verrebbe risolto attraverso le consolidate procedure di garanzie costituzionali diffuse negli stati di democrazia liberale, che funzionano da anticorpi per qualunque violazione costituzionale, soprattutto di leggi liberticide figuriamoci di leggi che non esplicitano la conoscibilità e quindi il corretto funzionamento degli algoritmi. E comunque, anche a volere osservare la questione nella dimensione nazionale, si possono ricordare le note pronunce del Consiglio di Stato (sent. n. 2270/2019 e n. 8472, 8473, 8474/2019), che hanno giustamente messo in rilievo come l'algoritmo è una regola costruita dall'uomo per disciplinare le operazioni di calcolo effettuate dal *software*, che sarà comunque soggetto a valutazione da parte del giudice per verificarne la correttezza del processo automatizzato in tutte le sue componenti<sup>48</sup>.

Si è già iniziato a parlare di "algocrazia", ovvero di "dittatura dell'algoritmo"<sup>49</sup>. Posso comprendere il tono accattivante e provocatorio di queste definizioni ma mi sembrano esagerate, ovvero poco rispondenti alla realtà. E comunque, l'algoritmo, se lo si teme, lo si può circoscrivere nel suo uso, purché non lo si comprima e lo si sterilizzi. Peraltro, lo si può normare anche con leggi statali, come è stato fatto, per esempio, in Francia e, a livello statale, negli Usa<sup>50</sup>. E come si accinge a fare la UE, seppure in un contesto normativo che suscita però dubbi e perplessità applicative, come dirò più avanti. Sulla questione, vale qui ricordare l'art. 22, par. 1, GDPR, che recita: «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida

---

<sup>48</sup> Su questi temi e problemi, v. F. DONATI, *Intelligenza artificiale e giustizia*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 248 ss. V. anche numerosi spunti in S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi giuridica dell'economia*, n. 1, 2019.

<sup>49</sup> Per il primo termine, v. M. AINIS, *Il regno dell'uroboro. Benvenuti nell'era della solitudine di massa*, Milano, 2018, 19 ss.; per il secondo, S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2015, 33.

<sup>50</sup> Per la Francia, v. la *loi n. 2016-1321 du 7 octobre pour une République numérique* (con modifiche nel 2019), per gli Usa, v. la legge n. 49/2018 di NYC: *A Local Law in relation to automated decision systems used by agencies*, cfr. S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, cit., 109 ss.

in modo analogo significativamente sulla sua persona» (salvo prevedere delle deroghe: per la stipula di un contratto o sul consenso esplicito dell'interessato). Mi sembra che si tratti di una norma che funga da freno a possibili invasioni e predominanze dell'algoritmo sulle scelte che deve compiere l'uomo.

Dell'algoritmo, e più in generale della IA, bisogna cercare di avvalersi dei benefici, minimizzando i rischi e le criticità che indubbiamente ci sono: non bisogna però dimenticare che i sistemi di IA saranno il volano dello sviluppo mondiale di questo secolo, economico e scientifico. Allora, come è stato scritto in maniera condivisibile: «la *AI revolution* ha bisogno di essere accompagnata e “corretta” da un pensiero costituzionale, deve produrre una risposta in termini di concettualizzazione dei diritti e principi, allo stesso modo di come la rivoluzione industriale ha prodotto la evoluzione welfarista degli Stati liberali nel XIX secolo e il costituzionalismo sociale del XX secolo»<sup>51</sup>. Voglio aggiungere una cosa, che mi limito solo ad accennare: il *favor* per la IA e le sue benefiche applicazioni a vantaggio dell'umanità, esprime, oggi, una rinnovata concezione del liberalismo, dove, cioè, si pone come prioritaria la libertà per il progresso e verso nuove forme di sviluppo dell'individuo e del benessere delle società. La posizione di chi auspica e pretende forme regolative della IA, in forma pervasiva e dettagliata, è, oggi, riconducibile a nuove forme di statalismo, che si manifestano nella volontà di fondare e stabilire una nuova sovranità degli stati sulle piattaforme digitali.

## 8. Democrazia e società digitale

Il complesso e complicato rapporto fra internet, ovvero ciò che si manifesta attraverso la Rete e in particolare i c.d. *social*, e la democrazia, ovvero il modo e il metodo con il quale si organizza la società contemporanea, è ormai il tema che suscita larga attenzione e riflessione da parte degli studiosi delle scienze sociali. Divisi tra coloro che sostengono come e perché internet può rafforzare la democrazia e gli oppositori, che vedono in internet una minaccia per la tenuta democratica degli Stati<sup>52</sup>. Altrimenti, c'è

---

<sup>51</sup> Così, A. D'ALOIA, *Il diritto verso “il mondo nuovo”*. *Le sfide dell'Intelligenza Artificiale*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, cit., 33.

<sup>52</sup> Su queste questioni, v. S. COLEMAN, *Can The Internet Strengthen Democracy?*, Cambridge, 2017; v. altresì, da ultimo, P. COSTANZO, *La democrazia digitale (precauzioni per l'uso)*, in *Dir. pubbl.*, n. 1, 2019, 71 ss.

stato chi, addirittura, ha imputato a internet la responsabilità di avere destabilizzato il sistema rappresentativo e avere favorito l'avvento del populismo (digitale)<sup>53</sup>. Piaccia oppure no, siamo in presenza di una nuova forma di democrazia, che ha già ricevuto diverse denominazioni: democrazia “elettronica” (ma questo termine definisce lo strumento e non l'agente); “virtuale” (ma in tal modo l'indicazione politica ne risulta indebolita); “continua” (per il suo carattere di *referendum* perenne); ovvero ancora “nuova democrazia di massa” (con riferimento all'antica democrazia diretta)<sup>54</sup>. La questione di fondo può essere così formulata: l'impatto politico delle tecnologie informatiche su quei fragili sistemi complessi che sono le democrazie contemporanee favorirebbe la costruzione di una *agorà* o di un totalitarismo elettronici? La dialettica dei giudizi sulla nuova forma di democrazia è però fondata su un presupposto comune di discussione: il superamento, o piuttosto l'aggiornamento dell'attuale democrazia di tipo rappresentativo-parlamentare<sup>55</sup>.

Personalmente, ritengo che con Internet possa cogliersi un'opportunità per migliorare le forme della democrazia, specialmente in termini di partecipazione politica<sup>56</sup>. Certo, non credo però che questo approccio debba passare attraverso modi di esaltazione acritici e pertanto ignorare alcuni dubbi applicativi di Internet su alcune procedure di funzionamento della democrazia. Sul punto, si può ricorrere a corsi e ricorsi storici. Ieri era il video potere, che rischiava di minare le fondamenta della democrazia, secondo un'opinione che all'epoca si era diffusa, oggi le stesse critiche e riserve vengono rivolte al c.d. *internet power*. Credo, infatti, che anche il timore di una possibile “dittatura del *web*” sia eccessiva, e che si riduca,

---

<sup>53</sup> Da ultimo, M. BARBERIS, *Come internet sta uccidendo la democrazia*, Milano, 2020, 137, il quale, tra l'altro, afferma: «internet moltiplica i pregiudizi sino al parossismo, ma la rivoluzione digitale è la causa principale, benché non l'unica, del populismo odierno». Anche M. BETZU, *I baroni del digitale*, cit., 27, individua «forme di populismo digitale particolarmente pericolose per la stabilità della democrazia rappresentativa».

<sup>54</sup> Per le varie definizioni citate nel testo, v. nell'ordine i seguenti studi: L.K. GROSSMAN, *The Electronic Republic. Reshaping Democracy in the Information Age*, New York, 1995; L. SCHEER, *La democrazia virtuale*, tr.it., Genova, 1997; AA.VV., *La démocratie continue*, sous la direction de D. ROUSSEAU, Paris-Bruxelles, 1995; V. FROSINI, *La democrazia nel XXI secolo* [1997], nuova ed. con prefaz. di A. Jellamo e postfaz. di F. Riccobono, Macerata, 2010.

<sup>55</sup> V. I. BUDGE, *The new Challenge of Direct Democracy*, Cambridge, 1996. Con considerazioni in chiaroscuro, M. AINIS, *Democrazia digitale*, in *Rass. parl.*, n. 2, 2013, 263 ss. Da ultimo, i contributi di M. MONTI, *Le Internet platforms, il discorso pubblico e la democrazia*, in *Quad. cost.*, n. 4, 2019, 811 ss.; A. VENANZONI, *La matrice spezzata: ripensare la democrazia all'epoca di Internet*, in *Quad. cost.*, n. 1, 2020, 61 ss.

<sup>56</sup> Ho argomentato questa mia posizione in T.E. FROSINI, *Internet e democrazia*, cit.

come nel caso della televisione, in una paura poco fondata. E che semmai la politica, o più in generale le forme applicative delle procedure democratiche, potrebbe invece uscirne rafforzata, rinvigorita, rilanciata.

La rivoluzione tecnologica ha operato incisivamente sull'organizzazione politica della società occidentale, e ancora di più lo farà negli anni a venire. Ha creato le condizioni perché si venisse a formare una nuova democrazia di massa, come è stata chiaramente definita<sup>57</sup>, distinta e distante dai regimi di massa della prima metà del Novecento, in cui l'individuo singolo rimaneva in una soggezione psicologica recettiva e passiva con un totale obnubilamento delle libertà personali. Quelle stesse libertà che invece si esaltano e valorizzano nella nuova democrazia di massa. Che «non è tuttavia una destinazione fatale e irreversibile della società odierna. Essa è soltanto una direttiva di marcia dell'umanità, segnata dall'impronta della civiltà tecnologica che le imprime il procedimento. [...] In essa si realizza con apparente paradosso una nuova forma di libertà individuale, un accrescimento della socialità umana che si è allargata sull'ampio orizzonte del nuovo circuito delle informazioni, un potenziamento, dunque, dell'energia intellettuale e operativa del singolo vivente nella comunità»<sup>58</sup>.

Per il tramite della tecnologia mutano sempre più gli assetti istituzionali conosciuti e come il processo democratico venga a essere profondamente influenzato dal modo in cui circolano le informazioni, laddove cioè la disponibilità di queste da parte di tutti i cittadini appare come un prerequisito di quel processo. È questo il punto, credo: la libera circolazione delle informazioni può produrre la formazione di una coscienza civile e politica più avvertita con un richiamo non più episodico agli interessi e alla capacità di giudizio del singolo cittadino, il quale sarebbe piuttosto reso partecipe di un circuito comunitario di informazione e di responsabilità. La democrazia, e la sua forma, si prospetta in una forma diversa da quella che era nei secoli precedenti: mutano i significati di rappresentanza e di sovranità, avanza una nuova democrazia di massa, che rompe le cerchie chiuse delle élites al potere, obbligando per così dire i rappresentanti della volontà popolare a scendere sulla piazza telematica e a confrontarsi direttamente con i rappresentanti, nelle nuove forme assunte dalla tecnopolitica<sup>59</sup>. Per

---

<sup>57</sup> Così, V. FROSINI, *La democrazia nel XXI secolo*, cit., 23 ss.

<sup>58</sup> *Ibidem*, 34.

<sup>59</sup> Sulla questione, v. S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997; ID., *Libertà, opportunità, democrazia e informazione*, in *Internet e Privacy: quali regole?*, Atti del convegno organizzato dal Garante per la protezione dei dati personali, Roma, 1998, 12 ss. il quale, con riferimento a Internet, la definisce come «una forma

avviare così un processo di “orizzontalizzazione della politica”, e quindi non una mera subordinazione a decisioni imposte dall’alto, per così dire, ma piuttosto un modo per concorrere – orizzontalmente, per l’appunto – alle scelte nell’interesse della nazione e del bene comune (*common good*), quale principio della libertà.

Oggi, sebbene con qualche incertezza, stiamo assistendo alle trasformazioni della c.d. democrazia elettorale – quella fondata sul meccanismo del voto – in seguito allo sviluppo tecnologico delle società contemporanee. Per adesso, le trasformazioni riguardano essenzialmente le tecniche di votazione, ovvero sul come si vota. La scheda elettorale cartacea sulla quale si appone, con matita copiativa, la propria scelta politica è prossima a essere messa da parte. È già in fase di utilizzazione in diverse parti del mondo<sup>60</sup>, il c.d. voto elettronico, che prevede l’effettuazione del voto per il tramite dei *computers*. Anziché porre un segno con la matita sulla scheda elettorale, si potrà pigiare il tasto di una tastiera del *computer*, nel cui video verrebbe riprodotta la scheda elettorale elettronica, ed esprimere così il proprio voto e la propria preferenza politica. Questa tecnica di votazione – che si presenta semplice da realizzarsi nel caso del voto per i *referendum*, dovendo scegliere solo tra un “sì” o un “no” – consentirebbe di avere i risultati elettorali in brevissimo tempo una volta chiuse le votazioni, e di evitare defaticanti calcoli e scrutini peraltro sempre soggetti al rischio di brogli elettorali. La votazione *online* potrebbe altresì essere utilizzata, con semplificazione e razionalizzazione, per le primarie con le quali si selezionano i candidati alle cariche elettive. Anziché sparpagliati banchetti in giro per il territorio per la raccolta di voti, con rischi sempre più diffusi di brogli e pasticci di computo finale, basterebbe un’organizzazione sul *web*, dove chiamare a raccolta *online* coloro i quali volessero esprimere la loro preferenza per le candidature.

Ma gli scenari futuri della democrazia elettorale non si arrestano al voto elettronico. Infatti, si potrebbe inoltre prevedere il voto attraverso il proprio *home computer*, oppure addirittura attraverso il televisore con l’ausilio del telecomando. Certo, questa tecnica di votazione “casalinga” se da un lato potrebbe ridurre l’astensionismo (oltre alle spese elettorali), dall’altro lato però imporrebbe la fissazione di tutta una serie di garanzie (anche di carattere tecnico) per la salvaguardia della libertà di voto. Che anche – e

---

che la democrazia può assumere, è una opportunità per rafforzare la declinante partecipazione politica. È un modo per modificare i processi di decisione democratica».

<sup>60</sup> Sulla diffusione del voto elettronico e le sue implicazioni giuridico-costituzionali, v. ora, M. SCHIRRIPIA, *Le nuove frontiere del diritto di voto. Uno studio di diritto comparato*, Padova, 2021.

forse soprattutto – nell'epoca della politica “tecnologizzata” e “globalizzata” rimane sempre un valore costituzionale da custodire gelosamente<sup>61</sup>. Ma di fronte al futuro dobbiamo mostrarci ottimisti e concorrere a un rinnovato progresso della civiltà. Allora, ben venga la nuova democrazia tecnologica del XXI secolo, che si fonda sulla libera iniziativa individuale, sulla responsabilità del cittadino come persona, sulla sua facoltà di scelta e di decisione. Il voto individuale viene a essere protetto e potenziato nella sua collocazione telematica, che elimina le manipolazioni, gli errori e i brogli dei sistemi cartacei, che consente una possibilità di scelta con il voto disgiunto, o alternativo, o di riserva, che può essere controllato e calcolato con l'ausilio del *computer*. È una democrazia non delegante ma partecipativa, che manifesta una nuova forma di libertà segnata dalla partecipazione del cittadino alla vita della collettività in forma di partecipazione al potere politico. Nasce così una «libera repubblica dell'informazione automatizzata [che] equivale, per la sua funzionalità di comunicazione e quindi anche di suggerimenti, di rivelazioni, di accordi e di deleghe, a una nuova forma democratica di società: essa instaura le condizioni tecniche per l'attuazione pratica di un regime politico della democrazia di massa»<sup>62</sup>.

Certo, non nego che vi è un problema che attiene alla c.d. democrazia economica<sup>63</sup>. Si tratta della concentrazione di mercato da parte di alcune grandi aziende che operano su Internet: *Google*, *Facebook* e *Amazon*. La prima, *Google*, domina il proprio settore con una quota di mercato dell'88% nel *search advertising* (pubblicità su motori di ricerca); la seconda, *Facebook* (e le sue controllate: *Instagram*, *WhatsApp* e *Messenger*) possiede il 77% del traffico dei *social network* su dispositivi mobili e, infine, la terza, *Amazon*, ha una quota del 74% nel mercato dell'*e-book*. In termini economici classici, tutte e tre sono dei monopoli. Quindi, c'è un serio problema di privazione della libera concorrenza, che limita l'essenza della democrazia liberale, attraverso lo “abuso di posizione dominante” e la “dipendenza economica”. Non è però solo un problema di *antitrust*, che peraltro ha già fatto sentire, sia pure flebilmente, la sua voce attraverso l'Autorità garante europea e la Commissione europea, come nei casi *Microsoft* e *Google*, ponendo il dubbio che alcune pratiche commerciali (di *Google*, in particolare) siano da ritenersi in violazione dell'art. 102 del

---

<sup>61</sup> Su cui, v. C. MARCHESE, *Il diritto di voto e la partecipazione politica. Studio di diritto comparato*, Napoli, 2019.

<sup>62</sup> Così, V. FROSINI, *La democrazia nel XXI secolo*, cit., 33.

<sup>63</sup> Su cui, v. E.C. RAFFIOTTA, *Libertà economiche e Internet*, in *Diritti e libertà in Internet*, cit., 413 ss.

trattato sul funzionamento dell'Unione europea (TFUE) e dell'art. 54 dell'accordo SEE<sup>64</sup>.

Non è solo un problema di *antitrust*, dicevo. Dall'angolazione democratica, infatti, si possono temere rischi di un potentato economico così forte da condizionare non solo e non tanto il mercato economico ma piuttosto anche il mercato delle idee. Che potrebbe essere condizionato dalle scelte imposte dalle grandi aziende di internet, che sarebbero mirate anche al raggiungimento di un sistema più favorevole ai propri interessi economici. È auspicabile, quindi, una maggiore concorrenza nel comparto dell'internet, consentendo ad altri soggetti di entrare nel mercato senza rischiare di essere compressi dalle grandi imprese, che operano come se fossero in regime monopolista. Come scriveva Louis D. Brandeis, prima ancora di essere nominato da Woodrow Wilson giudice della Corte Suprema: «in una società democratica, l'esistenza di grandi centri di potere privati è pericolosa per la vitalità di un popolo libero»<sup>65</sup>.

Ampliare, allargare, espandere l'offerta *di e su* internet, per intensificare il pluralismo delle informazioni, delle opinioni, delle idee. Anche così si potrà consolidare internet quale strumento al servizio della democrazia e delle libertà.

## 9. Fake news e disinformazione

Un cenno finale occorre farlo con riferimento al tema delle *fake news*, che sono come la calunnia nell'aria rossiniana: «un venticello [...] prende forza a poco a poco, vola già di loco in loco». Si tratta, quindi, delle notizie false e tendenziose, che circolano sulla rete Internet e che potrebbero ingannare il consumatore, oppure informare scorrettamente e mendacemente il cittadino<sup>66</sup>. Sono stati invocati addirittura rischi per la democrazia e si è auspicato di sottoporre Internet a regole di garanzia sulla qualità delle notizie, magari certificate da un'Autorità indipendente. Le notizie false ci sono sempre state (e sempre ci saranno) in tutti i settori della comunicazione, pubblica e privata, sulla stampa e sulla rete. In quest'ultima, poi, te-

---

<sup>64</sup> Mi riferisco al caso *Microsoft*, su cui v. A. GIANNACCARI, *La concentrazione Microsoft-Skype (vs Facebook-WhatsApp?)*. Ovvero una guerra per bande alle spalle delle Telcos, in *Mercato Concorrenza Regole*, n. 1, 2014, 139 ss. In tema, v. ora V. FALCE, *Rapporti asimmetrici tra imprese e soluzioni pro-concorrenziali*, in *Riv. dir. ind.*, 4-5, 2021189 ss.

<sup>65</sup> Cfr. M.I. UROFSKY, *Louis D. Brandeis: a Life*, New York, 2012.

<sup>66</sup> Cfr. S. SASSI, *Disinformazione contro costituzionalismo*, Napoli, 2021.

nuto conto che si viene ad ampliare la libertà di espressione, che permette maggiore trasparenza e quindi consente un maggiore disvelamento della verità contro ogni censura.

Questione differente è quella della disinformazione, che non è la solo la notizia falsa ma più in generale un fenomeno degenerativo e disgregativo, che attenta alla libertà di informazione quale pilastro su cui si fonda il costituzionalismo. Certo, la disinformazione viaggia anche sulla televisione e sulla stampa ma assume forme più capziose e insidiose sulla rete, vuoi perché non c'è nessun tipo di controllo, se non quello dello dell'utente che dovrebbe sapere distinguere ciò che è buono da ciò che è cattivo, vuoi perché diventa "virale", potendo distribuirsi, in tempi rapidissimi, in numerosi siti internet in giro per il mondo, al punto da assumere una presunta ufficialità. In maniera un po' esagerata, c'è stato chi ha scritto che «di fronte alla rivoluzione digitale Schmitt dovrebbe riscrivere ancora una volta il suo principio della sovranità: *sovrano è colui che dispone delle informazioni in rete*»<sup>67</sup>. Si è financo ragionato su come provare a contrastare la disinformazione *online* e sono già state avanzate proposte legislative, specialmente nella UE. Attraverso una regolazione che sappia bilanciare l'algocrazia con l'algoritica, che «sviluppano un reticolo di norme di natura precipuamente orizzontale, che impongono doveri di diligenza in capo ai *Big Tech* posti a garanzia dei diritti fondamentali»<sup>68</sup>. Di tutt'altro modo e metodo l'impostazione statunitense che, vigente ancora la sez. 230 del *Communication Decency Act* del 1996, svincola le piattaforme digitali da qualunque responsabilità sui contenuti pubblicati dagli utenti<sup>69</sup>. Una soluzione dal sapore liberale, per così dire.

Certo, sulla rete, nonostante tutto, c'è concorrenza e pluralismo, in punto di offerta di informazioni<sup>70</sup>: occorre però ampliare, allargare, espandere l'offerta *di* e *su* internet, per intensificare il pluralismo delle informazioni, delle opinioni, delle idee. Anche così si potrà consolidare internet quale strumento al servizio della democrazia e delle libertà. Sul tema, soccorrono le parole del giudice Oliver W. Holmes, nella famosa *dissenting opinion* sul caso *Abrams vs. United States* (1919): «il bene supremo è meglio raggiunto attraverso il libero commercio delle idee, che la prova mi-

---

<sup>67</sup> B. CHUL HAN, *Infocrazia. Le nostre vite manipolate dalla rete*, tr. it., Torino, 2023, 16.

<sup>68</sup> Così, S. SASSI, *op.cit.*, 198.

<sup>69</sup> V. S.K. MYERS, *Wikimmunity: Fitting the Communication Decency Act to Wikipedia*, in *Harvard Journal of Law & Technology*, n. 20, 2006.

<sup>70</sup> Sul punto, F. DONATI, *Il principio del pluralismo delle fonti informative al tempo di Internet*, in *Percorsi Cost.*, n. 1, 2014, 31 ss.

gliore della verità è la capacità del pensiero di farsi accettare nella competizione del mercato e che la verità è l'unica base sulla quale i nostri desideri possono essere sicuramente realizzati»<sup>71</sup>.

## 10. Conclusioni

Si può concludere, sia pure provvisoriamente, come si è iniziato. L'ordine giuridico del digitale, quale statuto di norme, da intendersi come strutturata regolazione e codificazione, appare quale il metodo meno indicato per provare a dare un ordine giuridico al complesso mondo delle piattaforme digitali. Ecco perché non è da condividere la scelta della UE, peraltro opposta a quella adottata negli USA, di regolare gli sregolati con un profluvio di norme di dettaglio, alcune delle quali di difficile attuazione e pertanto rimandate alla concreta applicazione da parte dei singoli Stati. Come se fossero direttive più che regolamenti. Diversi anni fa, avevo scritto e teorizzato di *internet come ordinamento giuridico*<sup>72</sup>: dove c'è un ordine e un disordine; dove l'individuo è sovrano nell'esercizio di situazioni giuridiche e delle libertà costituzionali; dove ogni azione si inserisce in un insieme di regole, ogni regola trova attuazione nel comportamento.

L'elaborazione di una teoria di internet, ovvero il *cyberspace*, come ordinamento giuridico autonomo, proviene dalla dottrina costituzionalistica statunitense e muove dall'assunto che «*cyberspace is a distinct place for purposes of legal analysis by recognizing a legally significant border between cyberspace and the real world*». Ancora, il *cyberspace* diventa «*an important forum for the development of new connections between individuals and mechanism of self-governance*»<sup>73</sup>. Un diritto spontaneo, quindi. Un diritto pari a quello della *lex mercatoria*, con la quale si regolavano i rapporti commerciali nel medioevo. Una *lex informatica*, dunque; che può avvalersi di una *co-regulation*, in cui le leggi statali si verrebbero a integrare con una politica di *self-regulation* da parte degli utenti di internet<sup>74</sup>. Una sorta di applicazione del principio di sussidiarietà, in cui la *co-regulation* dello Sta-

<sup>71</sup> O.W. HOLMES, *Opinioni dissenzienti*, a cura di C. Geraci, Milano, 1975, 105.

<sup>72</sup> T.E. FROSINI, *Internet come ordinamento giuridico*, in *Percorsi cost.*, n. 1, 2014 (ora in ID., *Liberté Egalité Internet*, cit.).

<sup>73</sup> Cfr. D.R. JOHNSON, D. POST, *Law and Borders. The rise of Law in Cyberspace*, in *Stanford Law Review*, 48, 1996, 1378 e 1397.

<sup>74</sup> Tra i più convinti teorici della *co-regulation*, L. LESSIG, *Code and other law of Cyberspace*, New York, 1999.

to può venire in sussidio alla *self-regulation* degli utenti, quando questi la evocano ovvero quando la necessitano. La *self-regulation* agisce proprio in funzione di un ordinamento nel disordine della rete, dove ogni utente è in condizione di potere regolare le proprie situazioni a seconda delle esigenze e delle peculiarità. Forse il mio può apparire come un approccio illusorio, fin troppo ottimistico. Esprimere un *favor* per le piattaforme digitali, e tutte le sue declinazioni compresa la IA e le sue benefiche applicazioni a vantaggio dell'umanità, vuol dire, oggi, promuovere una rinnovata concezione del liberalismo, dove, cioè, si pone come prioritaria la libertà per il progresso e verso nuove forme di sviluppo dell'individuo e del benessere delle società. La posizione di chi auspica e pretende insistenti forme regolative delle piattaforme digitali, in forma pervasiva e dettagliata, a me appare come riconducibile a nuove forme di statalismo, che si manifestano nella volontà di fondare e stabilire una nuova sovranità degli stati sul digitale. Forse queste mie considerazioni mi costringono a sedermi dalla parte del dissenso, ma tutti gli altri posti risultano occupati.



Filippo Donati

## Quale disciplina per l'intelligenza artificiale?

SOMMARIO: 1. La rivoluzione dell'intelligenza artificiale. – 2. IA e tutela dei diritti. – 3. L'approccio risk-oriented. – 4. Profili di criticità. – 5. La sfida istituzionale.

### 1. La rivoluzione dell'intelligenza artificiale

Tutta la storia dell'umanità è stata caratterizzata dai cambiamenti prodotti dalle innovazioni tecnologiche. Alcune di queste hanno avuto una incidenza sulla società che può considerarsi rivoluzionaria. L'invenzione della stampa a caratteri mobili, ad esempio, ha radicalmente trasformato la diffusione delle conoscenze, fino ad allora affidata alla tradizione orale ovvero all'opera degli amanuensi e, pertanto, riservata a ristrette cerchie di persone. A partire dalla Bibbia di Gutenberg, la stampa ha permesso l'educazione delle masse e la circolazione su larga scala delle idee e delle informazioni.

Anche l'intelligenza artificiale può essere considerata tra le invenzioni con effetti "rivoluzionari" per la società<sup>1</sup>. L'intelligenza artificiale non è umana, è un procedimento creato dall'uomo. Essa, tuttavia, produce risultati che fino ad oggi si credeva potessero essere frutto soltanto della ragione. L'intelligenza artificiale aumenta anzi in maniera esponenziale le capacità dell'uomo, permettendogli di ottenere risultati non realizzabili soltanto con la mente.

Grande clamore, ad esempio, ha destato la scoperta di un nuovo potente antibiotico, *Halicin*, grazie all'impiego di un sistema di intelligenza artificiale elaborato da un gruppo di ricercatori del Massachusetts Institute of Technology (MIT). Gli studiosi del MIT hanno "programmato" l'algorit-

---

<sup>1</sup> A tal riguardo cfr. A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione*, Volume 1. Diritti fondamentali, dati personali e regolazione; Volume 2. Amministrazione, responsabilità, giurisdizione; Volume 3. Proprietà intellettuale, società, finanza, Bologna, 2022.

mo per individuare molecole con proprietà antibiotiche, aventi strutture differenti rispetto a quelle conosciute e non pericolose per l'uomo. L'algoritmo, dopo essere stato "addestrato" a riconoscere la struttura molecolare di un certo numero di antibiotici è riuscito, all'interno di un paniere di circa 6.000 molecole, ad individuarne una che presentava una potenziale attività antibatterica molto forte. La scoperta *Halicin* – nome ispirato a *Hal*, il computer del capolavoro di Kubrik *2001 Odissea nello spazio* – è stata un trionfo. *Halicin* è riuscito ad eliminare infezioni causate da ceppi batterici resistenti a tutte le altre formule conosciute. Con i mezzi tradizionali, la ricerca avrebbe richiesto grandi investimenti e tempi non brevi, con nessuna certezza di successo. I ricercatori del MIT hanno così aperto la strada per un impiego dell'intelligenza artificiale che potrà permettere di realizzare altri importanti progressi nel campo della medicina.

Grande entusiasmo ha poi suscitato *Chat GTP*, una *chatbox* che simula una conversazione umana, sviluppata dalla società americana *Open AI*. Si tratta di un sistema avanzato di intelligenza artificiale, basato su una tecnologia di *deep learning*, capace di rispondere pressoché a qualsiasi domanda, sia essa di storia, di matematica o di teoria generale. *Chat GTP* è in grado di scrivere o di completare lettere, presentazioni o saggi in qualsiasi lingua e in ottimo stile. Dal quando lo scorso 5 dicembre 2022 è stata resa disponibile al pubblico, la nuova *chatbox* è stata "presa d'assalto", al punto che spesso il sistema risulta non disponibile per eccessivo carico di richieste. Gli sviluppatori ne hanno annunciato ulteriori perfezionamenti, in modo da consentirgli di offrire risposte sempre più puntuali anche su argomenti di stretta attualità. Sistemi come questo potranno, in futuro, influenzare i comportamenti di milioni di persone.

L'intelligenza artificiale viene oggi quotidianamente applicata in numerosi settori, dall'agricoltura alla mobilità, dalla sicurezza alla difesa, dall'educazione alla salute. Hanno dunque ragione Henry Kissinger, Eric Schmidt e Daniel Huttenlocher quando sostengono che la diffusione dei moderni sistemi di intelligenza artificiale abbia comportato una rivoluzione, inaugurando una nuova era nella storia dell'umanità<sup>2</sup>.

Non è necessario proseguire con altri esempi. Nessuno ormai più dubita che grandi sono le potenzialità aperte dallo sviluppo dell'intelligenza artificiale. Ma grandi sono anche i rischi derivanti dal suo utilizzo. Come conciliare quindi potenzialità e rischi derivanti dall'impiego dei nuovi sistemi di intelligenza artificiale?

---

<sup>2</sup>H. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER, *The Age of AI And Our Human Future*, New York-Boston-London, 2021.

## 2. IA e tutela dei diritti

A differenza degli algoritmi tradizionali, quelli di *machine learning* spesso non sono trasparenti, spiegabili o interpretabili e, pertanto, sono paragonati ad una *black box*, una scatola chiusa, che non può essere aperta facilmente<sup>3</sup>. Questa opacità solleva una serie di delicati problemi.

Eventuali vizi del sistema, dovuti o ad errori nella progettazione del *software* oppure all'impiego, nella fase di addestramento, di dati incompleti o imprecisi, possono contribuire a decisioni errate o discriminatorie. I sistemi di IA, pur essendo ormai uno strumento essenziale per lo sviluppo economico e il benessere sociale, possono, dunque, comportare un rischio, anche molto elevato, di lesione dei diritti fondamentali, dei principi democratici e della *rule of law*<sup>4</sup>.

Non possiamo, ad esempio, trascurare le conseguenze di eventuali difetti di programmazione o di funzionamento, quando i sistemi di intelligenza artificiale sono impiegati per decidere sulla concessione di un mutuo o sull'apertura di una linea di credito, per selezionare studenti o aspiranti a posti di lavoro, per l'adozione di provvedimenti amministrativi o di decisioni giudiziarie e, più in generale, per assumere decisioni che impattano sui diritti della persona. L'intelligenza artificiale, inoltre, si presta ad essere utilizzata per fini illeciti, come ad esempio la creazione e la diffusione di notizie false e di campagne di disinformazione, capaci di influenzare le scelte di grandi masse di persone e di incidere sui processi democratici. La recente guerra in Ucraina, d'altro canto, ha confermato le grandi potenzialità dei sistemi di intelligenza artificiale persino nei conflitti armati.

Rischi del genere non possono ovviamente essere sottovalutati. Chi si concentra troppo sui rischi che l'intelligenza artificiale comporta per i diritti e i principi fondamentali, però, non è in grado di valorizzare adeguatamente le opportunità che il progresso tecnologico è oggi in grado di offrire alle persone. Occorre inoltre considerare che pregiudizi ed errori possono sussistere anche nelle decisioni umane e che i sistemi di intelligenza artificiale non necessariamente offrono un grado di affidabilità inferiore a quello delle persone fisiche. Per non parlare poi del fatto che tali sistemi operano meccanicamente e, pertanto, non sono esposti a quei rischi di cor-

---

<sup>3</sup>Cfr. F. PASQUALE, *The black box society: The secret algorithms that control money and information*, Cambridge-London, 2015.

<sup>4</sup>Per un approccio di cautela in considerazione dei rischi derivanti dall'impiego dell'intelligenza artificiale cfr., tra gli altri, A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaaw journal*, 2019, 63 ss.

ruzione o di indebito condizionamento cui, purtroppo, alcune persone non sono state in grado di sottrarsi. Se utilizzata correttamente, inoltre, l'intelligenza artificiale può contribuire al rafforzamento dei diritti della persona (si pensi alle possibili applicazioni delle nuove tecnologie nel campo della salute, dell'agricoltura, della sicurezza, ecc.), allo sviluppo economico e al benessere sociale.

La scelta se consentire o meno l'impiego di sistemi di intelligenza artificiale, pertanto, non deve riflettere una alternativa tra le esigenze di efficienza e quelle di tutela dei diritti delle persone. L'adozione di tali sistemi, invece, deve essere accompagnata dalla consapevolezza della possibilità di un diverso modo di tutelare i diritti delle persone. Nei sistemi di intelligenza artificiale, infatti, la tutela dei diritti deve essere garantita soprattutto nelle fasi di progettazione, di addestramento e di controllo sul funzionamento del *software*.

È questa la filosofia cui si ispira la politica dell'Unione europea in materia di intelligenza artificiale. Le proposte della Commissione sono infatti basate sull'idea che soltanto un'adeguata regolazione può rendere i sistemi di intelligenza artificiale non più una minaccia per i diritti delle persone, ma uno strumento a servizio degli stessi. Il piano dell'Unione europea muove dunque dalla convinzione che la tutela della sicurezza e la garanzia dei diritti fondamentali rappresentano presupposti indispensabili per promuovere lo sviluppo e la diffusione in Europa dell'intelligenza artificiale, garantendo.

In questa prospettiva, la Commissione ha presentato una proposta di regolamento<sup>5</sup>, volta a controllare e prevenire i rischi derivanti dall'impiego

---

<sup>5</sup>Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 21 aprile 2021, COM/2021/206 final. Cfr. al riguardo A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Volume 1. *Diritti fondamentali, dati personali e regolazione*, cit., 127 ss.; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di Regolamento dell'intelligenza artificiale*, *ivi*, 111 ss.; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 415 ss.; O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *La proposta di Regolamento sull'intelligenza artificiale: Verso una nuova governance europea*, in *Agenda Digitale, L'intelligenza artificiale made in Ue è davvero "umano-centrica"? I conflitti della proposta*; F.C. LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale*, in *Diritto penale e uomo*, 2021, 1 ss.; M. EBERS, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. DI MATTEO, M. CANNARSA, C. PONCIBÒ (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, in corso di pubblicazione ma reperibile in <http://dx.doi.org/10.2139/ssrn.3900378>; M. EBERS, V.R.S. HOCH, F.

dell'intelligenza artificiale. A questa ha fatto seguito una proposta di direttiva, volta ad armonizzare il regime di responsabilità nel caso in cui tali sistemi comportino la violazione di diritti<sup>6</sup>, ed una proposta volta ad estendere il campo di applicazione della direttiva sulla responsabilità per danno da prodotti difettosi, includendovi anche *software*, servizi digitali e sistemi di intelligenza artificiale<sup>7</sup>.

### 3. L'approccio risk-oriented

La politica dell'Unione europea muove dalla consapevolezza che i nuovi sistemi di intelligenza artificiale saranno la chiave per lo sviluppo dell'economia e della società e che un'adeguata regolazione può renderli non più una minaccia, ma anzi uno strumento per migliorare la vita delle persone e il godimento dei diritti fondamentali.

In questa prospettiva, la Commissione ha elaborato una disciplina basata sulla individuazione del livello di rischio per i diritti fondamentali derivante dal tipo di utilizzo del *software*.

In particolare, la proposta di regolamento vieta i sistemi considerati come fonte di rischi inaccettabili per la dignità umana e per i diritti fondamentali della persona, come quelli che impiegano tecniche subliminali, sfruttano la vulnerabilità di specifici gruppi per distorcere il comportamento delle persone, permettono forme di *social scoring* o consentono l'identificazione biometrica remota in tempo reale in spazi aperti al pubblico. Sono invece assoggettati a una stringente disciplina i sistemi che comportano un

---

ROSENKRANZ, H. RUSCHEMEIER –, B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act-A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J 2021, 4, 589-603, <https://doi.org/10.3390/j4040043>; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, L. WENLONG, R. PISELLI, K. YEUNG, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act* (August 5, 2021), in <http://dx.doi.org/10.2139/ssrn.3899991>; 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*, in *Computer Law Review International*, 4/2001, 97 ss.; P. GLAUNER, *An Assessment of the AI Regulation Proposed by the European Commission*, in S. EHSANI, P. GLAUNER, P. PLUGMANN, F.M. THIERINGER (eds.), *The Future Circle of Healthcare: AI, 3D Printing, Longevity, Ethics, and Uncertainty Mitigation*, in corso di pubblicazione, ma reperibile in <https://arxiv.org/pdf/2105.15133.pdf>.

<sup>6</sup>Proposta di direttiva *relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)*, 28 settembre 2022, COM(2022)496 final.

<sup>7</sup>Proposta di direttiva *sulla responsabilità per danno da prodotti difettosi*, 28 settembre 2022, COM(2022)495 final.

alto rischio di violazione dei valori e dei diritti fondamentali, come quelli impiegati per la gestione di infrastrutture essenziali, per la selezione di studenti e lavoratori, per misurare l'affidabilità creditizia delle persone, per valutare la pericolosità delle persone nell'ambito di attività di prevenzione o repressione del crimine, per la gestione della migrazione, dell'asilo e del controllo alle frontiere, per lo svolgimento dell'attività giurisdizionale. Questi sistemi sono sottoposti a valutazione di conformità, certificazioni, obblighi di registrazione e controlli *ex post* per verificare l'osservanza delle prescrizioni dirette a garantirne la trasparenza, l'affidabilità ed il controllo da parte dell'uomo. Per i sistemi considerati a rischio limitato, come i *chatbot*, sono imposti meri obblighi di segnalazione per gli utenti. Nessuna restrizione è infine prevista per i sistemi di intelligenza artificiale che comportano livelli di rischio ritenuti minimi, come ad esempio quelli impiegati per servizi di traduzione automatica, videogiochi, filtri antispam, ecc.

Anche la proposta di direttiva sulla responsabilità civile per danni da intelligenza artificiale intende contribuire allo sviluppo e alla diffusione di sistemi sicuri, affidabili e rispettosi dei valori e dei diritti dell'Unione, attraverso un'armonizzazione normativa volta a ridurre l'incertezza per le imprese che sviluppano o utilizzano l'IA in relazione a possibili esposizioni a responsabilità civile. Le caratteristiche specifiche dell'IA, tra cui la complessità, l'autonomia e l'opacità (il c.d. effetto *black box*), possono infatti rendere difficile o eccessivamente costoso, per quanti subiscono un danno, identificare il responsabile e dimostrare la sua responsabilità. La proposta intende superare o attenuare le specifiche difficoltà di prova quando vengono in rilievo sistemi di intelligenza artificiale, al fine di garantire un'idonea tutela ai soggetti che ne fanno uso.

Anche la proposta di direttiva prevede un regime differenziato per i sistemi di IA considerati ad alto rischio. La proposta facilita, infatti, la possibilità di accesso o la conservazione degli elementi di prova pertinenti relativi ai danni causati da tali sistemi, per consentire all'attore in un'azione civile di responsabilità extracontrattuale per colpa di motivare adeguatamente la domanda di risarcimento del danno. Essa incentiva, inoltre, il rispetto dei requisiti e degli obblighi previsti dal regolamento per i sistemi ad alto rischio, stabilendo che la non conformità ad essi può comportare, a determinate condizioni, l'applicazione di una presunzione di causalità.

#### 4. Profili di criticità

La scelta di adattare la nuova disciplina al grado di rischio derivante dall'impiego dei diversi sistemi di intelligenza artificiale è condivisibile,

perché idonea a bilanciare l'esigenza di tutela dei diritti con quella di promuovere lo sviluppo dell'innovazione tecnologica. Non possono, però, essere sottovalutati possibili problemi.

Uno di questi è correlato al fatto che il quadro normativo proposto dalla Commissione si basa su una identificazione del grado di rischio effettuata in astratto e in via preventiva, che potrebbe in certi casi rivelarsi troppo rigida, inadeguata alla prova dei fatti e non facilmente modificabile.

Inoltre, l'obiettivo di assicurare il controllo umano, la trasparenza e la tutela dei diritti e delle libertà delle persone già è difficile da raggiungere con riguardo ai singoli sistemi di intelligenza artificiale. Lo sarà ancora di più con la crescente diffusione dell'*Internet of things*, cioè la connessione a Internet di oggetti fisici. Un numero sempre maggiore di oggetti che impiegano sistemi di intelligenza artificiale, dai cellulari agli impianti domestici, dagli strumenti medici ai sistemi per la sicurezza dei trasporti, ecc., inizieranno verosimilmente ad interagire tra di loro, con effetti potenzialmente imprevedibili. Un esempio è quello del mondo della finanza, dove gli algoritmi che dispongono vendite o acquisti a seguito del raggiungimento di certe soglie di prezzi si sono trovati ad interferire tra di loro, dando vita ad effetti cumulativi che hanno portato a oscillazioni della quotazione di strumenti finanziari del tutto imprevedute e imprevedibili. Il collegamento di algoritmi che operano in maniera significativamente autonoma dalle istruzioni inizialmente ricevute dai programmatori, perché basati su sistemi di auto-apprendimento, potrebbe dunque accrescere la loro autonomia. In casi del genere, il nuovo quadro normativo potrebbe rivelarsi non sufficiente per a garantire un effettivo controllo *ex ante* e una efficace tutela *ex post* in caso di lesioni causate da sistemi di intelligenza artificiale.

## 5. La sfida istituzionale

In definitiva, le proposte della Commissione riflettono un ragionevole bilanciamento tra l'esigenza di promuovere lo sviluppo e l'impiego dei sistemi di intelligenza artificiale e l'esigenza di proteggere i diritti della persona. Nonostante alcune criticità, nel loro complesso le proposte meritano una valutazione positiva. È dunque auspicabile una loro veloce approvazione.

Il successo o meno del nuovo quadro dipenderà però in larga misura dalle istituzioni chiamate ad applicarlo: non solo le autorità giurisdizionali, ma anche i nuovi organismi cui la proposta di regolamento affida il compito di garantire l'attuazione della nuova disciplina.

La valutazione della conformità dei sistemi di IA ad alto rischio rispetto ai requisiti previsti dal regolamento è affidata a organismi nazionali di certificazione. Ciascuno Stato membro dovrà, inoltre, istituire appositi organismi (le autorità di notifica), chiamate a valutare e notificare le autorità di certificazione<sup>8</sup>. Gli Stati membri, nel disciplinare l'organizzazione e il funzionamento degli organismi di notifica e degli organismi nazionali di certificazione, dovranno “*salvaguardare l'indipendenza, l'obiettività e l'imparzialità delle loro attività*”<sup>9</sup>.

La proposta di regolamento prevede l'istituzione del Comitato europeo per l'intelligenza artificiale, organo di consulenza della Commissione sulle questioni relative all'applicazione del regolamento e di coordinamento tra questa e le autorità nazionali. Faranno parte del Comitato la Commissione, che lo presiede, le autorità nazionali di vigilanza e il Garante europeo della protezione dei dati. Altre autorità nazionali potranno essere invitate alle riunioni, laddove si discuta di materie di loro interesse<sup>10</sup>. È infine previsto che ciascuno Stato membro istituisca o designi una o più autorità nazionali competenti a garantire l'applicazione e l'attuazione del regolamento, garantendone l'imparzialità e dotandole di personale con adeguate competenze tecniche<sup>11</sup>.

Questo nuovo, complesso, sistema di *governance* sarà chiamato a svolgere un compito tanto importante quanto difficile. La nuova disciplina richiede infatti delicati bilanciamenti tra l'esigenza di favorire lo sviluppo dei sistemi di IA, da una parte, e l'esigenza di tutelare i diritti e le libertà delle persone contro le minacce che discendono dall'impiego di tali sistemi, dall'altra parte.

L'idoneità o meno dei nuovi organismi previsti dal regolamento ad effettuare in maniera corretta questi delicati bilanciamenti dipenderà dalla qualità e dalla competenza tecnica delle persone chiamate a farne parte. Occorreranno persone capaci di valutare e risolvere, in piena indipendenza e autonomia, i molteplici problemi di natura tecnica, legale ed etica che possono nascere dall'impiego dei nuovi sistemi di intelligenza artificiale.

L'autonomia, l'indipendenza e la preparazione tecnica delle autorità chiamate ad applicare la nuova disciplina rappresentano un presupposto necessario per consentire lo sviluppo e la diffusione di un'intelligenza artificiale sicura, affidabile ed etica.

---

<sup>8</sup> Cfr. l'art. 30 della proposta di regolamento.

<sup>9</sup> Cfr. l'art. 33 della proposta di regolamento.

<sup>10</sup> Cfr. l'art. 57 della proposta di regolamento.

<sup>11</sup> Cfr. l'art. 59 della proposta di regolamento, dove (comma 4) si chiede una profonda conoscenza in materia di tecnologie dell'intelligenza artificiale, data science, diritti fondamentali, salute e sicurezza, standard e normativa applicabile.

Cristina Schepisi

## Brevi note sulla “dimensione europea” della regolamentazione dell’intelligenza artificiale: principi, obiettivi e requisiti

SOMMARIO: 1. Introduzione. – 2 La dimensione europea, l’esigenza di non frammentare il mercato e il bilanciamento con la tutela dei diritti. – 3. Il pre-requisito per una dimensione europea: una definizione uniforme e chiara di “sistema di intelligenza artificiale”. – 4. La precisazione del rapporto tra la tutela del mercato e quella dei diritti fondamentali. – 5. La dimensione europea dei diritti, l’identificazione *ex ante* di alcuni diritti davvero fondamentali. – 6. Il necessario bilanciamento *ex ante* tra i vari diritti. – 7. L’aspetto procedurale europeo: la scelta della base giuridica e della misura da adottare. – 8. Profili conclusivi.

### 1. Introduzione

La regolazione dell’intelligenza artificiale è un tema che occupa il dibattito europeo da alcuni anni. I sistemi che usano tale tecnologia consentono innegabili benefici, sia economici che sociali ma dall’altro possono, come noto, comportare rischi, anche molto elevati, di lesione dei diritti fondamentali, della *rule of law* e dei principi democratici. L’opacità, la complessità, la dipendenza dai dati, il comportamento autonomo sono tutte caratteristiche dei sistemi di IA che possono incidere negativamente su una serie di diritti protetti dalla Carta europea<sup>1</sup>.

Di fronte alle sfide che pone l’uso di sistemi di intelligenza artificiale la strada scelta dall’Unione europea è stata, come noto, quella di proporre

---

<sup>1</sup> V. punto 3.5, della Relazione alla proposta di regolazione dell’IA, 13; la Comunicazione della Commissione “*Creare fiducia nell’intelligenza artificiale antropocentrica*” (COM(2019)168 final); la Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell’intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

l'adozione di un regolamento sulla base giuridica dell'art. 114 TFUE<sup>2</sup>, con l'obiettivo di introdurre, in capo a coloro i quali producono, mettono in servizio o usano sistemi di intelligenza artificiale, divieti, obblighi ed adempimenti procedurali, calibrati sul diverso livello rischio di lesione che tali sistemi sono suscettibili di produrre per i diritti fondamentali.

Sulla base di tale proposta<sup>3</sup> sono vietati i sistemi che comportano un rischio inaccettabile e dunque i sistemi che usano tecniche subliminali e manipolatorie, che attribuiscono un punteggio sociale, i sistemi di riconoscimento biometrico *in real time*, con eccezioni di taluni casi particolari<sup>4</sup>.

I sistemi ad alto rischio sono invece definiti dall'art. 6 (prodotti o componenti di sicurezza di prodotti) e includono tutti i sistemi indicati nell'Allegato III: la gestione e funzionamento delle infrastrutture critiche, l'istruzione e formazione professionale, l'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; l'accesso a prestazioni e servizi pubblici e a servizi privati essenziali; i servizi di emergenza di primo soccorso compresi vigili del fuoco, le applicazioni utilizzate per le attività di contrasto, la gestione della migrazione, dell'asilo e del controllo delle frontiere, l'amministrazione della giustizia e processi democratici<sup>5</sup>.

Per tali sistemi, il Capo 2 del regolamento impone una numerosa serie di requisiti (accuratezza, robustezza e cybersicurezza<sup>6</sup>; gestione di rischi; *governance* dei dati; trasparenza e informazioni; conservazione delle registrazioni; ecc.<sup>7</sup>), obblighi in capo ai fornitori distributori e utilizzatori (gestione

<sup>2</sup> Proposta di regolamento *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM (2021)206 def., 21 aprile 2021.

<sup>3</sup> Art. 5.

<sup>4</sup> In riferimento alla proposta iniziale della Commissione, le eccezioni sono le seguenti: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'art. 2, par. 2, decisione quadro 2002/584/GAI del Consiglio punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

<sup>5</sup> Sulla regolazione dell'IA nell'ambito della pubblica amministrazione si rinvia a E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni: prove generali*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) *Intelligenza artificiale e diritto: una rivoluzione?*, Il Mulino, Bologna, 2022.

<sup>6</sup> Art. 15.

<sup>7</sup> Artt. da 9 a 16.

della qualità, certificazioni, trasparenza)<sup>8</sup> e controllo da parte delle autorità nazionali<sup>9</sup>. L’art. 14 richiede inoltre che sia comunque sempre assicurato il controllo umano e che un sistema ad alto rischio possa essere vietato qualora comporti, all’esito di una verifica, rischi non prevedibili o non controllabili.

Sono invece soggetti solo ad un obbligo di trasparenza e informazione i sistemi di IA destinati a interagire con le persone fisiche come ad esempio i sistemi per il riconoscimento delle emozioni di una persona o categorizzazione biometrica e i sistemi che generano o manipolano immagini o contenuti audio o video e che potrebbero apparire falsamente autentici o veri per una persona (“deep fake”)<sup>10</sup>.

Il presente contributo non intende esaminare nel dettaglio il contenuto della proposta, che è ancora in discussione<sup>11</sup>. L’obiettivo è invece quello di svolgere alcune brevi riflessioni sulla ‘dimensione’ europea che caratterizza la regolazione dell’IA con particolare riferimento alla proposta della Commissione europea e tenendo conto anche delle modifiche apportate durante l’iter della sua adozione, ancora in corso, con riferimento alla posizione assunta dal Consiglio dell’Unione nel suo Compromesso finale adottato a fine anno 2022<sup>12</sup>.

---

<sup>8</sup> Artt. da 16 a 29.

<sup>9</sup> Art. 59 ss. V. la struttura di *Governance*, art. 56 ss.

<sup>10</sup> Art. 52.

<sup>11</sup> Per alcuni commenti, *ex multis*, A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) *Intelligenza artificiale e diritto: una rivoluzione?*, vol. I, II e III, il Mulino, Bologna, 2022; G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell’intelligenza artificiale*, il Mulino, Bologna, 2021; A. ADINOLFI, *L’Unione europea dinanzi allo sviluppo dell’intelligenza artificiale: la costruzione di uno schema di regolamentazione europea tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell’era dell’intelligenza artificiale*, Pacini, Pisa, 2020, 13 ss.; G. CONTALDI, *La proposta di regolamento sull’intelligenza artificiale e la protezione di dati personali*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2022, 205 ss. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell’Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 415 ss.; M. EBERS, *Standardizing AI – The Case of the European Commission’s Proposal for an Artificial Intelligence Act*, in L.A. DI MATTEO, N. CANNARSA, C. PONCIBO (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge; O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *La proposta di Regolamento sull’intelligenza artificiale: Verso una nuova governance europea*, in *Agenda Digitale, L’intelligenza artificiale made in Ue è davvero “umano-centrica”? I conflitti della proposta*.

<sup>12</sup> Consiglio dell’Unione europea – *Orientamento generale* del 25 novembre 2022 – Fascicolo Interistituzionale.

## 2. La dimensione europea, l'esigenza di non frammentare il mercato e il bilanciamento con la tutela dei diritti

Regolare i sistemi di intelligenza artificiale a livello di Unione evita innanzitutto la frammentazione del mercato interno e il rischio di coesistenza di distinti meccanismi di regolazione, *ex ante* o *ex post*, per singoli settori e pertanto giustifica, agli occhi della Commissione, la scelta dell'art. 114 TFUE come base giuridica per l'adozione del futuro atto normativo<sup>13</sup>. Se ciascuno Stato – anche in nome di esigenze più che legittime di tutela dei diritti – ponesse unilateralmente limiti e divieti all'uso di sistemi di intelligenza artificiale, ne deriverebbero evidenti restrizioni alla libera circolazione dei servizi e dei prodotti tra uno Stato e l'altro.

La scelta di procedere con una regolazione orizzontale ha dunque prevalso su quella di disciplinare verticalmente i diversi settori (o solo alcuni di essi, es. lavoro, sanità, istruzione, giurisdizione) nei quali i sistemi di intelligenza artificiale possono generare maggiore preoccupazione, o direttamente e singolarmente i diversi sistemi (prodotti, *machine learning*, *deep fake*, ecc.), approccio quest'ultimo che sarebbe risultato assai limitativo viste le molteplici applicazioni che un sistema di IA può avere nei vari settori e il diverso impatto che può produrre.

I livelli di rischio, e i connessi divieti e obblighi procedurali prescindono inoltre anche dalle dimensioni del fornitore e/o della piattaforma digitale (a differenza invece di quanto previsto dal *Digital Markets Act*<sup>14</sup> e del *Digital Services Act*<sup>15</sup>).

La dimensione europea della regolazione dell'IA va tuttavia ben oltre ad una evidente esigenza di non frammentare il mercato, non esaurendosi affatto in essa.

Secondo quanto si legge nella Relazione di accompagnamento della proposta l'obiettivo è innanzitutto quanto meno duplice e rimarca quanto già

---

<sup>13</sup> Per alcune riflessioni sulla correttezza della base giuridica prescelta, cfr. 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*, cit.

<sup>14</sup> Proposta di regolamento del Parlamento europeo e del Consiglio *relativo a mercati equi e contendibili nel settore digitale (DMA)* COM(2020)842 final, 15 dicembre 2020).

<sup>15</sup> COM(2020)845 final, 15 dicembre 2020, Proposta di regolamento del Parlamento europeo e del Consiglio *relativo a un mercato unico dei servizi digitali (DSA) e che modifica la direttiva 2000/31/CE*; Cfr. Da ultimo, G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di) *Verso una legislazione europea dei mercati e dei servizi digitali*, Cacucci, Bari, 2022.

indicato anche nel Libro Bianco<sup>16</sup>. L’interesse dell’Unione europea è da un lato quello di «preservare la leadership tecnologica dell’UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell’Unione». Dall’altro è di basarsi «sui valori e sui diritti fondamentali dell’UE» e «dare alle persone e agli altri utenti la fiducia per adottare le soluzioni basate sull’IA, incoraggiando al contempo le imprese a svilupparle»<sup>17</sup>.

Quali sono i presupposti e i requisiti per una regolamentazione europea che sia al contempo uniforme, chiara ed equilibrata? L’adozione di una regolamentazione uniforme presuppone infatti che siano precisati non solo gli obiettivi che essa si pone ma anche cosa si vuole regolare e a quale livello. Il risultato dipende dunque dalle diverse scelte e dai differenti valori sui quali l’Unione si fonda rispetto ad altri sistemi nel contesto mondiale.

### **3. Il pre-requisito per una dimensione europea: una definizione uniforme e chiara di “sistema di intelligenza artificiale”**

Il primo presupposto alla base di una regolamentazione uniforme è l’adozione di una definizione unica e sufficientemente chiara di sistema di intelligenza artificiale. Un “sistema di intelligenza artificiale” può infatti indicare una molteplicità di tipologie e distinte applicazioni e che potrebbe dunque essere soggetto ad interpretazioni divergenti. La stessa Relazione illustrativa chiede che la nozione di sistema di IA debba «essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici»<sup>18</sup>.

---

<sup>16</sup> *Libro bianco sull’intelligenza artificiale – Un approccio europeo all’eccellenza e alla fiducia*, cit.

<sup>17</sup> *Libro bianco sull’intelligenza artificiale – Un approccio europeo all’eccellenza e alla fiducia*, 19 febbraio 2020 COM(2020)65 final. Si veda anche il Report *Getting the future right – Artificial intelligence and Fundamental rights* – FRA – European Union Agency for Fundamental Rights (December 2020), secondo la quale: «A wider range of rights need to be considered when using AI, depending on the technology and area of use. In addition to rights concerning privacy and data protection, equality and non-discrimination, and access to justice, other rights could be considered. These include, for example, human dignity, the right to social security and social assistance, the right to good administration (mostly relevant for the public sector) and consumer protection (particularly important for businesses). Depending on the context of the AI use, any other right protected in the Charter needs consideration» (7); nonché la *Relazione del PE sull’intelligenza artificiale nell’istruzione, nella cultura e nel settore audiovisivo* (2020/2017 (INI)) A9-0127/2021; e le Conclusioni della presidenza del Consiglio dell’Unione *The Charter of Fundamental rights in the context of Artificial Intelligence and Digital Change* – 21 October 2020 1148/20.

<sup>18</sup> V. il punto 7 della Relazione illustrativa secondo cui «La nozione di sistema di IA do-

Le difficoltà nel precisare tale nozione (e nel farlo in maniera corretta) sono evidenti, mancando a livello globale una definizione univoca di ‘sistema di intelligenza artificiale’, senza considerare inoltre che in alcuni contesti non è stata neppure esplicitata.

Nonostante la definizione inserita nella proposta di regolamento sia stata frutto di un lungo *iter* di modifiche e rimaneggiamenti al fine di renderla il più esaustiva possibile, è ancora in discussione una sua migliore precisazione.

Secondo tale iniziale definizione, un sistema di IA – che può consistere sia un prodotto che una componente di sicurezza di un prodotto – dovrebbe consistere in «un software sviluppato con una o più tecniche specifiche<sup>19</sup>, che può, per una determinata serie di obiettivi definiti dall’uomo in grado di generare contenuti, previsioni, decisioni che influenzano gli ambienti con cui interagiscono»<sup>20</sup>.

Critiche sono in particolare giunte da coloro che l’hanno ritenuta troppo generica<sup>21</sup>, e dunque suscettibile di divergenze interpretative e/o troppo ampia sì da comportare il rischio di una sovra regolamentazione. Una definizione eccessivamente dettagliata comporterebbe, per altri versi, numerosi dubbi circa l’inclusione o meno di taluni sistemi, nonché il rischio, che a seguito dell’evoluzione tecnologica, alcuni sistemi non vi rientrino affatto e che tale definizione diventi pertanto obsoleta.

In linea con la prima posizione, il Consiglio dell’Unione ha adottato, all’esito di una serie di testi di compromesso, la versione finale del suo “orientamento generale”<sup>22</sup> nel quale ha invece ristretto la definizione iniziale, ritenendo necessario distinguere i “sistemi di IA” dai sistemi software più classici<sup>23</sup>. Secondo una nuova formulazione (art. 3, par. 1), sa-

---

rebbe essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici».

<sup>19</sup> Secondo l’Allegato I «Tecniche e approcci di intelligenza artificiale di cui all’articolo 3, punto 1), tali tecniche consistono negli: a) Approcci di apprendimento automatico, compresi l’apprendimento supervisionato, l’apprendimento non supervisionato e l’apprendimento per rinforzo, con utilizzo di un’ampia gamma di metodi, tra cui l’apprendimento profondo (*deep learning*); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione».

<sup>20</sup> Definizione contenuta nell’art. 3, par. 1, proposta.

<sup>21</sup> La definizione è stata ritenuta da alcuni fin troppo ampia e suscettibile di questioni interpretative. Cfr. *Joint letter on the European Commission’s Proposal for an AI Act*.

<sup>22</sup> Consiglio dell’Unione europea – *Orientamento generale* del 25 novembre 2022 – Fascicolo Interistituzionale 2021/0106(COD).

<sup>23</sup> Secondo il considerando n. 6 «La definizione dovrebbe essere basata sulle principali ca-

rebbero ricompresi nei sistemi di IA solo i sistemi sviluppati mediante *approcci di apprendimento automatico e approcci basati sulla logica e sulla conoscenza*<sup>24</sup>.

Nonostante una maggiore chiarezza, anche la nuova definizione potrebbe tuttavia presentare talune criticità<sup>25</sup>. Tra tutte quella di rendere complicata la classificazione dei sistemi a seconda che usino o meno modalità di apprendimento automatico e quella di prestarsi ad elusioni da parte dei programmatori al fine di aggirare la regolamentazione.

Una nozione ampia, purché chiara dei sistemi di intelligenza artificiale sarebbe effettivamente preferibile perché consentirebbe la necessaria elasticità interpretativa. Oltre ad essere più coerente con un approccio europeo sarebbe al contempo in linea con la definizione adottata in seno ad alcune organizzazioni internazionali (tra le quali ad esempio il Consiglio d’Europa o l’Unesco). D’altra parte, come correttamente osservato<sup>26</sup>, a parte i divieti assoluti, solo alcuni sistemi di intelligenza artificiale (quelli ad alto rischio che tuttavia sono la minoranza) sono soggetti a una regolamentazione stringente. Pertanto, il fatto di rientrare in una definizione lata di sistema di intelligenza artificiale non necessariamente comporta l’obbligo di

---

ratteristiche funzionali dell’intelligenza artificiale, quali le sue capacità di apprendimento, ragionamento o modellizzazione, e distinguerla da sistemi software e approcci di programmazione più semplici. In particolare, ai fini del presente regolamento, i sistemi di IA dovrebbero avere la capacità, sulla base di input e dati elaborati dalle macchine e/o dall’uomo, di dedurre come raggiungere una serie di obiettivi finali che sono assegnati a tali sistemi dall’uomo, avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e di produrre output quali contenuti per sistemi di IA generativi (ad esempio testo, video o immagini), previsioni, raccomandazioni o decisioni, che influenzano l’ambiente con cui il sistema interagisce, tanto in una dimensione fisica quanto in una dimensione digitale. Un sistema che utilizza regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico non dovrebbe essere considerato un sistema di IA. I sistemi di IA possono essere progettati per funzionare con livelli di autonomia variabili e per essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato). Il concetto di autonomia di un sistema di IA si riferisce al grado di funzionamento di tale sistema senza il coinvolgimento umano».

<sup>24</sup> La nuova formulazione è la seguente: «“sistema di intelligenza artificiale” (sistema di IA): un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall’uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativi), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce».

<sup>25</sup> Illustrate esaurientemente da A. RENDA, A. ENGLER, *What’s the name? Getting the definition of Artificial Intelligence right in the EU’s AI Act*, in *CEPS Explainer*, 2023.

<sup>26</sup> A. RENDA, A. ENGLER, *What’s the name?*, cit.

rispetto di tutta una serie di oneri specifici, i quali conseguono invece alla classificazione di un dato sistema (dal suo uso e caratteristiche) come ad alto rischio e tale definizione è dettagliata nell'Allegato III che sarà periodicamente rivisto dalla Commissione.

Non va infine dimenticato che una definizione sufficientemente ampia ed elastica lascerebbe inoltre maggiore spazio alla Corte di giustizia per precisare e chiarire di volta in volta taluni profili (e adeguare eventualmente il significato di talune disposizioni e definizioni). L'uniformità di interpretazione (data anche dall'effetto *erga omnes* delle sue pronunce) sarebbe dunque assicurata. Senza tralasciare che un eventuale intervento della Corte avrebbe inoltre effetto pratico perché andrebbe a fornire un ausilio concreto al giudice del rinvio per la soluzione di una determinata controversia.

#### **4. La precisazione del rapporto tra la tutela del mercato e quella dei diritti fondamentali**

La scelta di regolamentare i sistemi di intelligenza artificiale e le modalità in cui questa avviene riflette, in secondo luogo, le peculiarità dell'ordinamento da cui deriva caratterizzandosi a seconda dei casi da una differente tensione tra i valori in gioco e da un diverso bilanciamento tra le esigenze del mercato e dello sviluppo tecnologico, da un lato, e la tutela dei diritti dall'altro.

Una dimensione europea della regolamentazione dei sistemi di intelligenza artificiale presuppone dunque che sia chiaro il rapporto che l'Unione si prefigge di mantenere tra la tutela del mercato interno e la protezione dei diritti fondamentali. È un rapporto tra regola ed eccezione? Quali sono gli spetti che a seconda dei casi devono prevalere? Ed a quale livello?

La Relazione allegata alla proposta di regolamento sembra precisare più compiutamente tale rapporto poiché l'accento non appare primariamente posto sul primo obiettivo, e cioè quello di regolare in maniera uniforme i requisiti tecnici dei sistemi di IA, tenendo *anche* conto dell'obiettivo di rispettare i diritti fondamentali. Al contrario, appare invece ben enfatizzato l'intento di eliminare o minimizzare i rischi per i diritti fondamentali, evitando l'introduzione di requisiti eccessivamente stringenti per le imprese. Dei due obiettivi previsti nel Libro bianco – «promuovere l'adozione dell'IA e affrontare i rischi associati a determinati utilizzi di tale tecnologia» – la proposta «mira ad attuare il secondo obiettivo al fine di sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile». Infatti «L'IA do-

rebbe rappresentare uno strumento per le persone e un fattore positivo per la società, con il fine ultimo di migliorare il benessere degli esseri umani».

È la tutela dei diritti fondamentali a garantire un ecosistema di fiducia e a favorire pertanto lo sviluppo tecnologico ed affidabile dell’IA<sup>27</sup>.

A prescindere dall’effettiva realizzazione di tale auspicio e dalla rispondenza del contenuto della proposta agli obiettivi prefigurati, quel che certamente la proposta sembra far emergere è che la regolazione (del mercato, e cioè dei prodotti e servizi che hanno sistemi di IA) non avviene ‘nel rispetto dei’ diritti fondamentali, bensì ‘per’, o meglio, ‘attraverso’ il prisma dei diritti fondamentali. È il differente diritto o il diverso livello di tutela dei diritti che guida un *risk based approach* consistente nell’imporre ai vari soggetti (utilizzatori, produttori, ecc.) divieti o obblighi tecnico-procedimentali, con gradazione diversa a seconda dei sistemi, dei settori e quindi dello standard di tutela considerato. Attraverso la “procedimentalizzazione” del rischio la tutela del diritto è incorporato *by design* nel sistema di IA.

Tale approccio presuppone (e chiede) necessariamente che lo standard di tutela dei diritti fondamentali sia, nel rispetto della Carta europea, non solo elevato ma soprattutto *uniforme* nell’ordinamento dell’Unione.

Un ulteriore importante obiettivo della dimensione europea è dunque quello di non frammentare, oltre al mercato, la stessa tutela dei diritti, evitando che siano i singoli Stati membri a decidere un diverso *standard* di tutela dei diritti fondamentali nel contesto dell’IA, con il rischio di fughe in avanti di alcuni Stati (divieti assoluti di alcuni sistemi) e indietro di altri (immissione nel mercato di sistemi nocivi per la salute, la vita la dignità delle persone)<sup>28</sup>.

---

<sup>27</sup> Secondo la Commissione «Le regole per l’IA disponibili sul mercato dell’Unione o che comunque interessano le persone nell’Unione dovrebbero pertanto essere incentrate sulle persone, affinché queste ultime possano confidare nel fatto che la tecnologia sia usata in modo sicuro e conforme alla legge, anche in termini di rispetto dei diritti fondamentali. Gli obiettivi espressamente indicati dalla Commissione nella Relazione di accompagnamento alla proposta sono i seguenti: i) assicurare che i sistemi di IA immessi sul mercato dell’Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell’Unione; ii) assicurare la certezza del diritto per facilitare gli investimenti e l’innovazione nell’intelligenza artificiale; iii) migliorare la *governance* e l’applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; iv) facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato».

<sup>28</sup> Per alcuni contributi in dottrina, cfr. 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), *Intelligenza artificiale e diritto: una rivoluzione?*, cit., 127 ss.; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull’intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di) *Intelligenza artificiale e diritto: una rivoluzione?*, cit., 111 ss.

Va inoltre, e infatti, osservato che, in assenza di una regolazione europea, le questioni che giungerebbero alla Corte di giustizia (sulla base del meccanismo di rinvio pregiudiziale) non potrebbero essere dirette a vagliare la compatibilità di normative alla luce della Carta europea (la quale come noto si applica solo nell'ambito del Trattato e non estende le competenze dell'Unione). Sarebbero invece questioni presumibilmente poste (solo) per verificare la legittimità di restrizioni nazionali alla luce delle norme sulla libera circolazione dei servizi o delle merci, nel consueto rapporto dunque di regola (le libertà di circolazione espresse nel TFUE) ed eccezione (la tutela dei diritti fondamentali<sup>29</sup>).

L'ulteriore effetto di un intervento legislativo europeo sarà dunque quello di lasciare la possibilità ai giudici nazionali di utilizzare lo strumento dell'art. 267 TFUE e consentire alla Corte di giustizia di vagliare il nuovo strumento regolatorio alla luce della Carta europea dei diritti sulla quale peraltro esso stesso si fonda. Resterà ovviamente da vedere se la Carta europea sia sufficiente ad esprimere i nuovi 'diritti digitali' (diritto al controllo umano, diritto alla trasparenza algoritmica, ecc.) o se vi sia necessità di un nuovo catalogo di diritti, come prevede la Commissione<sup>30</sup>.

## 5. La dimensione europea dei diritti, l'identificazione *ex ante* di alcuni diritti davvero fondamentali

Il *risk based approach*, nell'evitare, in una dimensione europea, la frammentazione dei diritti oltre che del mercato, presuppone e valorizza un ulteriore elemento: e cioè che sia definita a monte la centralità di uno specifico diritto fondamentale, la sua irrinunciabilità o comunque la sua minore o maggiore rilevanza per un dato settore o per una data applicazione di IA.

Una delle premesse da cui infatti partire per comprendere le ragioni di un intervento regolatorio *ex ante*, è che in presenza di un diritto fonda-

---

<sup>29</sup>Una delle conseguenze sarebbe un presumibile aumento degli interventi da parte delle Corti costituzionali nel caso di ipotetico contrasto delle regolazioni nazionali con i diritti fondamentali del proprio ordinamento. Su altri aspetti Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw journal*, 2019, 63 ss.

<sup>30</sup>Comunicazione della Commissione, relativa alla definizione di una *Dichiarazione europea sui diritti e i principi digitali* del 26 gennaio 2022 (COM(2022)27 e COM(2022)28; per commenti si rinvia a P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in DUE (osservatorio), marzo 2022, 1 ss., nonché E. CELESTE, *Towards a European Declaration on Digital Rights and Principles: Guidelines for the Digital Decade*, in *dcubrexitinstitute.eu*, 7 February 2022).

mentale della persona, il danno che può essere provocato da un uso non calibrato di tali applicazioni (o quanto meno di talune) è in alcuni casi talmente grave da *non* essere in alcun modo riparabile o compensabile *ex post*<sup>31</sup> (considerata peraltro anche l'estrema velocità con la quale si muove lo sviluppo delle nuove tecnologie)<sup>32</sup>.

L'identificazione *ex ante* dei diritti che in un dato ordinamento sono considerati inviolabili e non riparabili rispetto ad altri che possono essere considerati 'cedevoli' è un'operazione ovviamente indispensabile con riferimento ai sistemi che sono considerati con un rischio inaccettabile e dunque vietati.

Come più volte ripetuto nei Considerando della proposta, la dignità della persona, la vita e la salute sono nel diritto dell'Unione europea, considerati irrinunciabili rispetto ad altre esigenze, siano esse di carattere economico, sociale o anche di protezione di altri diritti.

Il nuovo testo proposto dal Consiglio dell'Unione sembra sottolineare con maggior vigore l'essenzialità di taluni diritti, anche a seguito delle critiche che erano giunte sulla proposta e dirette a stigmatizzare un rapporto

---

<sup>31</sup> In tal senso anche C. REED, *How should we regulate artificial intelligence?*, in *Phil. Trans. R. Soc A* 376, 2018; P. NIEMITZ, *Constitutional Democracy and Technology in the age of Artificial Intelligence*, Royal Society Philosophical Transactions, 2018. V. anche il Report *Need for democratic governance of artificial intelligence* 24 September 2020 (Parliamentary Assembly, Council of Europe); e Report CAHAI(2020)23 *Ad hoc Committee on artificial intelligence*, cit. Si pensi infatti ai danni che possono coinvolgere l'integrità fisica (si pensi ad esempio al caso classico delle auto a guida autonoma o alle diagnosi mediche errate o a prodotti difettosi e pericolosi) o psichica di una persona (manipolazioni, valutazioni errate, amministrative o giudiziarie, gravi discriminazioni sulla base dell'appartenenza ad una determinata etnia, mancato beneficio di servizi essenziali, lesione della privacy, bias cognitivi).

<sup>32</sup> La prevenzione del danno corrisponde del resto ad un principio generalmente riconosciuto sia a livello nazionale che internazionale, come infatti dimostra il richiamo che ne fa, nel contesto della regolazione dell'IA, il Consiglio d'Europa Report CAHAI(2020)23 *Ad hoc Committee on artificial intelligence*, cit., «The prevention of harm is a fundamental principle that should be upheld, in both the individual and collective dimension, especially when such harm concerns the negative impact on human rights, democracy and the rule of law. The physical and mental integrity of human beings must be adequately protected, with additional safeguards for persons and groups who are more vulnerable. Particular attention must also be paid to situations where the use of AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens». Anche la Relazione alla proposta spiega che «Gli obblighi di prova *ex ante*, di gestione dei rischi e di sorveglianza umana faciliteranno altresì il rispetto di altri diritti fondamentali, riducendo al minimo il rischio di decisioni errate o distorte assistite dall'IA in settori critici quali l'istruzione e la formazione, l'occupazione, servizi importanti, le attività di contrasto e il sistema giudiziario. Nel caso in cui si verificano comunque violazioni dei diritti fondamentali, un ricorso efficace a favore delle persone lese sarà reso possibile assicurando la trasparenza e la tracciabilità dei sistemi di IA unitamente a rigidi controlli *ex post*» (punto 3.5., p. 13).

in alcuni ambiti eccessivamente sbilanciato a favore delle esigenze dello sviluppo tecnologico e degli interessi del mercato, con l'effetto di sacrificare in particolare, e al di là di alcuni diritti specifici, la *dignità* della persona.

Di esempi ve ne sono parecchi. Tra i tanti, l'estensione del divieto dell'uso di sistemi di punteggio sociale anche per soggetti privati e non solo per le pubbliche autorità (art. 5, par. 1, lett. c); e del divieto dei sistemi che usano tecniche subliminali e manipolatorie non più solo limitato a gruppi di persone in ragione dell'età o della disabilità ma anche della *specifica situazione sociale o economica* (art. 5, par. 1, lett. b).

La necessità di evitare *ex ante* la lesione di diritti fondamentali di primaria importanza (dignità, diritto alla privacy, ecc.), non può inoltre essere riguardata in una dimensione unicamente individuale, ma va anche letta in considerazione dell'interdipendenza dei diritti tra loro, del loro valore per la società nel suo complesso, e dunque della loro inscindibilità dalla tutela della *rule of law* e dei principi democratici di un determinato ordinamento<sup>33</sup>.

«*Human rights, democracy, and the rule of law are closely linked*», così ricorda il Report del Consiglio d'Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law* riprendendo a sua volta quanto ben sintetizzato nella Dichiarazione di Vienna del 1993 «*All human rights are universal, indivisible and interrelated*»<sup>34</sup>.

E dunque, solo per fare qualche esempio<sup>35</sup>, quando è l'algoritmo a decidere come veicolare dati e notizie, è noto che l'impatto si produca sia sui

---

<sup>33</sup> V. anche l'*Explanatory memorandum*, allegato alla proposta di regolamento sull'IA, ove la Commissione precisa «the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society [...] artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law» (considerando 4).

<sup>34</sup> Council of Europe, June 2021 «Human rights, democracy, and the rule of law are closely linked. The capacity of legitimate governments to effectively safeguard human rights is predicated on the interdependence of robust and accountable democratic institutions, inclusive and transparent mechanisms of decision-making, and an independent and impartial judiciary that secures the rule of law. Most generally, human rights are the basic rights and freedoms that are possessed by every person in the world from cradle to grave and that preserve and protect the inviolable dignity of each individual regardless of their race, ethnicity, gender, age, sexual orientation, class, religion, disability status, language, nationality, or any other ascribed characteristic. These fundamental rights and freedoms create obligations that bind governments to respecting, protecting, and fulfilling human rights. In the absence of the fulfilment of these duties, individuals are entitled to legal remedies that allow for the redress of any human rights violations».

<sup>35</sup> Si vedano in particolare e più diffusamente i Report e gli Studi del Consiglio d'Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law* (a Primer), June 2021; *Towards Regulation of AI systems* (December 2020); *Ad hoc Committee on artificial intelligence*,

diritti del singolo (corretta informazione) che sui principi democratici, influenzando i processi elettorali<sup>36</sup> o favorendo la creazione di nuovi modelli sociali e politici anche a causa della concentrazione di potere solo in alcune piattaforme digitali. Lo stesso dicasi per i sistemi di riconoscimento biometrico che possono condurre, oltre alla violazione della privacy o di dati personali, anche ad una sorveglianza di massa, con rischi di autoritarismo o assunzione di decisioni restrittive allo scopo di controllare le proteste o anche di prevederle (e quindi evitare che si svolgano). La mancanza di anonimato può inoltre scoraggiare i cittadini a una libera manifestazione del pensiero, a una partecipazione attiva nella società e ad esprimere opinioni e giudizi<sup>37</sup>. Decisioni che vengano elaborate attraverso sistemi di IA possono minare sia il diritto del singolo a veder tutelati i propri interessi che i principi *rule of law* nella misura in cui incidano sull’indipendenza del giudice<sup>38</sup>, così come sulla partecipazione ai processi di *decision making*, o sul buon andamento e trasparenza della pubblica amministrazione. Analisi predittive e le valutazioni da parte di enti creditizi, datori di lavoro o anche pubbliche autorità possono erodere i diritti civili e al contempo creare di-

---

Feasibility Study, 17 December 2020 (CAHAI (2020) 23); *Study on the impact of Digital transformation on Democracy and good governance*, 26 July 2021.

<sup>36</sup> Sul punto si veda anche l’Opinion No. 974/2019, *European Commission for Democracy through Law (Venice Commission), Principles for a fundamental Rights-compliant Use of Digital Technologies in electoral Processes* – approved by Council of Democratic Elections at its 70th online meeting (10 December 2020) and adopted by the Venice Commission at its 125th online Plenary Session (11-12 December 2020).

<sup>37</sup> V. il considerando n. 18 alla proposta secondo cui: «L’uso di sistemi di IA di identificazione biometrica remota “in tempo reale” delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto è ritenuto particolarmente invasivo dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbe avere ripercussioni sulla vita privata di un’ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l’esercizio della libertà di riunione e di altri diritti fondamentali. L’immediatezza dell’impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all’uso di tali sistemi che operano “in tempo reale” comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone oggetto di attività di contrasto».

<sup>38</sup> Sul punto v. anche la Comunicazione della Commissione *Digitalizzazione della giustizia nell’Unione europea Un pacchetto di opportunità*, 2 dicembre 2020 COM(2020)710 final. In dottrina cfr. F. DONATI, *Intelligenza artificiale giustizia*, in *Rivista AIC*, n. 1/2020, 415 ss. Si ricorda inoltre la *Carta etica europea sull’uso dell’intelligenza artificiale nei sistemi giuridici e negli ambiti connessi*, del 3 dicembre 2018; cfr. al riguardo, tra gli altri, A. PAJNO, *L’uso dell’intelligenza artificiale nel processo tra problemi nuovi e questioni antiche*, in *Astrid Rassegna*, n. 18/2021; M. LIBERTINI, M.R. MAUGERI, E. VINCENTI, *Giustizia predittiva e giurisdizione civile. Primi appunti*, in *Astrid Rassegna*, n. 16/2021; U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell’intelligenza artificiale*, Torino, 2021.

scriminazioni all'interno della società *targettizzando* gruppi di persone sulla base dell'età, etnia, lingua, ecc.

Si tenga peraltro presente che tali principi potrebbero essere violati anche nel caso in cui non si sia verificata una specifica lesione nel caso singolo. L'erronea attribuzione di un beneficio sociale, a seguito di un funzionamento non corretto di un sistema di IA, a favore di un cittadino che non avrebbe i requisiti per ottenerlo, non viola nel caso specifico alcun diritto individuale ma lede certamente il principio del buon andamento dell'amministrazione<sup>39</sup>. Può inoltre accadere che non vi sia a livello individuale un'esatta percezione della lesione (o che la percezione sia addirittura assente) che invece ha rilievo se riguardata a livello collettivo. Si pensi alla sorveglianza di massa o alla disinformazione sulle piattaforme digitali.

Poiché la lesione che sistemi di intelligenza artificiale possono cagionare ai diritti fondamentali può essere particolarmente elevata e soprattutto in grado di minare direttamente i principi democratici e la *rule of law*, emerge dunque in maniera del tutto chiara la valutazione di rischio inaccettabile che presentano alcuni sistemi di IA in ragione dell'interesse pubblico (europeo) sotteso<sup>40</sup> e dunque della centralità del valore tutelato a livello collettivo rispetto ad altre esigenze.

---

<sup>39</sup>V. anche *Getting the Future – Artificial Intelligence and Fundamental rights*, cit., 28, il quale ad esempio precisa che «A public agency combatting hate crime uses an AI-based tool to detect online hate speech by analysing patterns of speech online. On the basis of the processing, the system determines which social groups are targeted. This helps law enforcement adopt measures to protect them before threats are realised. Although the tool aims to identify potential victims, rather than perpetrators, law enforcement can use the information generated by the system to ask social media providers for information on users to pursue criminal investigations» (p. 36).

<sup>40</sup>Il regolamento persegue una serie di motivi imperativi di interesse pubblico «quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali (Considerando 1). L'intelligenza artificiale può nel contempo, a seconda delle circostanze relative alla sua applicazione e al suo utilizzo specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale». Sull'interesse pubblico nella regolazione dell'IA, sulla sua definizione, sui differenti approcci e soluzioni, anche nei diversi contesti in cui operano i sistemi di IA, cfr. in dottrina G. GANTZIAS, *Dynamics of Public Interest in Artificial Intelligence: 'Business Intelligence Culture' and Global Regulation in the Digital Era*, in S.H. PARK et al. (eds), *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, Hellenic Open University, Patras Greece, 2021, 259 ss.; A. DIGNAM, *Artificial intelligence, tech corporate governance and the public interest regulatory response*, in *Cambridge Journal of Regions, Economy and Society*, 2020, 37 ss., secondo cui «The biggest challenge lies not in identifying the problems with AI and its controllers but the public governance response»; N. ELKIN-KOREN, *Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence*, in *Big Data and Society*, 2020, 1 ss.

## 6. Il necessario bilanciamento *ex ante* tra i vari diritti

Dall’esame del contenuto della proposta, il *risk based approach* conduce tuttavia anche un altro tipo di operazione, non limitato ad un bilanciamento tra il diritto fondamentale e lo sviluppo dell’IA. Poiché i sistemi di IA possono invece anche dare un notevole contributo alla stessa tutela e rafforzamento dei diritti<sup>41</sup> (si pensi all’uso di tale tecnologia per le diagnosi sanitarie<sup>42</sup> o per la ricerca di persone scomparse o semplicemente per una maggiore trasparenza nelle selezioni, nell’adozione di decisioni amministrative o giurisdizionali, ecc.), la valutazione che il rischio che tali sistemi possono produrre per altri diritti fondamentali può essere bilanciato con i benefici che è in grado di generare per gli stessi diritti.

Ai fini dell’immissione nel mercato o dell’uso di un sistema di IA la valutazione del connesso rischio di violazione di un diritto fondamentale va dunque svolta, in taluni casi, mediante il bilanciamento tra più diritti fondamentali e non tra i diritti, da un lato, e le esigenze del mercato.

Poiché la prevalenza di un diritto sull’altro dipende, anche in tal caso, dal rilievo che un dato ordinamento attribuisce ad un determinato diritto, la proposta rispecchia evidentemente le caratteristiche e specificità dell’ordinamento europeo.

Solo per fare un esempio, il rischio inaccettabile che pone un sistema di riconoscimento biometrico *in real time* da parte delle autorità pubbliche a fini di contrasto (e quindi il suo divieto) e la definizione comunque ad alto rischio di tale sistema se ‘a posteriori’, esprime la scelta di dare priorità al diritto fondamentale della vita privata e della tutela dei dati personali (di

---

<sup>41</sup> Si veda quanto espresso nella Relazione alla Proposta di regolazione dell’IA: «Definendo una serie di requisiti per un’IA affidabile e di obblighi proporzionati per tutti i partecipanti alla catena del valore, la presente proposta migliorerà e promuoverà la protezione dei diritti tutelati dalla Carta: 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). Essa mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione (articolo 11) e 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. La presente proposta inciderà inoltre positivamente, secondo quanto applicabile in determinati settori, sui diritti di una serie di 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 l’inserimento delle persone con disabilità (articolo 26). Rilevante è anche il diritto a un livello elevato di tutela dell’ambiente e al miglioramento della sua qualità (articolo 37), anche in relazione alla salute e alla sicurezza delle persone».

<sup>42</sup> Per alcuni spunti, cfr. in dottrina, C. DE COSTANZO, *Access to intensive care and Artificial Intelligence. A Constitutional Perspective*, in *Italian Journal of Public Law*, n. 2/2021, 494 ss.

qui la base giuridica anche dell'art. 16 TFUE oltre che dell'art. 114 TFUE) rispetto al diritto alla sicurezza, che potrebbe essere garantito da una generale attività di sorveglianza di massa per fini di contrasto del crimine. La Corte ha già infatti stigmatizzato, come contrarie al diritto dell'Unione e alla Carta dei diritti, le attività di raccolta e la conservazione generalizzata e indifferenziata di dati personali per finalità di sicurezza nazionale<sup>43</sup>.

Qualora però il sistema sia finalizzato alla ricerca *mirata* di potenziali vittime di reato, alla prevenzione di minacce di attacchi terroristici o all'azione penale di cui alla decisione quadro 2002/584/GAI del Consiglio<sup>44</sup>, il diritto alla vita privata e alla tutela dei dati personali (ed anche alla dignità) cede invece dinanzi a minacce all'integrità fisica delle persone. Conformemente a consolidati orientamenti, la compressione di tale diritto è dunque giustificata solo quando strettamente indispensabile al perseguimento di un obiettivo legittimo (quale può essere la vita e la sicurezza di altre persone) e limitata nel tempo<sup>45</sup>.

Da notare inoltre, l'ampliamento dei casi in cui la modalità in *real time* (a tutela dei diritti fondamentali) può essere effettuata, secondo l'ultima versione del testo. La minaccia (da prevenire) non deve necessariamente essere *imminente* e non si limita alla "vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico" ma è estesa al *l'infrastruttura critica delle persone fisiche* e alla *salute*. Valori quest'ultimi evidentemente ritenuti anch'essi prioritari rispetto ad altri diritti della persona.

Criticità maggiori erano invece emerse in riferimento all'uso dei *deepfake*. Ci si era infatti chiesti<sup>46</sup> come mai l'uso di tali sistemi, che il Parlamento

---

<sup>43</sup> V. ad esempio, Corte giust., 6 ottobre 2020, cause 511/18, 512/18 e C-520/18, *La Quadrature du Net French Data Network Fédération des fournisseurs d'accès à Internet associatifs*, e causa C-623/17, *Privacy International*, concernenti il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche.

<sup>44</sup> Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, *relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri* (G.U. L 190 del 18 luglio 2002, p. 1).

<sup>45</sup> Si veda anche la posizione del Parlamento europeo e il comunicato del 22 marzo 2022 secondo cui «The draft text also stresses that AI technologies could pose crucial ethical and legal questions. It highlights the challenge of reaching a consensus within the global community on minimum standards for the responsible use of AI, and concerns about military research and technological developments into lethal autonomous weapon systems. MEPs say that certain AI technologies enable the automation of information processing to an unprecedented scale. This paves the way for mass surveillance and other unlawful interference and poses a threat to fundamental rights, in particular the rights to privacy and data protection. Authoritarian regimes apply AI systems to control, exert mass surveillance and rank their citizens, or restrict freedom of movement. Dominant tech platforms use them to obtain more information on a person. Such profiling poses risks to democratic systems as well as to the safeguarding of fundamental rights, say MEPs».

<sup>46</sup> Sia consentito rinviare a C. SCHEPISI, *Intelligenza artificiale tra Diritti fondamentali, principi democratici e rule of law: quale ruolo e quali responsabilità per gli Stati nella regolazione*

europeo aveva suggerito di limitare al massimo in quanto altamente lesivi (della dignità, del diritto all’informazione)<sup>47</sup>, fossero invece considerati sistemi a rischio lieve, soggetti dunque solamente ad un obbligo informativo.

Per di più tale obbligo sarebbe caduto non solo qualora l’uso fosse autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati, ma anche quando fosse *necessario per l’esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell’UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi*. A differenza pertanto di altri sistemi indicati sempre dall’art. 52 (i sistemi che interagiscono con le persone – i c.d. *chabot* – i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica) in riferimento ai quali la deroga all’obbligo informativo era prevista solo (e più correttamente) nei casi autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, nel caso dei *deepfake* la libertà di espressione (e la libertà delle arti e scienze) sarebbe prevalsa dunque, secondo una valutazione *ex ante*, sugli altri diritti considerati dalla norma. Tale previsione tuttavia appariva stridere con la centralità riservata dall’Unione al diritto alla dignità della persona e alla protezione dei diritti democratici<sup>48</sup>, e con l’approccio adottato recentemente in altri contesti pa-

---

*dell’intelligenza artificiale*, in *Studi sull’integrazione europea*, n. 1/2022, 41 ss., e in F. DONATI, PAJNO, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Il Mulino, Bologna, 2022, 203 ss.

<sup>47</sup> V. la Risoluzione del Parlamento europeo 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)). Al punto 76, il Parlamento «esprime profonda preoccupazione per le tecnologie di *deepfake*, che consentono di produrre foto, audio e video falsificati sempre più realistici che potrebbero essere utilizzati per compiere ricatti, creare notizie false o minare la fiducia dei cittadini e influenzare il dibattito pubblico; ritiene che tali pratiche siano in grado di destabilizzare paesi, diffondere la disinformazione e influenzare le consultazioni elettorali; chiede pertanto l’introduzione di un obbligo in base al quale tutti i materiali *deepfake* o altri video artificiali realizzati in modo realistico debbano essere etichettati come “non originali” dal loro creatore, con severi limiti al loro utilizzo a fini elettorali, e che tale obbligo sia applicato rigorosamente; chiede che siano svolte adeguate attività di ricerca in questo campo per garantire che le tecnologie di contrasto dei suddetti fenomeni siano al passo con gli utilizzi dolosi dell’IA».

<sup>48</sup> V. anche la bozza di Risoluzione del PE del novembre 2021; il PE «Illustrates that AI technologies could also help perpetrators by simplifying the use of very sophisticated cyberattacks, such as through AI-powered malware, identity theft using biometric data or adversarial AI that causes other AI systems to misinterpret input; points, in particular, to the rise in deepfakes, which already lead to doubts about the authenticity of all digital content, including genuinely authentic videos; warns that deepfakes could contribute to a broad climate of public mistrust in AI, as well as a deeper socio-political polarisation within our societies». In linea generale l’approccio del-

ralleli (come ad esempio nell'ambito del *Digital Services Act*<sup>49</sup>). E pertanto non appariva in linea con un corretto bilanciamento tra i vari diritti in gioco secondo quello che era l'orientamento europeo.

Il nuovo testo viene parzialmente incontro a tale criticità restringendo i casi in cui l'obbligo informativo verrebbe meno. La deroga è infatti prevista «se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati” o se il contenuto *fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico o fittizio*, fatte salve le tutele adeguate per i diritti e le libertà dei terzi». Dunque, secondo il compromesso raggiunto in seno al Consiglio, i fornitori e utenti di sistemi di IA come *deep fake* sono esonerati da obblighi informativi solo qualora sia chiaramente e manifestamente evincibile la manipolazione di immagini e contenuti audio per le finalità di cui sopra.

Nella stessa direzione, e dunque operando un nuovo bilanciamento tra i diritti, il nuovo testo elimina inoltre dall'elenco dall'Allegato III, riferito ai sistemi di IA considerati ad alto rischio, «i sistemi destinati a essere utilizzati dalle autorità di contrasto per individuare i “deep fake” di cui all'articolo 52, paragrafo 3».

La proposta è in ogni caso ancora in discussione e potrebbe essere suscettibile di modifiche. Quel che tuttavia preme in tale sede evidenziare è che laddove la norma sia vaga e il margine sia sufficientemente ampio da consentire un bilanciamento *ex post* (eventualmente anche da parte della Corte di giustizia), ne verrebbe forse meno la certezza del diritto in termini di classificazione di un sistema come vietato o ad alto rischio e dunque l'efficacia dello stesso *risk based approach* ma lascerebbe spazio ad eventuali correzioni ed evoluzioni interpretative. Al contrario, qualora la norma sia eccessivamente dettagliata, il bilanciamento tra i diritti già svolto *ex ante*

---

l'Unione appare discostarsi da quello statunitense. Il primo, nel porre al centro la dignità della persona, porta ad esempio a ritenere cedevole la libertà di espressione e informazione se ciò comporta la diffusione di *hate speeches*, *fake news* attraverso le piattaforme digitali; il secondo, invece, ritiene che la libertà di espressione non possa in alcun modo essere limitata e censurata dal pubblico potere e si affida pertanto all'autoregolazione da parte delle stesse piattaforme.

<sup>49</sup> Il Parlamento europeo aveva ad esempio proposto un emendamento al considerando n. 63 (pubblicità nelle piattaforme), ritenendo fosse necessario l'etichettatura di “*qualsiasi file video, audio o di altro tipo di cui sia nota l'origine deepfake*”, unitamente all'inserimento di un nuovo art. 30 bis, secondo cui «Qualora una piattaforma online di dimensioni molto grandi si renda conto di contenuti deepfake, ossia di immagini o contenuti audio o video generati o manipolati che presentano una notevole somiglianza con persone, oggetti, luoghi o altre entità o eventi reali e che sono tali da falsamente apparire autentici o veritieri, il prestatore etichetta tali contenuti in modo da informare in maniera chiaramente visibile per il destinatario dei servizi che si tratta di contenuti non autentici».

rischia di non lasciare spazio a correzioni e dunque presuppone che tale bilanciamento sia svolto con la massima attenzione.

## 7. L’aspetto procedurale europeo: la scelta della base giuridica e della misura da adottare

La finalità di tutela (anche) dei diritti fondamentali perseguito dalla proposta di regolazione dell’IA non scalfisce in ogni caso la correttezza della scelta della base giuridica dell’art. 114 TFUE, peraltro arricchita dal riferimento anche all’art. 16 TFUE (che consente alle istituzioni di adottare atti a tutela dei dati personali). Resta fermo infatti il carattere strumentale dell’intervento rispetto all’obiettivo del mercato interno, né si sarebbero potute percorrere altre vie. L’art. 2 TUE, ad esempio, non legittima l’adozione di atti da parte delle istituzioni, mentre l’art. 19 TFUE oltre ad avere un profilo limitato al principio di non discriminazione non costituirebbe un’idonea base giuridica in ragione della procedura legislativa speciale prevista nella stessa norma<sup>50</sup>.

L’opzione di adottare un regolamento, piuttosto che una direttiva, ricalda inoltre quella già effettuata con GDPR<sup>51</sup> nonché con le più recenti adozioni o proposte di altri atti normativi (DGA, DMA, DSA, ecc.), anche essi sulla base dell’art. 114 TFUE.

In tutti i casi citati, compreso il regolamento sull’IA, si tratta tuttavia di regolamenti che lasciano un certo spazio di discrezionalità agli Stati membri. Il ricorso al regolamento, dettato dall’esigenza di adottare una disciplina del tutto uniforme nel territorio dell’Unione europea rende pertanto la differenza con lo strumento della *direttiva* sostanzialmente molto labile.

È pur vero, da un lato, che il requisito della diretta applicabilità del regolamento non implica automaticamente che le norme in esso contenute siano tutte immediatamente applicabili o dotate di efficacia diretta<sup>52</sup>. La

---

<sup>50</sup> In questo senso cfr. 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) *La rivoluzione dell’intelligenza artificiale: profili giuridici*, Il Mulino, Bologna, in corso di pubblicazione 2022, al cui contributo si rinvia per approfondimenti sul punto.

<sup>51</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR).

<sup>52</sup> Cfr. ex multis, L. DANIELE, *Diritto dell’Unione europea*, Milano, 2020, 291; R. ADAM, A. TIZZANO, *Manuale di Diritto dell’Unione europea*, Torino, 2017, 171-172.

complessità che a volte tali atti presentano (pensiamo proprio al regolamento *privacy*) può rendere necessaria l'adozione di misure di integrazione, esecuzione, accompagnamento al fine di rendere concretamente operativo il suo funzionamento<sup>53</sup>. E questo è certamente anche il caso del regolamento sull'IA.

Tuttavia, e dall'altro lato, la necessità da parte degli Stati membri, di precisare e integrare le varie disposizioni del regolamento assume nel caso specifico una portata non indifferente.

A parte alcune disposizioni di carattere sostanziale, un importante ambito di discrezionalità riguarda la struttura di *governance* che gli Stati dovranno predisporre a livello nazionale, e la funzione di controllo e di sanzione.

Il regolamento prevede infatti (art. 59) che ogni Stato membro provveda a designare l'autorità competente a livello nazionale «al fine di garantire l'applicazione e l'attuazione del presente regolamento» e che agisce «in qualità di autorità di notifica e di autorità di vigilanza del mercato»<sup>54</sup>. Lo Stato dovrà garantire l'obiettività e l'imparzialità dei suoi compiti dell'autorità e che questa disponga di risorse finanziarie e umane adeguate per svolgere i loro compiti<sup>55</sup>.

Senza voler entrare nel dettaglio dei meccanismi di funzionamento e di *governance* della futura autorità, quello che in questa sede preme solo sottolineare è la particolare attenzione che il regolamento dedica alla dovuta e necessaria autonomia, indipendenza, professionalità<sup>56</sup>, requisiti che devono essere garantiti dallo Stato e sui quali esso è tenuto a vigilare in maniera particolarmente attenta<sup>57</sup>. È inoltre indubbio, data la molteplicità delle di-

---

<sup>53</sup> Corte giust., 26 febbraio 2008, causa C-132/05, *Commissione c. Germania*; 11 febbraio 2001, causa C-403/98, *Monte Arcosu*.

<sup>54</sup> Il regolamento lascia aperta la doppia opzione di indicare due autorità o invece di concentrare nella medesima autorità entrambe le competenze. Inoltre la Commissione suggerisce che possa essere designata anche un'autorità già esistente

<sup>55</sup> La norma prevede che «Gli Stati membri riferiscono annualmente alla Commissione in merito allo stato delle risorse finanziarie e umane delle autorità nazionali competenti, con una valutazione della loro adeguatezza. La Commissione trasmette tali informazioni al comitato affinché le discuta e formuli eventuali raccomandazioni».

<sup>56</sup> Cfr. sul punto anche E. CHITI, B. MARCHETTI, N. RANGONE, *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni: prove generali*, cit.; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, cit.; M. ANZINI, *The Artificial Intelligence Act Proposal and its implications for Member States*, in *EIPA Briefing* 2021/5.

<sup>57</sup> V. anche il Report CAHAI(2020)23 *Ad hoc Committee on artificial intelligence*, cit., 46; Report *Need for democratic governance of artificial intelligence* 24 settembre 2020 (Report – Parliamentary Assembly, Council of Europe), e la successiva risoluzione n. 2341/2020; nonché *Presiden-*

scipline applicabili anche a medesimi operatori, che i componenti e lo staff di tali autorità dovranno anche essere in grado di coordinare il loro operato anche con quello di altre autorità o organismi<sup>58</sup>. Non va infatti sottaciuto il rischio che gli operatori possano essere soggetti ad obblighi tra di loro in contrasto, con l'ulteriore rischio di una lesione di alcuni diritti fondamentali<sup>59</sup>.

L'autorità di vigilanza (unitamente agli organismi notificati), potrà avere un ruolo particolarmente importante nel controllo *ex post* e dunque nelle sanzioni. Ed anche sotto tale profilo lo Stato (e il legislatore nazionale) gode, da un lato, di una certa discrezionalità. Lo Stato dovrà innanzitutto decidere quale autorità sia deputata a infliggerle, inclusa la possibilità di attribuire tale compito ai tribunali, specie se queste abbiano natura penale. Esso resta inoltre libero di stabilire che le sanzioni possano infliggersi anche alle autorità pubbliche (come anche previsto dal regolamento *privacy*)<sup>60</sup>. Sarà poi anche compito dello Stato stabilire l'ammontare delle stesse. Il regolamento si limita, e solo per alcune tipologie, a stabilire gli importi minimi e massimi, o in termini assoluti o con valori percentuali. Per il resto, e in coerenza con i principi generali, viene richiesto che le sanzioni siano effettive, proporzionate e dissuasive (art. 71)<sup>61</sup>. Va da sé che lo Stato dovrà dunque ben ponderare l'esigenza che le sanzioni siano sufficienti a dissuadere gli operatori dal violare il regolamento, ma al contempo è tenuto a garantire che le stesse, specie laddove siano qualificabili come penali<sup>62</sup>, siano anche sorrette da tutte le garanzie richieste dalla CEDU e dalla Carta europea dei diritti (compreso il principio del *ne bis in idem*).

---

*cy Conclusions of the Council of the European Union, The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 21 October, 2021; EDPB, GEPD, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, del 18 giugno 2021.

<sup>58</sup> EDPB, GEPD, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, del 18 giugno 2021.

<sup>59</sup> Sotto tale profilo va ovviamente auspicata (*in primis* a livello di Unione) la coerenza e completezza dell'intero quadro normativo applicabile agli operatori che prestano servizi digitali *Joint Letter on the European Commission's Proposal for an AI Act*.

<sup>60</sup> Un terzo ambito è la predisposizione di spazi di sperimentazione normativa per l'IA (art. 53).

<sup>61</sup> Per alcuni approfondimenti si rinvia a V.C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3/2021, 415 ss.

<sup>62</sup> Cfr. A. LAVORGNA, G. SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Dir. pen. contemporaneo*, 2/2021, 88 ss.

Il margine di discrezionalità che pertanto il regolamento lascia agli Stati soprattutto dal punto di vista del controllo e dell'*enforcement* (ai quali si aggiungono compiti di coordinamento con gli organismi europei) è dunque certamente molto ampio e sotto tale profilo la sfida sarà sia in termini di efficienza (ed efficacia) della nuova struttura nazionale sia di coordinamento con altre autorità che, infine, di rigoroso rispetto dei principi del giusto processo e di garanzia di rimedi giurisdizionali. Tenuto conto della numerosità degli adempimenti cui è tenuto lo Stato (e della necessaria precisazione degli stessi), va da sé che anche la misura del regolamento non implicherà, in questo specifico caso, una totale identità di disciplina tra uno Stato e l'altro. Quel che è certo è che il ricorso allo strumento del regolamento corrisponde in ogni caso ad una modalità sempre più seguita dalla Commissione nel settore digitale, tenuto conto delle implicazioni tecniche che questo comporta.

Fa ovviamente eccezione la recente scelta di proporre una direttiva sul connesso tema della responsabilità da intelligenza artificiale<sup>63</sup> – anch'essa con base giuridica sull'art. 114 TFUE – perché relativa ad un ambito – la responsabilità civile e il risarcimento del danno – nel quale l'Unione europea non ha competenze specifiche e può solo procedere all'armonizzazione delle regole nazionali.

## 8. Profili conclusivi

La proposta presentata dalla Commissione, ancora migliorabile in alcune sue parti, rappresenta un progetto di ampia portata poiché investe in maniera trasversale tutti i settori e si fonda su un difficile e complesso bilanciamento tra le esigenze del mercato e la tutela dei diritti fondamentali, nonché tra gli stessi diritti. La dimensione europea di tale regolamentazione è tangibile sotto più punti di vista. Del resto la disciplina sull'intelligenza artificiale – per le implicazioni che comporta sia in termini di mercato che di tutela dei diritti fondamentali – non può che rispecchiare fedelmente i valori dell'Unione.

Va inoltre considerato che la sfida che l'Unione si pone non è solo quella di diventare leader mondiale nello sviluppo di un'intelligenza artificiale, ma anche quella di imporre un elevato *standard* di diritti fondamentali. L'oc-

---

<sup>63</sup> Proposta di direttiva *relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)*, del 28 settembre 2022, COM(2022)496 final.

casione è dunque quella di generare un nuovo ‘effetto Bruxelles’<sup>64</sup>, come già avvenuto per il regolamento privacy e che rivestirà particolare importanza proprio per la tutela o esportazione di principi democratici e della *rule of law*. Il fatto che via sia una condivisione tra i valori della proposta europea e quelli del Consiglio d’Europa faciliterà ad esempio e senz’altro tale compito<sup>65</sup>. Ma l’Unione dovrà saper imporre il suo sistema di valori (che include un corretto bilanciamento tra tutti i diversi interessi in gioco) anche in contesti internazionali ulteriori cercando di “imporre” i suoi *standard* e riuscirà a farlo solo se la regolamentazione che sarà alla fine adottata sarà davvero chiara, uniforme, e con una dimensione tipicamente europea.

Ricordiamo infatti che quest’ultimo ha già preannunciato l’adozione di una convenzione, obbligatoria per gli Stati membri, per dare seguito alla Risoluzione del 2020 il cui titolo ben sintetizza il suo auspicio: *Need for democratic governance of AI*<sup>66</sup>.

---

<sup>64</sup> F. DONATI *Verso una nuova regolazione delle piattaforme digitali*, in rivista della regolazione dei mercati, n. 2/2021, 238 ss.

<sup>65</sup> In ambito europeo i punti in comune tra Consiglio d’Europa e Unione europea sono infatti numerosi ponendosi entrambe le organizzazioni l’obiettivo di uno *standard* particolarmente elevato nella tutela dei diritti fondamentali, dei principi democratici e della *rule of law* Report del Consiglio d’Europa *Artificial Intelligence, Human rights, democracy, and the Rule of Law* (a Primer), June 2021; *Towards Regulation of AI systems* (December 2020); *Ad hoc Committee on artificial intelligence*, Feasibility Study, 17 December 2020 (CAHAI (2020) 23); *Study on the impact of Digital transformation on Democracy and good governance*, 26 July 2021; *Artificial Intelligence in the audiovisual sector*, European Audiovisual Observatory, 2020.

<sup>66</sup> Risoluzione n. 2341/2020, *Need for democratic governance of AI*, del 22 ottobre 2020. Tra le altre Risoluzioni adottate v. risoluzione n. 2343/2020 *Preventing discrimination caused by the use of artificial intelligence*, del 22 ottobre 2020; Risoluzione n. 2345/2020 *Artificial intelligence and labour markets; friends or foe?*, del 22 ottobre 2020.



Alberto M. Gambino

## Piattaforme, IA e data sharing: premessa

L'invisibile filo che lega piattaforme, IA e data sharing si chiama algoritmo. Un algoritmo, non solitario, che opera abitualmente in interazione con le tracce umane abbandonate dagli utenti nella quotidiana navigazione delle reti<sup>1</sup>. È la profilazione<sup>2</sup>, tecnica di trattamento automatico, mediante algoritmi appunto, di tipologie di dati relativi a elementi personali per attribuirne un profilo, così da definire categorie e parametri funzionali alla ricerca e al raggiungimento dello scopo degli utenti; il *target* è studiato considerando abitudini di consumo, stili di vita che ne rivelano attitudini e capacità di spesa, gusti per alcuni prodotti o servizi e disinteresse per altri, caratteristiche legate all'identità personale. La dinamica che consente la creazione della categoria specifica prevede un sistema di aggregazione in *clusters*, che avviene tramite l'incrocio e l'associazione di alcuni dati personali degli utenti con le informazioni elaborate mediante algoritmo, di natura geografica, socio-demografica, economica.

Una vera e propria lente di ingrandimento. Quanto più il *cluster* risulta individuato nel dettaglio, tanto più le informazioni possono essere rivelatrici degli aspetti sensibili della vita dei soggetti profilati. La dottrina più avveduta sintetizza tale vicenda coll'espressione "potere informativo"<sup>3</sup>.

L'utilizzo di sistemi di IA nei servizi della società dell'informazione rivela, dunque, criticità legate al potenziale rischio anticoncorrenziale: il mi-

---

<sup>1</sup> Efficace l'espressione "società delle piattaforme" coniata da P. STANZIONE, *Introduzione*, in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, 1. Cfr., anche, il pensoso bel lavoro di E. CATERINI, *L'Intelligenza artificiale "sostenibile" e il processo di socializzazione del diritto civile*, Napoli, 2020.

<sup>2</sup> Per le tipologie della profilazione si rimanda a A.M. GAMBINO, A. STAZI, D. MULA, *Diritto dell'Informatica e della Comunicazione*, 3<sup>a</sup> ed., Torino, 2019, 106 ss.

<sup>3</sup> In tema v. *amplius* R. GIORDANO, A. PANZAROLA, A. POLICE, M. PROTO (a cura di), *Il diritto nell'era digitale*, Milano, 2022; cfr. anche il filo conduttore dei saggi contenuti in D. POLETTI, A. MANTELERO (a cura di), *Governare la tecnologia*, Pisa University Press, Pisa, 2018.

gliore degli algoritmi si rapporta alla ingente quantità di dati a propria disposizione e alla conseguente capacità di dominare il mercato<sup>4</sup>. La digitalizzazione delle attività produttive e distributive aziendali, che nasce dalla convergenza tra *Information Technology* e *Operational Technology* – nella prassi indicata come Industria 4.0, fabbrica digitale o *smart manufacturing* – si configura, nella *vulgata* tecnocratica – quale principale strumento di crescita per l'economia.

Eppure, proprio in tema di abuso di posizione dominante, l'Antitrust europeo ha fronteggiato, negli ultimi anni, vicende che hanno messo alla prova il diritto con ripensamenti sui temi riguardanti il mercato rilevante e l'individuazione del potere di mercato e del suo abuso<sup>5</sup>. Il contesto competitivo offerto dagli operatori che concorrono nel mercato IT, costringono a confrontarsi quotidianamente con una realtà, già a suo tempo definita come “caleidoscopica”<sup>6</sup>.

Tecnicamente la piattaforma rientra fra quelli che vengono definiti “*two-sided market*”, e dunque oggetto di indagine antitrust sia per quanto riguarda la concorrenza con altri *player* di comparazione e ricerca, sia per quanto riguarda la concorrenza con aziende pubblicitarie. La stessa piattaforma si trova, poi, in diretta competizione con gli aggregatori di notizie e i *social network*.

Il potere di mercato si individua generalmente nel nesso tra l'ingente volume di dati detenuto da un'impresa e la capacità dei sistemi di IA di cui si dispone<sup>7</sup>, ma il problema si sta progressivamente eradicando dal profilo della raccolta di enormi quantità di dati, per trasferirsi ai profili meno in-

---

<sup>4</sup> Si rinvia allo studio arioso e completo di M. DELMASTRO, A. NICITA, *Big Data: come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019 e, si consenta, anche il rinvio a A.M. GAMBINO, M. MANZI, *L'intelligenza artificiale tra protezione del consumatore e tutela della concorrenza*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 325 ss. Cfr. MAYER, V. SCHÖNBERGER, K.N. CUKIER, *Big Data*, Mariner Books, New York (USA), 2013 (trad. in italiano *Big Data*, Garzanti, Milano); cfr. MAYER, V. SCHÖNBERGER, T. RAMGE, *Reinventing Capitalism in the Age of Big Data*, Basic Books, New York, 2018 (trad. in italiano *Reinventare il capitalismo nell'era dei big data*, Egea, Milano); cfr. M. MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018; V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the “big data revolution”*, in *Conc. merc.*, 2016, 39 ss.; G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Dir. inf.*, 2015, 909 ss.

<sup>5</sup> Si veda F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, 1064 ss.

<sup>6</sup> Cfr. P. SABBATINI, *Il caso Microsoft*, in *Moneta e credito*, n. 207, 1999, 349-350.

<sup>7</sup> Cfr. R. ANGELINI, *Intelligenza artificiale e governance. Alcune riflessioni di sistema*, 301, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di F. Pizzetti et al., Torino, 2018.

dagati dell'utilizzo di sofisticati strumenti di IA di analisi per astrarre valore, trasformando i dati in conoscenza.

Che l'utilizzo dell'IA non rilevi in termini di solo dibattito *antitrust*, ma consti di una realtà ben più insidiosa, concreta e ineludibile, lo fanno intendere le dinamiche giuridico-normative sottese alle fattispecie che empiricamente emergono nel mercato digitale. La prospettiva concorrenziale la c.d. “*algorithmic accountability*” si in strada, difatti, nello scenario applicativo degli artt. 101 e 102 TFUE, i quali, come noto, non presentano alcuna menzione dell'elemento psicologico come requisito perché si configuri un illecito antitrust<sup>8</sup>. Nell'ottica Antitrust, i tradizionali profili della nozione di imputabilità dell'illecito comportano l'attribuzione diretta alle imprese delle condotte “autonome” poste in essere dagli algoritmi, anche ove non si rilevino moventi programmatici a monte finalizzati a porre in essere condotte anticoncorrenziali<sup>9</sup>. Le imprese non sono, cioè, sottratte alla loro responsabilità attraverso lo schermo dell'operato degli algoritmi e ciò in forza anche del parametro dell'ordinaria diligenza che comprende la prevedibilità congenita degli effetti delle pratiche governate da algoritmi e la conoscibilità dei loro meccanismi di funzionamento<sup>10</sup>.

Non sfugge, però, che tale itinerario finisca per mal celare, data l'irrilevanza, anche taluni profili soggettivi, in senso schiettamente civilistico, di moventi e motivi sottostanti alla programmazione algoritmica delle IA.

Così, gli algoritmi, pur con la loro capacità di influenzare condizioni di mercato, da un lato, godono di “buona stampa” in quanto idonei a favorire, ad esempio, la trasparenza dei prezzi e ad incentivare interazioni economiche “utili” per il consumatore, nonché, per le imprese, riescono a rendersi fattori necessari alla difesa e alla reazione rapida e precisa alle azioni dei concorrenti<sup>11</sup>; ad un *meeting of minds*, in altri termini, si an-

---

<sup>8</sup> Cfr. L. CALZOLARI, *op. cit.*, 15; cfr. M.E. STUCKE, *Is Intent Relevant?* (26 gennaio 2012), in 8 *J. L. Econ. & Pol'y* 801 (2012), *University of Tennessee Legal Studies Research Paper* No. 178. Disponibile al sito internet: SSRN: <https://ssrn.com/abstract=1992761> or <http://dx.doi.org/10.2139/ssrn.1992761>, 802 ss.

<sup>9</sup> Cfr. OECD, *Algorithms and collusion – Note from the European Union* (2017), 14 June 2017, DAF/COMP/WD (2017)12, 7.

<sup>10</sup> Cfr. M. VESTAGER, *Algorithms and competition*, Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2017, disponibile al sito internet: [https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en).

<sup>11</sup> Cfr. V. FALCE, G. COLANGELO, *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Il Mulino, Bologna, 2017; cfr. V. FALCE, G. OLIVIERI (a cura di), *Big Data e Concorrenza nei mercati dell'innovazione*, Milano, 2017.

drebbe a sostituire un *meeting of algorithms* e occorrerà verificare se piuttosto non si prospetti una nuova forma di collusione tacita algoritmica, particolarmente difficile da individuare.

Allo stesso tempo, però, la crescente profilazione dei consumatori, nel delineare una vera e propria identità digitale, al contempo permette di determinare in maniera puntuale e precisa il loro *status* economico, utile a valutare il relativo potere d'acquisto e il conseguente prezzo-soglia oltre il quale l'utente presumibilmente non si spingerà. Così attraverso sistemi di apprendimento automatico<sup>12</sup> (*machine learning*), proliferano vere e proprie *black box* che inducono a prospettare forme discriminatorie<sup>13</sup> tanto da parte dei loro architetti, quanto da parte di chi ne faccia materialmente utilizzo<sup>14</sup>.

In questo scenario si iscrive la proposta di regolamento UE sull'Intelligenza Artificiale pubblicata dalla Commissione europea il 21 aprile 2021 che detta norme e divieti rispetto all'integrazione di algoritmi sofisticati e meccanismi di intelligenza artificiale all'interno dei modelli di *business* che aumentano il rischio di un accrescimento esponenziale del potere tecnologico<sup>15</sup> funzionale al *market power*. Ancora più specifico è il DMA (Digital Markets Act) che, insieme al Digital Services Act (DSA) andrà comporre il quadro regolatorio.

Il modello di *business*, dunque, non sta nell'acquisizione dei dati personali di un singolo utente, ma nell'aggregazione dei dati di una «folla» di utenti. Il gap informativo, il non innocente meccanismo dell'*opt-out* ne sono gli strumenti abilitanti.

Nell'accesso ad un *social*, la circolazione «utile» sta nella ritrasmissione del dato dall'operatore verso quelle aziende che, componendo la platea degli utenti e affinandone gusti e comportamenti, sono in grado di mirare il *marketing* direttamente verso i soggetti potenzialmente interessati a prodotti e servizi, così abbattendo i costi di una campagna pubblicitaria tradizionale che non possieda *target* così puntuali.

---

<sup>12</sup> Cfr. K. KERSTING, U. MEYER, *From Big data to Big artificial intelligence?*, in SPRINGER, *KI – Künstliche Intelligenz* (2018) 32:3-8 <https://doi.org/10.1007/s13218-017-0523-7>, 3.

<sup>13</sup> Cfr. L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, (23 May 2017), in 16 *Duke Law & Technology Review* 18 (2017), 19, disponibile al sito internet: <https://ssrn.com/abstract=2972855>.

<sup>14</sup> Cfr. OECD, *Algorithm and Collusion – Background Note by the Secretariat* (2017), DAF/COMP (2017)4, 21-23 June 2017, 51.

<sup>15</sup> Con una certa ariosità, il tema del potere tecnologico è affrontato nello studio di matrice etico-filosofico di L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale*, Roma, 2020, *passim*.

L'inquadramento giuridico della fase dell'accesso alla piattaforma con l'utente ignaro che consegna elementi utili al business delle società di marketing, segnala la reale dimensione economica del fenomeno, rilevandone la prospettiva «massiva» di relazioni singole che assumono compiuta e decisiva rilevanza giuridica solo nella fase della cessione a terzi del dato, del suo riutilizzo nell'orizzonte più ampio della protezione del consumatore; con un *caveat* però: che la sua libertà di scelta non ha solo contenuto economico.

Sul piano strettamente giuridico, secondo la prospettiva della *circolazione*, non circola certo il dato ma la posizione giuridica cui si riferisce quel dato<sup>16</sup>.

La premessa corretta per affrontare compiutamente la rilevanza giuridica di Piattaforme, IA e data sharing richiede di concentrarsi su chi governa la posizione giuridica sottesa al dato: esattamente in questo crocicchio emerge un'interazione tutta da esplorare, plasticamente incarnata dalle giurisdizioni settoriali dell'autorità Antitrust, della giustizia amministrativa e, poi, del Garante per la protezione dei dati personali, senza dimenticare l'Autorità Giudiziaria Ordinaria.

Le fonti-atto segnano le competenze: l'utilizzo dei servizi social postula, a monte, un contratto<sup>17</sup> e, dunque, una fase prenegoziale, per quanto repentina e fugace, che implica informazioni e comunicazioni rivolte all'utente. Sempre.

Ancora più monte della fase negoziale ci sono le libertà, le scelte individuali, il consenso ad aprire le porte della propria sfera personale. Beni di rango sovraordinato: allora la fonte-atto dell'accesso alle piattaforme web non può essere soltanto un accordo preceduto da un coacervo di informazioni spesso commerciali non idonee a dedurre nel loro oggetto beni per natura e per scelta di sistema non suscettibili di essere trattati come patrimonio economico.

Cruciale è perciò la prospettiva soggettivo-informativa. Nel segmento spazio-tempo della decisione dell'utente, attratto ad entrare nel web, dovrebbe allora stagliarsi vivido ed efficace il suo catalogo dei diritti e dei doveri, ma non con minuziose e sfuggenti sottoscrizioni, quanto piuttosto con regole ferree che consacrino l'intangibilità delle tracce che l'utente lascia

---

<sup>16</sup> Il tema della circolazione è affrontato con contributi ben radicati nella materia GDPR in A.M. GAMBINO, A. STAZI (a cura di), *La circolazione dei dati*, Pisa, 2020, *passim*.

<sup>17</sup> Cfr., due lavori, che colgono in maniera diversa le metamorfosi delle dichiarazioni negoziali a cospetto della *data society*: A. QUARTA, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2022.

agli altri naviganti, salvo che se ne formuli un chiaro consenso legittimante. Ciò vale sia per lo scenario antitrust, sia nell'ambito del consenso della protezione dei dati personali, sia, infine, nel contesto del rapporto strettamente negoziale: uno *spatium cogitandi* unificante di istituti giuridici distinti.

Soltanto principi e norme «prudenti» atti a recuperare consapevolezza e pienezza percettiva dei modelli economici di mercato nel web ne riducono le insidie; si pensi in definitiva allo scenario dei minori<sup>18</sup> e a vicende che vanno ad intaccare l'integrità psichica e fisica della persona umana.

---

<sup>18</sup> In tema di tutela dei minori, v., da ultimo, il volume di E. ANDREOLA, *Minori e incapaci in Internet*, Napoli, 2019.

Roberto Bocchini

# La rilevanza economica delle piattaforme digitali tra sfide ed opportunità pro-concorrenziali

SOMMARIO: 1. La ricerca. – 2. La rilevanza economica delle piattaforme. – 3. La necessità di ricorrere ad una regolazione organica delle piattaforme. – 4. Spunti di riflessione.

## 1. La ricerca

Le piattaforme digitali sono state, oramai da diversi anni, ampiamente scelte dai consumatori per i loro servizi innovativi e l'efficienza nel soddisfare le esigenze quotidiane acquisendo un potere economico immanente per influenzare i mercati, le dinamiche competitive e il benessere stesso dei consumatori<sup>1</sup>. Come confermato anche dall'ultimo report 2022 dell'AGCOM le incredibili economie di scala e di varietà determinano la necessità di disciplinare il “vero mercato” in modo economicamente efficiente tutelando

---

<sup>1</sup>La rilevanza nel mercato digitale dei *gatekeepers* quali principali attori che svolgono una funzione trainante che può essere paragonata per la loro forza a quella di organismi sovranazionali indipendenti e potentissimi impone di immaginare la necessità di controllare questo potere con l'impiego del diritto internazionale e del diritto transnazionale delineando un nuovo paradigma affidato alla *soft law* (F. BASSAN, *Digital platform and Global Law*, Egea, 2022). Al contempo una diversa ricostruzione può portare ad immaginare che gli stessi *gatekeepers* devono da un lato essere controllati dalle Autorità indipendenti tramite degli *audit* periodici ed al contempo devono essi stessi diventare controllori del sistema ed infatti il regolamento UE 2022/1925 (DMA) prevede all'art. 25 che qualora nel corso dei procedimenti a norma dell'art. 18 il *gatekeeper* interessato offra di assumersi impegni relativi ai pertinenti servizi di piattaforma di base tali da garantire l'osservanza degli obblighi sanciti dagli artt. 5, 6 e 7, la Commissione può adottare un atto di esecuzione che rende tali impegni vincolanti per tale *gatekeeper* e dichiarare che il proprio intervento non è più giustificato. Tale atto di esecuzione è adottato secondo la procedura consultiva di cui all'art. 50, par. 2. Ci si avvia verso un meccanismo per il quale i controllati devono diventare anche controllori in un meccanismo sinergico di forze.

i diritti degli utenti dai servizi nel rispetto dell'innovazione tecnologica e della condivisione dei servizi nel mondo digitale<sup>2</sup>.

La ricerca che abbiamo avviato<sup>3</sup> è sempre stata progettata in modo interdisciplinare anzitutto con gli economisti secondo un metodo di *Law and economics*, ma che deve interagire almeno con i filosofi, gli statistici e gli ingegneri, i cui studi sono fondamentali per un corretto approccio allo studio delle Piattaforme digitali le “nostre” E-AGORÀ in quanto i profili giuridici ed economici non possono essere disgiunti dalla conoscenza dei meccanismi tecnici che sovrintendono le piattaforme con i loro algoritmi e per poter anzitutto comprendere con gli ingegneri il meccanismo tecnico che regola il sistema perché anche la normativa segue la particolarità tecnica del sistema e mai come per questa materia vale il principio *ex facto oritur ius* secondo un'interdisciplinarietà dello studio molto proficua nell'approfondimento di un *novum organum* secondo un metodo Baconiano.

E non da meno appare fondamentale l'approfondimento dell'insieme dei principi, delle idee e delle convinzioni sui quali una persona o un gruppo di persone fondano la propria concezione della vita in quanto la stessa concezione della vita sociale cambia con l'utilizzo estremo delle piattaforme digitali che non diventano più un mero strumento come tanti altri, ma permeando le vite, specialmente dei più giovani, ne determinano comportamenti ed idee diverse dai più anziani che, ad ogni modo, convivono con la *vita telematica*<sup>4</sup>. In tal senso è necessario individuare in apice i giusti valori da tutelare attraverso le norme che devono riequilibrare la disparità di forze economiche in campo.

Senza prendere aprioristicamente posizione sul fine della norma tra co-

---

<sup>2</sup> A. IANNOTTI DELLA VALLE, *La tutela della concorrenza ai tempi di google android tra fondamenti costituzionali e analisi tecnologica*, in *Riv. dir. inf.*, 2021, 283.

<sup>3</sup> Il presente contributo si pone all'interno della Progetto di Ricerca di Rilevante Interesse Nazionale 2020 che ha ottenuto il finanziamento dal MUR dal titolo “E-Agorà – Online Platforms Contracts. Economic efficiency and rights' protection of service users. Technological innovation and service sharing in a social world” con le Università di Napoli Parthenope (capofila), Università Europea di Roma, Università Cattolica del Sacro Cuore di Milano, Università di Verona ed Università di Perugia.

<sup>4</sup> M. AINIS, *L'autorità antitrust alla prova dei mercati digitali*, in *Dir. inf. ed informatica*, 2022, 1, secondo cui “Siamo nel tempo dell'algocrazia. Governati da un tiranno che non è un omaccione in divisa bensì una formula, un algoritmo. E l'algoritmo ci dispensa opportunità e vantaggi, però anche dei pericoli. Sulla qualità della vita democratica (camere dell'eco, infodemia, fake news, hate speech), ma anche sul versante dell'economia, sulla concorrenza economica. È necessario disciplinare il potere senza compromettere l'innovazione di cui le piattaforme sono il vero volano”.

loro i quali sostengono che essa deve tutelare valori<sup>5</sup> e coloro che, seguendo Kelsen<sup>6</sup>, sostengono che la norma è una pura decisione politica che non tutela valori, tale termine viene qui utilizzato nel suo senso semantico e letterale e, quindi, come *ratio legis* della decisione politica. Invero la *funzione della digitalizzazione* diventa una lente di ingrandimento dalla quale guardare il mercato delle piattaforme e che deve attraversare orizzontalmente il fenomeno nei suoi molteplici profili.

## 2. La rilevanza economica delle piattaforme

I principali mercati dove le piattaforme digitali operano sono soggetti a pervasive esternalità di rete, sia a) dirette (dette anche economie di scala dal lato della domanda), sia b) indirette (dette anche incrociate).

L'intero meccanismo si basa su un patrimonio immenso: i dati e la loro registrazione gratuita basata su diversi fondamenti che componendo un patrimonio dell'umanità, generato dall'umanità, dovrebbe essere anche redistribuito all'umanità che lo produce in una enorme fabbrica invisibile in cui le persone lavorano senza saperlo, o ad una enorme borsa invisibile in cui le persone producono valore senza saperlo<sup>7</sup>.

In ragione delle esternalità dirette, un aumento della base utenti della piattaforma comporta, con alta probabilità, un aumento della disponibilità a pagare di ciascun utente.

Tuttavia, in ragione delle esternalità indirette ciò non implica necessariamente un aumento del prezzo per l'adesione dell'utente finale alla piattaforma. Infatti, in molti casi, per ottenere il maggior numero di utenti possibile, i *matchmaker* possono introdurre strategie di prezzo (monetario) uguale a zero in un versante del mercato, indipendentemente dal loro potere di mercato e contrattuale, così da aumentare i ricavi nell'altro versante così come i ricavi complessivi.

Come notato correttamente nella dottrina specialistica<sup>8</sup>, rendimenti di scala crescenti, economie di varietà, esternalità di rete indirette e dirette tendono a determinare un aumento del livello di concentrazione nei mercati delle piattaforme digitali, che nella maggior parte dei casi sono soggetti

---

<sup>5</sup> Per tutti v. R. DWORKIN, *I diritti presi sul serio*, 1977, trad. da F. Oriana, ult. rist., Bologna, 2010.

<sup>6</sup> H. KELSEN, *La dottrina pura del diritto*, 1934, a cura di M.G. Losano, ult. rist. Torino, 2021.

<sup>7</sup> M. FERRARIS, *Documanità. Filosofia del mondo nuovo*, Bari, 2021, *passim*.

<sup>8</sup> A. MANGANELLI, *Il regolamento Eu per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in *Merc. conc. reg.*, 2021, 475.

a un fenomeno noto come *tipping*: una volta che una piattaforma raggiunge una certa massa critica l'aumento di scala della piattaforma si autoalimenta e rinforza a causa degli effetti di rete e del crescente costo-opportunità di uscita, che spingono verso una continua espansione della rete di utenti, potenzialmente fino a una situazione in cui un singolo operatore rimane monopolista nel mercato.

Questa situazione – in mancanza di interoperabilità esterna – rappresenta un intralcio assai difficile da affrontare per i concorrenti, effettivi e potenziali, che dovrebbero superare la massa critica esistente per potersi affermare e competere in modo sostenibile sul mercato<sup>9</sup>. È infatti estremamente arduo superare i costi di coordinamento collettivi per gli utenti che dovrebbero spostarsi insieme per ridurre il loro costo-opportunità unilaterale.

Nonostante questo scenario, lo sviluppo di politiche pubbliche di regolazione delle piattaforme digitali non è stato un processo né facile, né lineare. Innanzitutto, i mercati digitali sono stati oggetto di un approccio regolamentare intenzionalmente prudente, finalizzato alla minimizzazione del rischio di un intervento sbilanciato che potesse ostacolare l'innovazione.

La motivazione economica di un approccio regolatorio prudenziale trova, tuttora, fondamento sul fatto che le *Big Tech*, nonostante il loro potere economico, possano comunque essere sottoposte a un'adeguata pressione concorrenziale, soprattutto potenziale, in mercati dove le dinamiche competitive si strutturano principalmente in una concorrenza per il mercato. In altri termini, il potere di mercato nel mondo digitale esiste ma è intrinsecamente temporaneo, poiché le imprese «dominanti» sono soggette a spiazzamenti schumpeteriani da parte di nuovi entranti più innovativi, similmente a quanto accaduto in passato per Myspace, rimpiazzato da Facebook, Yahoo da Google, Netscape da Microsoft Explorer, per non parlare adesso dell'ormai prossimo Metaverso di Meta/Facebook<sup>10</sup>.

### **3. La necessità di ricorrere ad una regolazione organica delle piattaforme**

La soluzione a volte adottata di una «autoregolamentazione supervisionata» non sembra rappresentare, tuttavia, uno strumento efficace – anche

---

<sup>9</sup> A. MANGANELLI, *op. cit.*, 476.

<sup>10</sup> Per un primo inquadramento dei problemi giuridici v. G. CASSANO, G. SCORZA (a cura di), *Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT*, Pisa, 2023.

in ragione della mancanza di poteri ispettivi e di controllo sulle piattaforme, sui loro algoritmi di funzionamento<sup>11</sup>, sui flussi di raccolta, aggregazione e utilizzo dei dati, che in ultima analisi avrebbero consentito di verificare l'impatto delle regole private.

L'applicazione del diritto della concorrenza ha assunto la guida dell'intervento pubblico, in ragione della sua flessibilità applicativa e della sua capacità di adattarsi a nuove circostanze di mercato, in quanto basato su principi generali che vengono declinati e contestualizzati nella loro applicazione *ex-post*.

Nonostante il crescente numero di casi a livello EU ed anche a livello nazionale (che hanno anche portato a sanzioni record – vedi il caso tedesco Facebook 2018<sup>12</sup> e l'italiano Amazon 2021<sup>13</sup>) l'applicazione del diritto della concorrenza nei mercati digitali è, tuttavia, percepita da molti come non completamente adeguata a limitare il potere di mercato ed economico delle piattaforme: troppo lenta rispetto alle dinamiche di mercato ed efficace solo per evidenti casi di esclusione in cui una piattaforma dominante sfrutta il proprio potere di mercato su un altro mercato (a valle o a monte).

Inoltre, la definizione dei mercati rilevanti si è sempre rivelata piuttosto problematica, data la natura conglomerale degli intermediari, attivi tra più mercati e più versanti, e le caratteristiche peculiari delle transazioni economiche digitali<sup>14</sup>.

L'ampiezza del tema è evidente rispetto ad un'analisi che non può essere completa, tuttavia possono essere individuati<sup>15</sup> tre elementi principali relativi all'economia delle piattaforme:

a) le transazioni digitali si basano sullo scambio implicito di dati per servizi a basso costo o gratuiti in un contesto di mercato a più versanti;

b) i dati raccolti consentono un incremento costante di efficienza delle piattaforme e degli algoritmi, sì da comprendere e adeguarsi alle preferen-

---

<sup>11</sup> Si veda F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. il caso « mevaluate»*, in *Dir. Inf. ed informatica*, 2021, 1005.

<sup>12</sup> Per una recente ricostruzione della vicenda v. F. LAVIOLA, *Il diritto all'autodeterminazione informativa tra concorrenza e data protection. Riflessioni a margine della saga Facebook vs. Bundeskartellamt nella giurisprudenza delle Corti tedesche ed in attesa della Corte di Giustizia*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali*, Torino, 2022, 27 ss.

<sup>13</sup> Consultabile in [https://www.agcm.it/dotcmsdoc/allegati-news/A528\\_cbiusura%20istruttoria.pdf](https://www.agcm.it/dotcmsdoc/allegati-news/A528_cbiusura%20istruttoria.pdf).

<sup>14</sup> M. BOURREAU, A. DE STREEL, *Digital Conglomerates and Eu Competition Policy*, in *Cerre Policy Paper*, 2019, 20 ss.

<sup>15</sup> M. DELMASTRO, A. NICITA, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019.

ze dei consumatori, anche minimizzando i loro costi di transazione e di ricerca;

c) l'informazione di mercato non è più perfettamente osservabile da tutti come avviene nei mercati in concorrenza e viene (di fatto) internalizzata e sfruttata dalle grandi piattaforme per «diventare il mercato»<sup>16</sup>.

Su questi presupposti fin dall'inizio il Digital Markets Act specifica esplicitamente che gli obiettivi da perseguire riguardano l'equità (*fairness*) e la contendibilità dei mercati digitali<sup>17</sup> che non sono formalmente definite nell'art. 2, lasciando qualche ambiguità nella loro interpretazione.

Nella parte introduttiva del regolamento si afferma «Le pratiche sleali e la mancanza di contendibilità creano inefficienze nel settore digitale in termini di prezzi più alti, qualità inferiore, minore scelta e minore innovazione, a scapito dei consumatori europei».

Il riferimento all'efficienza potrebbe suggerire il tentativo di stabilire una relazione tra gli obiettivi del DMA e quelli tradizionali della politica della concorrenza (surplus dei consumatori, efficienza allocativa).

Uno dei pilastri fondativi della proposta di DMA è la stretta necessità di un intervento eurounitario che, applicando il principio di sussidiarietà (art. 5 TFEU), contrasti gli effetti indesiderati nei mercati in cui operano le grandi piattaforme digitali in quanto «gli Stati membri applicano, o intendono applicare, norme nazionali divergenti».

Nel rispetto del principio di proporzionalità dell'azione europea (art. 5 TFEU), la proposta si concentra solo sui servizi digitali maggiormente utilizzati dagli utenti commerciali e dagli utenti finali, definiti «servizi di piattaforma di base» (o più significativamente: *Core Platform Services* – CPS), nei quali attualmente – secondo la Commissione – vi sono i più evidenti timori di una scarsa contendibilità e di pratiche sleali da parte dei *gatekeeper* (art. 1.2 DMA).

Le misure regolamentari del DMA sono espressamente limitate ai CPS, individuati puntualmente dal suo art. 2: a) servizi di intermediazione *online*, b) motori di ricerca *online*, c) *social network*, d) servizi di piattaforma per la condivisione video, e) servizi di comunicazione elettronica interpersonale indipendenti dal numero, f) sistemi operativi, g) servizi di *cloud computing* e h) servizi di intermediazione pubblicitaria, erogati da un fornitore di uno dei servizi di piattaforma di base elencati alle lettere precedenti.

---

<sup>16</sup> Così A. MANGANELLI, *op. cit.*, 479.

<sup>17</sup> L'art. 1 stabilisce: «Il presente regolamento stabilisce norme armonizzate volte a garantire che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (controllori dell'accesso) siano equi e contendibili in tutta l'Unione».

Ai sensi dell'art. 17 possono essere tuttavia aggiunti nuovi servizi a seguito di un'indagine (o meglio analisi) di mercato.

Un aspetto essenziale della regolazione dei mercati digitali è, quindi, l'identificazione dei *gatekeeper*, attività questa affidata in maniera esclusiva alla Commissione e rivista almeno ogni tre anni, anche sulla base delle notifiche che i fornitori di CPS hanno l'obbligo di effettuare se raggiungono i limiti quantitativi (artt. 3, 4 e 15).

Il DMA contiene un elenco di diciotto obblighi imposti ai *gatekeeper* designati, che disciplinano quattro principali aree, ovvero:

- a) uso e accesso ai dati;
- b) interoperabilità;
- c) interazioni degli utenti business con i *gatekeeper*, da un lato, e con i consumatori finali, dall'altro; e
- d) maggiore consapevolezza degli utenti finali.

Alcuni di essi, ai sensi dell'art. 5, sono applicabili senza ulteriori specificazioni, mentre altri, ai sensi dell'art. 6, sono «suscettibili di essere ulteriormente specificati» a seguito di un «dialogo normativo» tra il *gatekeeper* e la Commissione.

Tutti gli obblighi sono comunque direttamente applicabili, in quanto il DMA qualifica quei comportamenti, se posti in essere dai *gatekeeper* dei CPS, come «*particolarmente iniqui o dannosi*» senza nessun bisogno di ulteriore analisi caso per caso.

Secondo questa architettura regolatoria, la definizione dei criteri per identificare i *gatekeeper*, oltre a definirne il numero, acquista un rilevante significato economico: difatti, l'immediata applicabilità degli obblighi che conseguono alla qualificazione di un operatore come *gatekeeper* perimetra l'estensione dell'intrinseco fallimento di mercato (definendo la necessità di un rimedio *ex ante*).

Gli obblighi comportamentali del DMA rappresentano un complemento al diritto vigente dell'UE (e quello interno degli Stati membri) in materia di concorrenza.

I primi, infatti, contrastano le pratiche sleali e anticoncorrenziali dei *gatekeeper* che non sono contemplate dalla disciplina della concorrenza o che da essa non possono essere disciplinate in modo efficace.

Nei considerando della proposta di regolamento DMA si afferma infatti che il «regolamento persegue un obiettivo complementare, per quanto non analogo, alla protezione della concorrenza non falsata su un dato mercato, quale definita in termini di diritto della concorrenza, e tale obiettivo consiste nel garantire che i mercati in cui sono presenti *gatekeeper* siano e rimangano equi e contendibili, indipendentemente dagli effetti reali, probabili o presunti sulla concorrenza in un dato mercato del comportamento di un dato *gatekeeper* contemplato dal presente regolamento. Il presente re-

golamento mira, pertanto, a proteggere un interesse giuridico diverso rispetto a tali norme e non dovrebbe pregiudicarne l'applicazione».

Questa dichiarata diversità di obiettivi sembra in evidente contrasto con la motivazione alla base dello sviluppo della proposta di regolamento: se la regolazione del DMA è necessaria in ragione dell'insufficienza della disciplina antitrust (azioni c.d. *stand-alone*), gli obiettivi del DMA e della disciplina antitrust devono essere quantomeno convergenti, se non lo stesso.

La complementarità, infatti, non risiede negli obiettivi, ma negli strumenti normativi utilizzati per raggiungere un obiettivo convergente – esattamente come avviene nei settori regolati in modo pro-concorrenziale, quali le telecomunicazioni.

La *ratio* del DMA è di introdurre una serie di obblighi che abbiano un impatto cumulativo sulla contestabilità e l'equità dei mercati digitali, i cui specifici fallimenti del mercato sono affrontati in modo sistemico, generale ed astratto, indipendentemente dagli effetti reali, probabili o presunti sulla concorrenza in un dato mercato del comportamento di un dato *gatekeeper* contemplato dal regolamento.

Per entrambi i motivi parte della dottrina<sup>18</sup> e dei portatori di interessi nel mercato sostengono la necessità di introdurre nel DMA una verifica di efficienza e proporzionalità della regolazione, sia in termini di a) una difesa *ex post* (tuttavia questo contravverrebbe all'obiettivo della Commissione di velocizzare i processi), oppure sotto la forma di b) una propedeutica analisi di impatto della regolazione, svolta in termini di analisi costi-benefici, finalizzata ad inserire nel DMA solo quegli obblighi che hanno un effetto positivo sul benessere complessivo<sup>19</sup>.

Si possono, tuttavia, rilevare due principali aspetti problematici di questo approccio di «codificazione» dei procedimenti antitrust nei mercati digitali (che non erano presenti negli altri mercati).

Primo, non vi è una giurisprudenza del tutto consolidata, sia per il circoscritto lasso di tempo in cui si è sviluppato, sia per il fatto che alcuni casi cui si può fare riferimento sono ancora in corso e nessuna delle pertinenti decisioni di infrazione della Commissione riguardante le grandi piattaforme *online*, tutte oggetto di ricorso, è stata ancora confermata da parte di entrambe le Corti europee<sup>20</sup>.

---

<sup>18</sup> 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*, 1, 2022.

<sup>19</sup> A. MANGANELLI, *Il regolamento Eu per i mercati digitali*, cit., 484.

<sup>20</sup> Sull'importanza, in particolare, del ruolo della Corte di Giustizia nell'opera di bilanciamento di interessi dell'UE e interessi dei singoli v. M. RABITTI, *Il ruolo della Corte di Giustizia nel diritto dell'economia*, in *Analisi giur. ec.*, 2018, 347 ss., spec. 358 ss.

Il secondo elemento è il più rilevante: mentre tutti gli operatori in mercati regolati in maniera pro-concorrenziale attraverso una codificazione della giurisprudenza antitrust (come le telecomunicazioni) sono assai simili, al contrario, una completa armonizzazione dei rimedi *ex-ante* tra i diversi CPS ed i diversi soggetti identificati come *gatekeeper* potrebbe rivelarsi decisamente complessa<sup>21</sup>.

In relazione agli strumenti di applicazione appare evidente che aprendo il DMA al *private enforcement* a differenza delle limitate competenze attribuite alle autorità nazionali garanti della concorrenza i tribunali nazionali hanno pieni poteri per applicare le disposizioni degli artt. 5, 6 e 7. Questo si teme però possa creare un rischio di frammentazione. In tal senso la prevista *class action* di cui all'art. 42 sulle azioni rappresentative promosse contro le violazioni da parte dei *gatekeeper* delle disposizioni del presente regolamento che ledono o possono ledere gli interessi collettivi dei consumatori rappresenta una porta attraverso la quale la tutela degli utenti non passa più solo per le strette e tecniche maglie delle Autorità nazionali, ma permette un'apertura verso le più ampie indagini da parte dei soggetti che operano nella rete.

Appare, inoltre, necessario un maggior coordinamento del DMA con alcuni dei principali atti normativi europei di regolazione, tra cui il codice delle comunicazioni elettroniche, per quanto riguarda i fornitori di servizi di comunicazione interpersonali indipendenti dal numero; la direttiva per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori digitali (c.d. direttiva Omnibus) e gli atti normativi sulla tutela dei dati, in particolare il regolamento generale sulla protezione dei dati (GDPR) ed il *Data governance Act* (DGA).

In assenza di interoperabilità, per superare gli effetti di rete, una scala minima di utenti complessivi deve trasferire i propri dati su una nuova piattaforma. Ciò richiede una costosa e faticosa attività di coordinamento per la gestione di un'uscita collettiva degli utenti da un *gatekeeper* (o anche solo una contrattazione collettiva in merito a un'eventuale uscita: ciò che è rilevante per esercitare un'efficace pressione concorrenziale dal lato della domanda).

Questa necessità delinea un possibile ruolo pro-concorrenziale per nuove piattaforme digitali, intermediari e/o aggregatori di dati di terzi, che per conto degli utenti potrebbero ridurre i costi di questa azione di coordinamento, sfruttando le caratteristiche economiche di efficienza produttiva ed allocativa delle piattaforme.

---

<sup>21</sup> A. MANGANELLI, *Il regolamento Eu per i mercati digitali*, cit., 485, il quale fa, inoltre, notare che i mercati digitali non sono un settore o un'industria e i soggetti operanti possono essere molto eterogenei.

Questi nuovi attori di intermediazione nel mercato dei dati sarebbero operatori terzi, cioè verticalmente non integrati e non attivi in altri versanti del mercato digitale regolato (Cps), e potrebbero aggregare gli utenti, che agendo nel mercato vanno a controbilanciare il potere economico e contrattuale delle piattaforme.

Il DMA chiarisce che spetta ai *gatekeeper* garantire che l'osservanza degli obblighi previsti dal regolamento avvenga nel pieno rispetto di altre normative dell'UE, come quella sulla protezione dei dati personali e della privacy o sulla tutela dei consumatori, senza tuttavia definire meccanismi e modalità specifiche di coordinamento.

#### 4. Spunti di riflessione

I *gatekeepers* che controllano il “mondo digitale” si muovono in un contesto di Internet decisamente differente rispetto a come il Web è nato e si è consolidato nel corso degli ultimi anni.

Quella attuale è l'era delle piattaforme che si basa su una rete che opera «*over the top*» per mezzo di *cloud* centralizzati e servizi che hanno piena disponibilità e controllo dei dati personali<sup>22</sup>.

Il DMA modella il proprio intervento su tale concezione di Web e non sembra guardare alle nuove sfide tecnologiche del 5G e dell'Internet of Things che mirano ad un Web differente e più aperto e ciò fa sorgere alcuni interrogativi.

In primo luogo la crescita esponenziale dei dati generati dall'Internet of Things muteranno il panorama globale e forse lo stesso DMA andrà in qualche modo aggiornato.

Inoltre ci si chiede come si fa a garantire in concreto l'esigenza di interoperabilità generalizzata degli algoritmi e di accesso ai dati<sup>23</sup>.

Ed infine l'ultima riflessione forse andrebbe fatta con riferimento alle future scelte europee di politica del diritto: per garantire e migliorare la contendibilità dei mercati digitali saranno sufficienti le tradizionali politiche pubbliche oppure sarà meglio procedere attraverso una modalità di co-regolazione che coinvolga le piattaforme digitali?

---

<sup>22</sup> M. POLO, A. SASSANO, *Dma: Digital Markets Act o Digital Markets Armistice?*, in *Merc. conc. reg.*, 2021, 529, i quali ritengono che “*in questa architettura i dati raccolti rimangono nella disponibilità della piattaforma, accelerano la dinamica di rafforzamento della sua posizione dominante e costituiscono una barriera all'entrata*”.

<sup>23</sup> Il recente Data Act offre spunti interessanti in tal senso ma forse non è ancora sufficiente.

**Guido Stazi**

## **Piattaforme e dati: una prospettiva concorrenziale**

Vorrei innanzitutto parlare del PRIN 2020 E-Agorà-Online Platform Contracts; a me sembra veramente importante questo nuovo approccio interdisciplinare alla ricerca accademica. Negli anni Ottanta ero ricercatore universitario e ricordo che, a presidio e finanziamento della ricerca di base, in ogni disciplina accademica, c'erano i piani di ricerca del CNR. Che erano molto settoriali e difesi come fortini dalle singole specialità accademiche ed era quindi quasi del tutto assente un confronto interdisciplinare. Invece, come è stato anche sottolineato da chi mi ha preceduto, la multidisciplinarietà, la convergenza di competenze è fondamentale e ormai imprescindibile nell'avanzamento del sapere.

Lo è ancora di più nel campo di cui oggi ci occupiamo, quello delle grandi piattaforme digitali che, tramite l'intelligenza algoritmica, processano quantità enormi di dati; e per questa via hanno costruito un modello di business che ha impresso alla rivoluzione digitale un percorso inaspettato rispetto al modello, quasi anarchico, di internet immaginato dal suo inventore Tim Berners-Lee. Siamo ormai in presenza non più e non solo di piattaforme digitali, ma di ecosistemi digitali. Cioè di mondi a parte, protetti da giardini murati come dicono negli USA, in cui l'utente entra, attirato dalle meraviglie gratuite offerte, ma poi non può più uscire e si perde dentro i vari Eden tecnologici delle Big Tech. Che sono diventate una sorta di stati paralleli, perché si son dati nel tempo le loro regole, facendo venir meno la fondamentale distinzione tra poteri pubblici e privati, alla base di ogni ordinamento giuridico statale. Hanno fatturati e capitalizzazioni equivalenti al PIL di grandi stati nazionali, grazie all'accumulo di denaro consentito da margini di profitto inimmaginabili nel mondo delle imprese tradizionali.

Nulla di nuovo sotto il sole dell'Occidente, si dirà. Basti ricordare la storia secolare della Compagnia delle Indie orientali britannica, un'impresa privata che tra il XVII e il XVIII secolo arrivò a governare l'India con un suo esercito, prima che il Parlamento di Londra riuscisse, in quasi mezzo secolo

di battagli politiche e parlamentari, a ricondurla sotto la giurisdizione dello stato. Certo, le grandi piattaforme digitali non hanno un esercito e non governano i territori; ma viene da chiedersi se ne abbiano davvero bisogno visto la pervasività della loro signoria: quando si raggiunge e si influenza un terzo della popolazione del pianeta non vi è necessità di ostentare una forza che si possiede già. Il vero potere non è forse quello che non si vede? Quelle di un tempo erano società per azioni che esercitavano una parte della sovranità delegata loro dal monarca in nome del profitto ma anche degli ideali del progresso: non vi era distinzione tra pubblico e privato perché le due dimensioni erano inseparabilmente intrecciate<sup>1</sup>. Di natura indissolubilmente ibrida, esse sfidavano i grandi teorici della sovranità come Hobbes e Bodin le cui ricette per l'assolutismo "erano più prescrittive che descrittive"<sup>2</sup>.

Creatura ibrida tra pubblico e privato la Compagnie delle Indie; altrettanto Facebook e Google che non mostrano alcuna timidezza nello svelare le loro ambizioni imperiali – qualcosa che Russi e Cinesi hanno intuito perfettamente avendo un senso della storia più sviluppato degli europei atlantici, ancorché parecchio distorto e selettivo.

Del resto, un punto in comune lampante con il loro grande precursore del Settecento lo hanno di sicuro: ossia la capacità di *lobbying* delle istituzioni politiche; inaugurata nel 1693 dalla Compagnia questa prassi e questo talento trovano degni eredi nei monopolisti di oggi<sup>3</sup>. In effetti, dice Lucie Greene in *Silicon States*<sup>4</sup>, le piattaforme si spingono oltre i limiti dell'immaginazione dell'osservatore. Efficacissime lobbiste, pronte sempre a sfruttare il mito degli eroi della tecnologia frenati dai burocrati, battono in breccia le iniziative legislative sgradite. Regolatori del mercato in cui esse stesse operano, relegano lo stato a una fastidiosa appendice. Chi è contro la Silicon Valley è *ipso facto* contro la tecnologia e il progresso: questa è la narrativa, sotto il sempiterno stendardo della "Nuova Frontiera" e all'insegna di un motto confortante: là dove c'è *network*, lì non può esservi ghetto o dominazione di classe<sup>5</sup>.

Del tutto coerentemente, Julie Cohen, giurista di Georgetown, invita a

---

<sup>1</sup> A. PHILLIPS, J.C. SHARMAN, *Outsourcing Empire. How Company-State Made the Modern World*, Princeton, 2020.

<sup>2</sup> PH.J. STERN, *The Company State. Corporate Sovereignty & the Early Modern Foundation of the British Empire in India*, Oxford, 2011.

<sup>3</sup> W. DARLYMPLE, *The Anarchy. The Rentless Rise of the East India Company*, London, 2019.

<sup>4</sup> L. Greene, *Silicon States. The Power and Politics of Big Tech and What It Means for Our Future*, Berkeley, 2018.

<sup>5</sup> *Ibidem*.

passare il Rubicone riconoscendo la plausibilità dell'ossimoro – “sovranità privata” – a favore di piattaforme che in tutto e per tutto operano quali grandi soggetti della diplomazia internazionale. Il loro potere è normativo, performativo, pratico e gli Stati le corteggiano per carpire i loro segreti: di quale altra prova vi è bisogno?<sup>6</sup>

Ora, se qualcosa insegna la vicenda della East India Company, nella versione originale nonché in quella sotto i nostri occhi, diciamo per comodità post-moderna, è questo: come rammenta David Runciman in *How Democracy Ends*: “se Facebook dovrà essere domata in un futuro prossimo, ciò avverrà da parte del potere posseduto dagli Stati, che sono le macchine inventate a questo scopo. Non potrà essere semplicemente il popolo vs. Facebook. Dovrà essere Leviatano contro Leviatano”<sup>7</sup>. Ne sapevano qualcosa i coloni americani nel loro apprendistato verso l'indipendenza. I barili di tè gettati a mare nel porto di Boston, non a caso di proprietà proprio della monopolista compagnia delle Indie, sembravano contenere “un veleno lento, in senso politico come fisico. Essi racchiudono qualcosa di peggio della morte: i semi stessi della schiavitù”<sup>8</sup>.

I feroci critici dello Stato dovrebbero riflettere sulla natura di Leviatano propria di una Facebook, ben più insidiosa rispetto alle tante entità territoriali create dal Cinquecento in poi. Ammonisce ancora Runciman: “Facebook è sia una gerarchia che una rete. È molto più gerarchico di qualsiasi Stato democratico: Zuckerberg e la sua cerchia immediata esercitano uno straordinario livello di controllo personale. È più simile a una corte medievale che a una comunità politica moderna. Il potere scorre dall'alto. Allo stesso tempo la sua rete è molto più inclusiva di qualsiasi Stato”. E non è finita: “lo Stato può farci sentire sicuri ma Facebook ci fa sentire amati”. È l'esatto contrario della democrazia rappresentativa che fu inventata dai rivoluzionari americani e francesi non per solleticare i nostri istinti ma per tenerli a bada, non per appagarli ma per trascenderli: ragion per cui tanto essa è frustrante, quanto invece appagante è l'esperienza del *social network* che ci regala scariche di dopamina.

Ben lontano da inverare la *Pax Technica* immaginata da Philip Howard<sup>9</sup>,

---

<sup>6</sup>J.E. COHEN, *Between Truth and Power. The Legal Construction of Informational Capitalism*, Oxford, 2019.

<sup>7</sup>D. RUNCIMAN, *How Democracy Ends*, London, 2018.

<sup>8</sup>T.H. BREEN, *The Marketplace of Revolution. How Consumers Politics Shaped American Independence*, Oxford, 2004.

<sup>9</sup>P.N. HOWARD, *Pax Technica. How the Internet of Things Set Us Free or Lock Us Up*, New Haven, 2015.

lo scenario che ci viene servito promette solo uno strisciante e molto accudente asservimento dei soggetti, agli antipodi esatti del paradigma individualista che ha fondato la modernità dal Seicento in poi. E per quanto possa deludere la prospettiva, l'unico ingrediente per resistere a questo imperialismo post-moderno è ricorrere allo Stato, sì proprio quello Stato che abbiamo speso trenta anni ad esecrare, almeno da quando Francis Fukuyama annunciò baldanzoso la fine della storia. Operazione necessaria ma non semplice perché la sfida è impari: "il mondo online", dichiara l'ex capo di Google Eric Schmidt, "non è veramente limitato da leggi terrestri... è il più grande spazio non governato della terra"<sup>10</sup>. Direi che ce ne siamo accorti.

Nonostante questi argomenti, si potrebbe ancora contro argomentare sostenendo che l'accostamento con le grandi compagnie del passato è nulla di più di una elegante *boutade*, una trovata ad effetto. No, non è affatto una trovata ad effetto, poiché il colonialismo dei dati si pone in piena continuità con il colonialismo storico per le modalità che presta al capitale al fine di procedere allo sfruttamento della materia prima. Con la differenza che il capitalismo dei dati non si accontenta di sottoporre al meccanismo di appropriazione ed estrazione del valore i corpi: pretende invece di carpire per i suoi scopi l'intera vita umana, catturata in relazioni sociali che passano necessariamente per le maglie strette della dataficazione. Il nuovo colonialismo, come argomentano Couldry e Mejias<sup>11</sup>, si basa sulla "naturale" disponibilità di dati sociali "a basso prezzo". Con il dispositivo di sfruttamento che lo ha storicamente preceduto, il nuovo colonialismo condivide gli assi portanti: una infrastruttura tecnologica per l'estrazione dei dati; un ordine sociale che vincola gli esseri umani a questa infrastruttura; un sistema economico costruito su infrastruttura e ordine; un modello di governo sociale che lega sempre di più gli individui al sistema; una razionalità che offre un orizzonte di senso allo sfruttamento; e persino un nuovo modello di conoscenza che esaurisce in sé, nei *big data*, lo spazio di ciò che si può apprendere sulla vita (in una convergenza senza precedenti tra potere economico e cognitivo)<sup>12</sup>.

La riduzione delle relazioni sociali a *commodity* rende tutto ciò possibile e plausibile. Certo Amazon non ha bisogno del suo esercito come la Com-

---

<sup>10</sup> E. SCHMIDT, J. COHEN, *The New Digital Age. Reshaping the Future of People, Nations and Business*, London, 2013.

<sup>11</sup> N. COULDRY, U.A. MEJIAS, *The Costs of Connection. How Data is Colonizing Human Life and Appropriating It for Capitalism*, Stanford, 2019.

<sup>12</sup> *Ibidem*.

pagna delle Indie. Il punto è che si pone esattamente anch'essa quale "compagnia-Stato" sfruttando l'enorme potenziale della sua logistica, di cui il *cloud*, la "nuvola", è la punta di diamante. In sintesi "se il colonialismo può essere capito come un processo che permette a una parte di occupare lo spazio vitale di un'altra e di appropriarsi delle sue risorse, sopraffacendola attraverso una combinazione di razionalizzazione ideologica e mezzi tecnologici (che includono l'uso della sorveglianza e del dominio), ebbene allora noi suggeriamo che siamo entrati in una nuova fase del colonialismo"<sup>13</sup>.

Insomma la piega che ha preso la rivoluzione digitale qualche problema sistemico lo sta creando. Nel libro che ho scritto insieme al Prof. Stefano Mannoni<sup>14</sup> dell'Università di Firenze e che è tra gli argomenti di discussione del nostro incontro odierno, abbiamo sintetizzato, mi sembra efficacemente, nel risvolto di copertina quello che è accaduto: la rivoluzione digitale ha consegnato a poche grandissime imprese un potere privato così vasto e penetrante da mettere in discussione il potere pubblico la sua *auctoritas* sovrana che, da Hobbes in poi, è stata concepita per frenare i poteri privati che minaccino di confiscare il potere di dettar legge, di imporre una eteronomia non legittimata. La tentacolare oligarchia degli *arcana imperii* digitali, fatta di algoritmi inaccessibili, di profilazione e sorveglianza digitale di miliardi di utenti più o meno consapevoli, ha messo a repentaglio i grandi capisaldi dell'Occidente e cioè la demarcazione tra Stato e società, la vitalità di una democrazia che non sia solo virtuale, la promozione di mercati concorrenziali. Col rischio di consegnare Società mercati e democrazia a una cyberutopia distopica. La riscossa dei poteri pubblici cui stiamo finalmente assistendo in questo campo in Europa negli Stati Uniti, rappresenta la riscoperta della sovranità.com perché capace, nella sua leggendaria duttilità, di adattarsi a una sfida quella lanciata nel cyberspazio dalle grandi piattaforme digitali, che sembrava vederla perdente. Chiaramente la partita è ancora del tutto aperta siamo solo all'inizio.

Comunque è molto importante il contributo della ricerca accademica per contenere questo tipo di fenomeni, il grande piano di cui parliamo oggi che coinvolge tante università in questo settore è veramente importante; con Mannoni, in un primo libro<sup>15</sup> che abbiamo scritto un po' di anni fa

---

<sup>13</sup> *Ibidem*.

<sup>14</sup> S. MANNONI, G. STAZI, *Sovranità.Com. Potere pubblico e privato ai tempi del cyberspazio*, Editoriale Scientifica, Napoli, 2021.

<sup>15</sup> S. MANNONI, G. STAZI, *Is Competition a Click Away? Sfida al monopolio nell'era digitale*, Editoriale Scientifica, Napoli, 2018.

sempre su questi temi, avevamo registrato una carenza di dibattito accademico in Italia e in Europa; in effetti la riscossa dei poteri pubblici di cui parliamo ha avuto dai due lati dell'Atlantico due origini diverse: da noi la Commissione europea ma anche le autorità nazionali di concorrenza. Ad esempio l'indagine conoscitiva di qualche anno fa, realizzata dall'Antitrust insieme all'Authority per la Privacy e all'Agcom è stato un esempio importante di cooperazione tra istituzioni che ha prodotto risultati, poi posti alla base di nostre istruttorie importanti avviate nei confronti del mondo delle grandi piattaforme digitali.

Quindi l'iniziativa in Europa è partita proprio dalle istituzioni a tutela della concorrenza: dalla Commissione per iniziativa della Commissaria alla concorrenza Vestager e da alcune autorità nazionali tra cui la nostra; negli Stati Uniti invece è successo che il mondo accademico ha avuto un ruolo importante, col coinvolgimento successivo della politica e delle autorità *antitrust* americane. È anche la storia incredibile di Lina Khan, una giurista di origine pachistane che pubblicò la sua tesi di dottorato sul *Yale Law Journal*, "Amazon's Antitrust Paradox"<sup>16</sup>: venivano contestati in modo convincente e analitico una serie di dogmi che dagli anni Ottanta avevano sostituito i fondamenti originari della teoria e della pratica antitrust negli Stati Uniti e nel mondo e che di fatto avevano favorito la crescita inarrestabile del potere monopolistico di Amazon e delle altre grandi piattaforme digitali; ma anche permesso abnormi processi di concentrazione in settori importanti dell'economia tradizionale, con le connesse lesioni dei meccanismi concorrenziali legati a una struttura dei mercati sempre meno plurale. "Possiamo avere la democrazia in questo Paese, oppure possiamo avere una grande ricchezza concentrata nelle mani di pochi, ma non possiamo avere entrambe le cose". Così negli anni Venti del secolo scorso il giudice della Corte Suprema USA, Louis Brandeis, ribadiva il nesso tra la tutela della concorrenza e la democrazia, su cui si fondava la legge *antitrust* americana. Lina Khan, è diventata rapidamente *leader* del movimento neo-brandeisiano, richiamandosi appunto alla tradizione madisoniana del giudice Brandeis, che considerava il processo concorrenziale a presidio di una crescita non diseguale e a tutela della democrazia; questo gruppo di attivisti è stato da principio sbeffeggiato dai custodi dell'ortodossia *antitrust* e chiamato Hipster Antitrust; ma progressivamente è riuscito a imporre la sua agenda nel dibattito, prima sui media e poi a livello accademico e, infine politico. La Columbia Law School ha assegnato a Khan un insegnamen-

---

<sup>16</sup>L. KHAN, *Amazon's Antitrust Paradox*, in *Yale Law Journal*, 2017.

to di Antitrust e nel 2021 Lina Khan è stata nominata da Biden Presidente della Federal Trade Commission (FTC), l'agenzia americana che si occupa di *antitrust* e tutela dei consumatori. La sua nomina è stata confermata dal voto a larga maggioranza bipartisan del Senato americano. Lina Khan è stata anche consulente della Commissione del Congresso USA presieduta dal deputato David Cicilline, che ha redatto nel 2020 un rapporto estremamente critico sul potere monopolistico dei Big Tech, raccomandando azioni molto incisive per ripristinare un corretto assetto concorrenziale nei mercati digitali. La documentazione a corredo del rapporto è molto interessante e comprende un elenco dettagliato delle centinaia di acquisizioni effettuate negli ultimi anni dalle prime cinque aziende che per capitalizzazione guidano il listino di Wall Street -Amazon, Microsoft, Apple, Google, Facebook- che, secondo il Congresso americano, hanno messo in atto una strategia diretta a rafforzare il loro potere monopolistico facendo una sorta di terra bruciata nei rispettivi settori, rastrellando *start-up* e imprese potenzialmente concorrenti senza badare a spese.

La Presidenza FTC di Lina Khan rappresenterà, in ogni caso, un punto di rottura con il debole approccio *antitrust* americano degli ultimi 40 anni, un deciso cambio di paradigma che guarderà allo Sherman Act delle origini, la prima legge *antitrust* che, come ricordato sopra, era nata per impedire che imprese troppo grandi monopolizzassero i mercati e, tramite l'accumulo di enormi ricchezze, accrescessero le disuguaglianze e condizionassero la democrazia americana.

Ad ulteriore e definitiva conferma della svolta che l'Amministrazione Biden ha voluto imporre alla politica antitrust americana la nomina, intervenuta successivamente a quella della Khan, di Jonathan Kanter a capo della Divisione Antitrust del Dipartimento della Giustizia; che negli USA è l'altra istituzione competente per la concorrenza. Kanter è noto per le sue battaglie antimonopolistiche, soprattutto nei confronti delle grandi piattaforme digitali.

Quindi sicuramente assistiamo a un grande cambiamento di clima politico e istituzionale che unisce i due lati dell'Atlantico. Propedeutico a un crescendo di iniziative che dovrebbero contribuire al riequilibrio tra i poteri pubblici e quelli privati, equilibrio messo seriamente a repentaglio dal tumultuoso e disordinato sviluppo della rivoluzione digitale e dei suoi protagonisti.

Voglio però tornare al tema centrale del mio intervento e cioè ricondurre l'economia dei dati, su cui si fonda il potere di mercato delle Big Tech, in una prospettiva concorrenziale. Per introdurre il mio ragionamento, occorre tornare un po' indietro nel tempo, per imbarterci ancora in Louis Brandeis.

Il 15 dicembre 1890 sull'*Harvard Law Review* apparve "The Right to Privacy". Gli autori erano due giovani avvocati, Samuel Warren e Louis

Brandeis, che con questo saggio fondarono il diritto alla *privacy*. Secondo loro la *privacy* era “*the right to be let alone*” e cioè il diritto a essere lasciati soli, senza intrusioni nella sfera della vita privata. Il diritto alla riservatezza veniva distinto dal diritto di proprietà privata, ma ne costituiva sul piano giuridico una sua estensione, beneficiando delle connesse protezioni. Senza quindi la necessità di un intervento normativo, sarebbero stati i giudici a riconoscere le opportune tutele. Incidentalmente va notato che in quello stesso anno, il 1890, negli Stati Uniti fu varata la prima legge antitrust, lo Sherman Act, alla cui tessitura teorica ed operativa Louis Brandeis, nominato nel 1916 giudice della Corte Suprema dal Presidente Wilson, avrebbe poi dato contributi straordinari. “The Right to Privacy” è ancora oggi riconosciuto come il fondamento del diritto all’invulnerabilità della sfera privata della persona e alla riservatezza sui dati personali sensibili.

Per più di un secolo quel concetto di *privacy* è rimasto pressoché immutato, ma l’avvento del web e la successiva rivoluzione digitale ha mutato radicalmente il contesto in cui la *privacy* come categoria concettuale opera e dispiega le sue prerogative. Una grande mutazione sia sotto il profilo giuridico che quello economico e una conseguente ridefinizione dei confini tra sfera privata e pubblica, sospinta dall’affermarsi di una società dell’informazione basata su uno straordinario sviluppo tecnologico, che ha condotto a una forte erosione della riservatezza.

L’avvento dei *big data* ha quindi cambiato tutto: grandissime quantità di dati personali raccolte e lavorate da imprese dotate di sofisticati algoritmi che valorizzano in modo esponenziale le informazioni, usandole per indirizzare offerte di beni e servizi, per fornire messaggi pubblicitari personalizzati; e per scambiarle su vari mercati, compreso quello della politica, nati appositamente. Ed è un valore generato con costi vicino allo zero -siamo tutti noi che forniamo gratis la materia prima, i dati-, ma ad altissimo rendimento, in quanto le cronologie delle azioni delle persone sul *web* rivelano desideri, interessi, intenzioni del tutto trasparenti; perché carpiuti spesso senza la consapevolezza o con un consenso indotto dal desiderio di continuare le esperienze di navigazione online e le sue indiscutibili opportunità; tutto ciò con una portata, un’ampiezza e un dettaglio che sono senza precedenti nella storia umana.

La quarta rivoluzione industriale ha interconnesso il mondo trasformandolo in un villaggio globale e i suoi straordinari traguardi tecnologici superano, oltre ogni immaginazione, le grandi trasformazioni che l’hanno preceduta. Al centro l’individuo e i suoi dati, principale beneficiario e vittima predestinata di un processo tanto più grande di lui; impossibilitato a rivendicare la proprietà dei suoi dati e a pretenderne la remunerazione per

l'uso, di fatto indotto ad autorizzare gratis le piattaforme digitali ad utilizzarli ai fini più disparati e a venderli a chiunque.

I dati, infatti, costituiscono la materia prima dell'economia digitale, ma anche il suo ricchissimo prodotto; sono quindi *input* e *output* di un'economia che si autoalimenta in modo circolare. Su questo modello di *business*, basato sull'acquisizione gratuita della materia prima, i dati, le grandi piattaforme digitali hanno costituito un formidabile oligopolio tecnologico e industriale ad altissimo rendimento e alta potenzialità distruttiva dell'industria tradizionale, *in primis* quella basata sulla proprietà intellettuale.

È vero che sta crescendo la consapevolezza di consumatori e utenti che dai loro dati il sistema delle imprese Big Tech trae grandi risorse e che lo scambio proposto in modo ossessivo dai motori di ricerca, dai social e, in definitiva, da qualunque sito *web*, nel momento in cui si concede il consenso alla cessione dei propri dati personali, dà origine a una sorta di baratto; cui però è molto difficile carpirne convenienza economica e capirne le conseguenze. Detto in termini tecnici, la dilagante asimmetria informativa tra consumatori e imprese tecnologiche rende veramente ardua l'analisi costi-benefici che è alla base della transazione economica che ha ad oggetto la cessione di dati personali, cioè di elementi costitutivi della propria *privacy*.

Eppure la scelta di rivelare le proprie informazioni personali, in modo consapevole o inconsapevole, in un'epoca in cui saremo sempre più immersi e dipendenti dall'ecosistema digitale, costituisce ormai l'atto economico più frequente e in prospettiva più rilevante del nostro agire. E lo compiamo in un contesto di crescente incertezza, in quanto non conosciamo quante e quali informazioni vengono in realtà acquisite, né come vengono utilizzate, a chi vengono cedute e che tipo di conseguenze potrebbero derivarne.

Insomma, la crescente complessità delle interazioni di utenti e consumatori con l'ecosistema digitale aumenta l'asimmetria informativa tra gli attori. Si assumono decisioni, relative al livello di tutela della *privacy* desiderato, spesso in condizioni di incertezza e vulnerabilità, cui in qualche modo vanno posti tutela e rimedio. L'inquadramento classico della *privacy* come diritto soggettivo è fortemente messo in discussione dalle complessità proprie dell'era dell'informazione e dallo straordinario sviluppo dei mercati connessi.

Si comprende come, vista la complessità di queste scelte si varcano i confini tra il diritto della *Privacy* e l'economia della *Privacy* ed è quindi su quest'ultima disciplina che dobbiamo far leva per valutare e definire questa dimensione digitale della *privacy*; e proprio in base all'osservazione delle scelte alternative compiute dai titolari dei dati al cospetto della rete si osserva come la *privacy*, nella realtà economica, tende a perdere le caratte-

ristiche di diritto soggettivo assoluto quando si scompone nel bilanciamento tra sfera privata e sfera pubblica, realizzato tramite l'analisi costi-benefici dall'individuo; in questo quadro la *privacy* diviene *commodity* e la cessione dei dati personali cessione di merce.

Già molti anni fa venivano analizzate le implicazioni economiche del diritto alla *privacy*; il fondatore della *law&economics*, Richard Posner argomentava come la *privacy* fosse uno strumento che gli attori del mercato utilizzano per nascondere selettivamente una serie di informazioni, a proprio vantaggio e a danno di altri<sup>17</sup>. Quindi secondo la Scuola di Chicago, le restrizioni del flusso di informazioni in nome della *privacy* inibivano i processi di mercato, aumentando i costi di transazione<sup>18</sup>. Naturalmente siamo molto distanti dalle problematiche attuali, ma già allora emergeva dai diversi interessi in gioco una dinamica di carattere economico.

Ma è stato Hal Varian, l'economista che, insieme a Carl Shapiro, ha fissato i fondamenti economici della *Network Economy*<sup>19</sup> (contribuendo anche in modo decisivo allo sviluppo del *business model* di Google fin dal 2002 in qualità di suo *chief-economist*) a superare il pregiudizio della teoria economica che, a partire da Posner, aveva visto la *privacy* come un ostacolo all'efficienza dei mercati.

In un pionieristico paper, scritto a Berkeley del 1996<sup>20</sup>, Varian apparentemente tornava alle origini brandeisiane affermando che, quando le persone parlano di *privacy*, in realtà parlano del diritto a non essere infastidite. Per Varian è importante riconoscere che questa forma di fastidio deriva dal fatto che il venditore ha informazioni non precise sull'acquirente. In questo contesto, più il venditore conosce le preferenze del possibile acquirente, meglio è. E quindi informazioni più precise (la profilazione online arriverà qualche anno dopo) sono preziose poiché riducono ulteriormente i costi di ricerca sia per l'acquirente che per il venditore.

Secondo Varian alcuni di questi problemi avrebbero potuto essere mitigati consentendo modi più espliciti di trasmettere informazioni tra acquirenti e venditori, in particolare assegnando "un diritto di proprietà relativo alle informazioni su un individuo a quell'individuo, e consentire la scrittu-

---

<sup>17</sup> R.A. POSNER, *The Right of Privacy*, in *Georgia Law Review*, 12, 1977.

<sup>18</sup> R.A. POSNER, *The Economics of Privacy*, in *American Economic Review*, 71, 1981.

<sup>19</sup> C. SHAPIRO, H.R. VARIAN, *Information Rules: A Strategic Guide to Network Economy*, Harvard Business School Press, Boston, 1998.

<sup>20</sup> H.R. VARIAN, *Economic Aspects of Personal Privacy*, University of California Berkeley, Berkeley, 1996.

ra di contratti per l'utilizzo di tali informazioni per tempi limitati e scopi specifici. In particolare, le informazioni personali non potrebbero essere rivendute o fornite a terzi senza il consenso esplicito del titolare"<sup>21</sup>. Quindi le norme sulla *privacy* e sui diritti che gli individui hanno sui propri dati, dovrebbero riconoscere esplicitamente che tali diritti possono contemplare la cessione o il noleggio dei propri dati ad altri per usi specifici, ma non possono essere rivenduti senza esplicita autorizzazione. Questa semplice riforma avrebbe costituito, secondo Varian, la base per una politica più flessibile e più utile sulla *privacy* individuale e avrebbe consentito modelli di *business* con costi di transazione ridotti e migliori corrispondenze tra acquirenti e venditori<sup>22</sup>. A questo proposito Varian allora affermava che per superare i problemi di esternalità e di fallimento del mercato in tema di *privacy*, andrebbe riconosciuto un diritto di proprietà in capo al titolare dei dati, con la relativa possibilità di cederli ricavandone un compenso. Ma i diritti di proprietà erano detenuti da coloro che raccolgono informazioni sugli individui, non dagli individui stessi e le vendono anche a terzi. Queste terze parti acquistano e vendono a loro volta informazioni che possono imporre costi ai soggetti titolari dei dati, senza che le persone siano direttamente coinvolte nelle transazioni. Quindi già molti anni fa veniva fotografata una situazione che oggi in termini macroscopici alimenta lo strapotere economico delle imprese Big Tech. Il cui geniale modello di *business* basato sulla raccolta massiva dei dati, la profilazione algoritmica di utenti e consumatori ai fini del confezionamento di offerte mirate di pubblicità online è stato inventato da Varian per Google e poi adottato in via generale come architrave del mercato digitale. Purtroppo si è perso il contributo innovativo che Varian avrebbe potuto dare allo sviluppo di un mercato dei dati più efficiente ed equo.

Sarebbe possibile, oggi, definire un diritto di proprietà sui dati in capo al titolare, l'individuo? In caso di risposta affermativa, ciò costituirebbe la premessa per un mercato più trasparente ed equo di quello che si è generato finora.

Anche perché, come abbiamo visto in precedenza, già esiste un mercato dei dati, seppure completamente sbilanciato a favore delle imprese digitali, che esprimono la domanda, rispetto agli utenti che, volenti o nolenti esprimono l'offerta, ma non possono reclamarne il prezzo. Perché, si dice, l'utente non è in grado di attribuire un valore ai suoi dati, non percepisce la catena del valore cui i suoi dati danno origine; e perché, nell'attuale as-

---

<sup>21</sup> *Ibidem*, 6.

<sup>22</sup> *Ibidem*, 7.

setto di mercato non può di fatto escludere gli altri dal godimento del suo bene (il dato personale). In questo senso il dato assumerebbe la natura di bene pubblico, che renderebbe impossibile un diritto proprietario.

I due elementi costitutivi del diritto di proprietà sono, infatti, il diritto di escludere e il diritto di alienare. Ed è l'ordinamento che deve provvedere all'assegnazione originaria di un diritto (*entitlement*). Secondo Guido Calabresi "Il primo problema che deve essere affrontato da ogni ordinamento giuridico è quello dell'assegnazione originaria dei diritti. Ogni qualvolta si presenta uno stato di interessi confliggenti tra due o più soggetti o gruppi di soggetti, l'ordinamento deve decidere quale parte favorire"<sup>23</sup>. Gli storici dell'economia hanno dimostrato come all'inizio dell'era moderna il mondo occidentale ha ordinato e accelerato il suo sviluppo rispetto alle altre parti del mondo grazie alla disciplina e alla tutela del diritto di proprietà<sup>24</sup>.

È curioso come la quarta rivoluzione industriale, la *big data economics*, sia partita senza riconoscere ai titolari dei dati l'*entitlement*. Riconoscendo invece, soprattutto in Europa, un diritto alla *privacy* molto importante ma difficile da maneggiare e da valorizzare per il titolare, in quanto il dato personale, considerato un diritto inalienabile della persona, non può essere venduto dal titolare; ma le autorizzazioni, da noi concesse con riflesso pavloviano, consentono gratis l'acquisizione dei nostri dati da parte della piattaforma, che diventa di fatto assegnataria di un diritto di proprietà, perché può cedere i dati a pagamento a centinaia di terze parti interessate a lavorarli.

La dispersione dei dati personali in mercati secondari comporta, da un lato la totale perdita di controllo da parte dell'utente delle informazioni rilasciate, dall'altro una valorizzazione esponenziale del dato di cui il titolare non beneficia minimamente, con una distribuzione del valore economico generato totalmente sbilanciata a favore delle imprese. Insomma, come pure autorevolmente affermato dal Prof. Ghidini: "In fondo noi forniamo dati della nostra vita che diventano merce di scambio. Perché non esigere un compenso?"<sup>25</sup>.

Appare quindi evidente l'opportunità di rendere trasparente questo mercato implicito basato su transazioni opache, i cui benefici, questa volta espliciti in termini di reddito e potere di mercato, sono completamente a favore delle piattaforme tecnologiche e dei *data broker*, gli altri attori del mercato dei dati.

---

<sup>23</sup> G. CALABRESI, A.D. MELAMED, *Property Rules, Liability Rules and Inalienability: one view from the Cathedral*, in *Harvard Law Review*, 85, 6, 1972, 1090.

<sup>24</sup> D.C. NORTH, R.P. THOMAS, *The Rise of Western World*, Cambridge, 1973.

<sup>25</sup> G. GHIDINI, D. MANCA, A. MASSOLO, *La nuova civiltà digitale. L'anima doppia della tecnologia*, I Solferini, Milano, 2020, 114.

Realizzare un mercato dei dati trasparente ed equo potrebbe essere possibile con una chiara assegnazione originaria del diritto di proprietà del dato al suo legittimo titolare, l'utente, conferendogli il diritto di escludere e la possibilità di negoziare contratti relativi ai dati da lui originati. Ponendo così l'individuo al centro della rivoluzione digitale.

La creazione di un mercato dei dati avrebbe effetti positivi sulle dinamiche concorrenziali dell'economia digitale; finora l'autorizzazione all'uso dei nostri dati personali che concediamo gratis alla piattaforma, di fatto assegnava a questa il diritto a decidere se e con chi condividere i dati; il regolamento europeo sulla protezione dei dati (GDPR), all'art. 20 prevede il diritto alla portabilità dei dati personali, cioè a chiederli e riceverli da chi li detiene e a trasferirli a chi vogliamo: se ben interpretato e attuato potrebbe rappresentare un punto di partenza per un nuovo assetto.

D'altronde, in Italia, l'Autorità garante della concorrenza e del mercato, in un caso nei confronti di Facebook<sup>26</sup>, ha affermato l'esistenza di un rapporto di consumo tra l'utente e la piattaforma digitale e sanzionato le pratiche di forzata condivisione di dati e la pubblicizzazione come gratuita di pratiche che comportavano la cessione di un bene economico, i dati personali. Il consenso prestato alla cessione dei dati personali costituisce quindi un corrispettivo per accedere alla controprestazione fornita dal gestore di servizi online. La pronuncia del giudice amministrativo, confermando la sanzione AGCM, ha statuito la necessità di offrire tutela giuridica anche al dato in quanto possibile oggetto di compravendita tra l'individuo che fornisce il dato personale e l'operatore di mercato che lo acquista; certificando l'esistenza e la rilevanza giuridica di un mercato dei dati. Naturalmente non solo in Italia, ma anche la Commissione europea ha affermato che i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico *de facto*. E la portabilità del dato personale, come sottolineato in precedenza, oltre ad essere un importante presupposto di disciplina concorrenziale delle piattaforme digitali dominanti, rappresenta un notevole passo del legislatore europeo verso una dimensione proprietaria e di mercato del dato personale. Anche perché la visione predigitale, romantica, del dato personale come inviolabile e inalienabile in quanto parte della nostra personalità, unica e non negoziabile, non è più sostenibile, e non pare aver più senso la delega che tramite il consenso concediamo ad altri per estrarre il valore dai nostri dati. E quindi una tutela della *privacy* fuori centro rispetto ai tempi e ai modelli di *busi-*

---

<sup>26</sup> AGCM, provv. n. 26597 dell'11 maggio 2017, *WhatsApp-Trasferimento dati a Facebook*, n. 27432 del 29 novembre 2018, *Facebook-condivisione dati con terzi*.

ness dell'economia digitale, si risolverebbe in uno schermo concorrenziale a favore delle grandi piattaforme digitali.

Sta quindi maturando, lentamente ma progressivamente il momento della restituzione della titolarità economica del dato personale al suo legittimo proprietario, che lo genera. Per partecipare, finalmente, al *revenue sharing* della catena del valore che si crea intorno ai dati. Un assetto del mercato digitale basato su una chiara assegnazione dei diritti di proprietà sui dati, determinerebbe una redistribuzione delle enormi ricchezze generate dai dati a favore della generalità degli individui; e potrebbe, in prospettiva, mettere in discussione il potere di mercato delle grandi piattaforme digitali che basano il loro modello di *business* sull'uso e lo sfruttamento esclusivo dei dati personali, ponendo le condizioni strutturali per lo sviluppo di più accentuate dinamiche concorrenziali: piena portabilità, condivisione dei dati e interoperabilità delle piattaforme, strumenti decisivi per limitare il potere di mercato e mantenere un ambiente competitivo nell'economia digitale, costituirebbero infatti una naturale conseguenza del nuovo assetto.

Certo è una soluzione diversa da quella propugnata da Shoshana Zuboff, il cui volume sul "Capitalismo della sorveglianza" è stato pubblicato in Italia dalla Luiss University Press. La Zuboff chiede *tout court* di metter fine: "all'invasione della *privacy* e al furto su larga scala di dati personali vietandone la raccolta"; ma forse non così lontana dall'approccio di mercato, nel momento in cui, una volta assegnato il diritto di proprietà, il legittimo titolare dei dati – l'utente che navigando in Internet lascia la sua scia di informazioni digitali – riceverebbe un compenso invece di subire una spoliazione.

In conclusione, ha ragione Marco D'Alberti quando argomenta che "i diritti fondamentali e i valori democratici sono ancora esposti a seri rischi derivanti dal lato oscuro della quarta rivoluzione industriale, principalmente dai comportamenti delle grandi imprese che aggregano, elaborano, utilizzano e detengono i nostri dati mutati in *big data*"<sup>27</sup>. Per fare luce su questo "lato oscuro", è in corso nell'Unione europea un intenso processo di normazione e regolazione dell'economia digitale ma, in ogni caso, la riconquista della sovranità digitale, sui dati innanzitutto, da parte dei cittadini e delle loro comunità statuali passa dal riequilibrio e il bilanciamento tra i poteri pubblici e quelli privati. Che riduce le disuguaglianze e tutela la democrazia. Ed è questa la direzione di marcia che, nei due lati dell'Atlantico, si sta ormai affermando.

---

<sup>27</sup> M. D'ALBERTI, *Concorrenza e giustizia sociale*, in *Mercato concorrenza regole*, 2, 2020.

Nicola M.F. Faraone

## Chi prima arriva [forse non] primo alloggia: questioni aperte in tema di concorrenza e regolamentazione *ex-ante* nei mercati digitali

SOMMARIO: 1. Premesse introduttive. – 2. Il diritto della concorrenza arranca e la regolazione è pronta a supplire: un’ultima decade di “riforme” vissuta “pericolosamente”. – 3. Il cumulo di procedimenti e sanzioni nel Digital Markets Act. – 4. Il caso di scuola del *ne bis in idem*. – 5. La novella dell’abuso di dipendenza economica nei mercati digitali introdotta dal DDL Concorrenza. – 6. Conclusioni.

### 1. Premesse introduttive

Il 3 maggio 2023 segna l’inizio dell’applicazione del Digital Markets Act (“DMA”) <sup>1</sup>. Come per il Regolamento generale sulla protezione dei dati (il

---

<sup>1</sup>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). Il DMA è stato approvato dal Parlamento europeo e dal Consiglio lo scorso 14 settembre 2022 e pubblicato in Gazzetta Ufficiale il successivo 12 ottobre 2022. Il DMA è entrato ufficialmente in vigore lo scorso 1 novembre 2022 e sarà applicabile a partire dal prossimo 2 maggio 2023. Lo scorso 9 dicembre 2022, la Commissione europea ha pubblicato una bozza di regolamento di attuazione relativa all’implementazione del DMA, sulla quale le parti interessate potevano presentare le proprie osservazioni sino allo scorso 6 gennaio 2023. Tuttavia, il lavoro preparatorio è stato relativamente breve, seppur travagliato. Di seguito vengono riassunte le principali tappe di approvazione, a partire dalla Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), COM(2020)842 final, 2020/0374(COD), 15 dicembre 2020. Successivamente, il c.d. Internal Market and Consumer Protection Committee (“IMCO”) in seno al Parlamento europeo ha adottato, in data 23 novembre 2021, con 42 voti a favore, 2 contrari e 1 astensione, la sua posizione sulla proposta di DMA, poi votata in seduta plenaria in data 15 dicembre 2021, confermando il mandato del Parlamento europeo per i negoziati. Parallelamente, il Consiglio – e, nello specifico, il “Competitiveness Council (Internal market and industry)” – ha all’unanimità approvato la sua posizione favorevole all’adozione

famigerato “GDPR”)<sup>2</sup>, l’Unione europea si conferma come precursore nella regolamentazione dell’economia digitale, rafforzando la propria *leadership* nella “produzione normativa” a livello mondiale, in ossequio al ben noto “effetto Bruxelles”<sup>3</sup>.

Il DMA rappresenta il “punto di caduta” finale di un percorso più risalente, che muove dall’emergere dei grandi attori tecnologici privati, delle piattaforme – che di queste imprese rappresentano l’infrastruttura essenziale per costituire l’ecosistema di riferimento –, che si è nutrito della sfiducia verso le attuali norme a tutela della concorrenza e che ha invocato la necessità di interventi “di sistema” per affrontare le sfide attuali.

Il diritto della concorrenza “tradizionale” – questo è l’assunto di base – non affronta le criticità relative al corretto funzionamento del mercato poste dalle condotte delle piattaforme digitali (i c.d. *gatekeepers*, nella terminologia del DMA), che non sono necessariamente dominanti nell’accezione tipica del diritto della concorrenza.

Secondo questa linea argomentativa, dato che il diritto della concorrenza, preso in sé, non è in grado di affrontare i problemi “strutturali” posti dalle dall’economia delle piattaforme, si è optato per un intervento normativo, di “stampo regolatorio”, che ha introdotto una serie di obblighi *ex-ante* per i *gatekeepers* digitali, e che finirà per dispensare gli operatori del diritto dal confrontarsi “a tutto tondo” con l’analisi *antitrust standard* (definizione del mercato rilevante, prova della posizione dominante e valutazione degli effetti anticoncorrenziali, impossibilità di proporre una difesa basata sull’efficienza).

Sulla base di tali premesse, il presente contributo, nel § 2, intende passare in rassegna il percorso di riforme intrapreso a livello europeo in tema di mercati digitali valorizzando le ragioni sottostanti al “cambio di paradigma” in favore della regolazione. Nel § 3, si procederà a indagare il ruolo “pivotale” del DMA e il suo rapporto con le altre norme (non solo) in materia di concorrenza europee e nazionali, focalizzando la nostra attenzione,

---

del DMA in data 25 novembre 2021. Il dialogo multilaterale e i negoziati tra i co-legislatori sono partiti ad inizio 2022. In data 24 marzo 2022, l’Unione europea ha presentato il testo finale (e aggiornato) di DMA, concordato a seguito del negoziato trilaterale tra la Commissione europea, il Parlamento europeo e gli Stati membri (guidati dalla Presidenza francese al Consiglio europeo), che è stato approvato dai rappresentanti degli Stati membri lo scorso 11 maggio 2022.

<sup>2</sup> 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).

<sup>3</sup> A. BRADFORD, *The Brussels effect: How the European Union rules the world*, Oxford University Press, New York, 2020.

nel § 4, sui pericoli di duplicazione di procedimenti (e sanzioni) che da tale sovrapposizione potrebbero discendere. Si affronteranno, dunque, le potenziali ripercussioni in tema di *ne bis in idem*, declinandole, nel § 5, anche alla luce dell'approvazione del DDL Concorrenza che ha introdotto una presunzione di abuso di dipendenza economica in caso di servizi resi da piattaforme digitali. Nel § 6, si "tireranno le fila" del discorso, proponendo delle conclusioni (necessariamente provvisorie, visto il dibattito ancora in corso).

## **2. Il diritto della concorrenza arranca e la regolazione è pronta a supplire: un'ultima decade di "riforme" vissuta "pericolosamente"**

Per molti anni, il contrasto e il contenimento del crescente potere delle piattaforme digitali è stato basato, da un canto, sull'applicazione dello strumentario normativo *antitrust* (in particolare, mediante il perseguimento di condotte integranti abusi di posizione dominante e il controllo delle operazioni di concentrazione) e, dall'altro, adoperando la "leva" della protezione della *privacy* e dei dati personali (a seguito dell'approvazione del GDPR e della sua entrata in vigore due anni dopo).

Da diverso tempo a questa parte, però, la Commissione europea e le autorità garanti per la concorrenza degli Stati membri sono state sottoposte a forti pressioni politiche per intervenire rapidamente contro i vari operatori digitali. Le ragioni sono molteplici. Tra le altre, lo straordinario successo finanziario di una minoranza di imprese tecnologiche, alcune delle quali hanno largamente beneficiato dalla crisi pandemica da Covid-19, unitamente alla percezione che esse siano riuscite a eludere, se non "aggirare", i sistemi di imposizione nazionali avvantaggiandosi di uno *status* fiscale *ad hoc*, hanno cementato un consenso "politico" trasversale intorno all'idea che il diritto *antitrust* non sarebbe più in grado di affrontare efficacemente le sfide e i problemi "strutturali" posti dall'ecosistema delle piattaforme e dall'irrompere onnipresente dell'economia dei dati nel mercato.

Il periodo di transizione post-pandemica ha rappresentato, poi, un banco di prova senza precedenti per verificare lo "stato di salute" delle regole europee (e non solo) a tutela della concorrenza

Le prese di posizione circa l'efficacia dell'intervento delle autorità garanti della concorrenza, più attive in Europa, meno negli Stati Uniti, sono state, dunque, veementi e contrastanti.

Il risultato ultimo di questa “levata di scudi” ha condotto a denunciare l’incapacità di affrontare la novità rappresentata dai *big data* e a postulare, al tempo stesso, una generale revisione dell’attuale regime delle norme a tutela della concorrenza<sup>4</sup>.

Riavvolgendo il “nastro” dell’ultimi dieci anni, infatti, quantomeno sul versante del controllo delle operazioni di concentrazione, la Commissione europea, pur conducendo approfondite istruttorie<sup>5</sup>, non è riuscita a impedire a Facebook e Google di acquisire imprese, all’epoca, “nascenti” e potenziali concorrenti in prospettiva (per esempio, WhatsApp e Instagram, nel caso di Facebook; Double Click, nel caso di Google<sup>6</sup>). Più nello specifico, il limite cui sarebbe incorsa la Commissione è stato quello di definire un mercato “ristretto” che non ha tenuto conto del ruolo che i *Big Data* hanno assunto nella definizione del potere di mercato<sup>7</sup>.

Più incisiva, invece, è stata l’azione della Direzione Generale Concor-

---

<sup>4</sup>Tra i numerosi contributi, si rimanda, in campo internazionale, a M.E. STUCKE, A.P. GRUNES, *Data-opolies*, in *Concurrences* No. 2-2017 e *University of Tennessee Legal Studies Research Paper* No. 316, 2017; ID., *Big Data and Competition Policy*, Oxford University Press, Oxford, 2016; A. EZRACHI, M.E. STUCKE, *Online Platforms and the EU Digital Single Market*, in *University of Tennessee Legal Studies Research Paper* No. 283, 2015; ID., *Virtual Competition: The Promise and Perils of the Algorithm Driven Economy*, Harvard University Press, United States, 2016; A. EZRACHI, *EU Competition Law Goals and the Digital Economy*, in *Oxford Legal Studies Research Paper* No. 17/2018 e, con riferimento all’Italia, tra gli altri, a V. FALCE, G. GHIDINI, G. OLIVIERI, *Informazione e Big Data tra innovazione e concorrenza*, in *Quaderni Romani di Diritto Commerciale*, vol. 36, 2018; S. MANNONI, G. STAZI, *Is competition a click away? Sfida al monopolio nell’era digitale*, Editoriale Scientifica, Napoli, 2018. Più in generale, la ragione di fondo sociopolitica che ha fatto scaturire questa presa di coscienza risiede nella diffusa mitizzazione di Internet quale “autostrada” delle libertà individuali, non “contingentabile” da una pervasiva regolamentazione pubblica. Si tratta di una narrazione delle virtù del *web* ora non più attuale, soprattutto da quando si è disvelata la consapevolezza che, lungi dall’essere un *network* di attori decentralizzati e slegati tra loro, la Rete si è tramutata in una struttura fortemente “oligarchica”, governata “dal centro” da poche piattaforme globali che disegnano e impongono regole private. L’alternativa che ci si pone dinnanzi sarebbe, quindi, non più tra “regolazione vs. non-regolazione”, ma tra “regolazione pubblica vs. regolazione privata”. Su tale ricostruzione, si veda A. MANGANELLI, A. NICITA, *Regulating Digital Markets: The European Approach*, Macmillan, Cham, Palgrave, 2022; A. MANGANELLI, *Il Regolamento UE per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in *Merc. conc. reg.*, n. 3, 2021, 473 ss.

<sup>5</sup>Tra le analisi sugli interventi della Commissione europea in materia di controllo delle concentrazioni, si veda il rapporto LEAR, *Ex-post Assessment of Merger Control Decisions in Digital Markets*, commissionato dalla Competition and Market Authority inglese (“CMA”), May 2019.

<sup>6</sup>COMMISSIONE EUROPEA, caso COMP/M.7217, decisione del 3 ottobre 2014, Facebook/WhatsApp e caso COMP/M.7217, decisione dell’11 marzo 2008, Google/DoubleClick.

<sup>7</sup>Per altro verso, occorre segnalare che – all’epoca delle summenzionate decisioni della Commissione – la definizione di *Big Data* era ancora in via di consolidamento, quantomeno in sede comunitaria.

renza della Commissione con riguardo al perseguimento di abusi di posizione dominante, come dimostrano le diverse istruttorie che hanno condotto all'accertamento di condotte anticoncorrenziali da parte di Google (tre casi, relativi ai mercati dei comparatori di prezzi online, dei sistemi operativi, della pubblicità *online*)<sup>8</sup>, di Facebook (fornitura di false informazioni in occasione dell'acquisizione di WhatsApp)<sup>9</sup>, di Apple<sup>10</sup> e Amazon<sup>11</sup>.

Sul versante della regolamentazione, infine, gli sforzi più importanti, per quanto insoddisfacenti, hanno portato alla introduzione di alcuni obblighi in capo alle piattaforme digitali nelle nuove versioni della direttiva sui Media audiovisivi<sup>12</sup> e in quella che istituisce il Codice europeo delle

---

<sup>8</sup> Si veda COMMISSIONE EUROPEA, caso AT.39740, decisione del 27 giugno 2017, Google Search (Shopping) e alla successiva pronuncia del TRIBUNALE DELL'UNIONE EUROPEA, causa T-612/17, Google and Alphabet v Commission, sentenza del 10 novembre 2021 (attualmente pendente l'impugnazione dinnanzi alla Corte di giustizia, causa C-48/22 P, Google e Alphabet/Commissione (Google Shopping)); caso AT.40099, decisione del 18 luglio 2018, Google Android e alla successiva pronuncia del Tribunale, causa T-604/18 Google e Alphabet c. Commissione (Google Android), 14 settembre 2022 (attualmente pendente l'impugnazione dinnanzi alla Corte di giustizia, causa C-738/22 P, Google e Alphabet/Commissione); caso AT.40411, decisione del 20 marzo 2019, Google AdSense e alla successiva causa, attualmente pendente dinnanzi al Tribunale, causa T-334/19, Google e Alphabet c. Commissione (Google AdSense for Search)). Si veda anche COMMISSIONE EUROPEA, caso AT.40670, Google – Adtech and Data-related practices, 22 giugno 2021. Più di recente, negli Stati Uniti, lo scorso 24 marzo 2023, il Dipartimento di Giustizia, unitamente ai procuratori generali di California, Colorado, Connecticut, New Jersey, New York, Rhode Island, Tennessee e Virginia, ha intentato una causa civile *antitrust* contro Google per aver monopolizzato diversi prodotti tecnologici di pubblicità digitale in violazione delle sezioni 1 e 2 dello Sherman Act (Case 1:23-cv-00108).

<sup>9</sup> COMMISSIONE EUROPEA, caso M.8228, decisione del 17 maggio 2017, Facebook/WhatsApp. In data 4 giugno 2021, la Commissione europea ha avviato, inoltre, un'altra istruttoria (caso AT.40684 – Facebook leveraging) avente a oggetto il potenziale legame del servizio di annunci online di Facebook – Facebook Marketplace – con la piattaforma di *social network* di Facebook e il potenziale utilizzo dei dati ottenuti da Facebook nell'ambito della pubblicità sulla piattaforma di *social network* per avvantaggiare altri prodotti/servizi di Facebook, come Facebook Marketplace, in diretta concorrenza con i prodotti offerti dagli inserzionisti di Facebook, almeno dal 1 gennaio 2015. Si veda anche COMMISSIONE EUROPEA, caso AT.40774, decisione del 11 marzo 2022, Google-Facebook (Open Bidding) agreement.

<sup>10</sup> Si rimanda, tra le altre, alle seguenti istruttorie: COMMISSIONE EUROPEA, caso AT.40437, decisione del 16 giugno 2020, Apple – App Store Practices (music streaming); COMMISSIONE EUROPEA, caso AT.40652, decisione del 16 giugno 2020, Apple – App Store Practices (e-books/audiobooks); COMMISSIONE EUROPEA, caso AT.40452, 16 giugno 2020, Apple – Mobile payments.

<sup>11</sup> Per i casi rilevanti riguardanti Amazon, si rimanda *infra* alle note 50-51.

<sup>12</sup> Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di

comunicazioni elettroniche, entrambe varate negli ultimi mesi del 2018<sup>13</sup>, oltre che nel Regolamento che disciplina le relazioni tra le piattaforme *online* e la clientela *business*<sup>14</sup>.

Solo di recente, tuttavia, la Commissione europea ha messo a punto una strategia complessa per contrastare il potere delle piattaforme digitali.

In realtà, il percorso della Commissione europea per garantire un assetto concorrenziale dei mercati digitali può essere fatto risalire all'inizio del decennio scorso, con il varo dell'Agenda Digitale nel 2010, cui seguiranno – con cadenza quinquennale – il *Digital Single Market* (nel 2015)<sup>15</sup> e quindi la nuova strategia definita in *Shaping Europe's Digital Future* (nel 2020)<sup>16</sup>.

Occorre premettere, fin d'ora, come non si tratti soltanto del consueto quadro di regole per la disciplina dei mercati, a tutela della concorrenza e del consumatore, ma di un'architettura regolamentare volta a promuovere la competitività dell'industria europea: in altri termini, si inizia a delineare una politica industriale europea per i mercati digitali.

Per quanto riguarda il quadro regolamentare, il salto di qualità e intensità si è prodotto con la pubblicazione del Rapporto *Competition policy in a digital era*, noto come "Rapporto Crémer", dal nome del capofila della commissione di tre esperti cui il Commissario Vestager ha affidato il compito di esaminare le possibili linee evolutive della politica della concorrenza per continuare a promuovere una innovazione a favore del consumatore nell'era digitale<sup>17</sup>.

servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato (Gazzetta ufficiale dell'Unione europea L 303/69).

<sup>13</sup> Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche.

<sup>14</sup> Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (Gazzetta ufficiale dell'Unione europea L 186/57).

<sup>15</sup> Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Strategia per il mercato unico digitale in Europa, Bruxelles, 6 maggio 2015 COM(2015)192 final.

<sup>16</sup> Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Plasmare il futuro digitale dell'Europa, Bruxelles, 19 febbraio 2020, COM(2020)67 final.

<sup>17</sup> J. CREMER, Y. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era*, in *Final Report for the EU Commission*, 2019. In sintesi, il rapporto esclude di fatto misure di tipo strutturale (*break up*) nei confronti delle grandi piattaforme tecnologiche e ribadisce che il *framework* di base della legge sulla concorrenza, come incorporato negli artt. 101 e 102 TFUE, continua a fornire una base adeguata e sufficientemente flessibile per proteggere la concorrenza nell'era digitale. L'approccio caso per caso proprio dell'*antitrust* rimane perciò, secondo il Rapporto, il migliore quadro legale per affrontare i problemi dei mercati digitali. Al di là di questo

Per quel che interessa in questa sede, il rapporto ammette l'esistenza di uno spazio per un intervento di tipo regolamentare, indicando i possibili oggetti di un eventuale intervento *ex-ante*, qualora l'applicazione della disciplina generale *antitrust* si dimostrasse insufficiente. Tra questi, vanno menzionati: i) la portabilità dei dati, con la previsione di obblighi più stringenti in capo alle piattaforme dominanti, rispetto a quelli definiti dall'art. 20 GDPR<sup>18</sup>; ii) l'interoperabilità dei dati, soprattutto allorché si tratti di dati richiesti per servire mercati complementari o *aftermarkets* (mercati appartenenti all'ecosistema). Conclusioni, queste ultime, confermate e corroborate da altri *report* e contributi di *policy* che si sono susseguiti negli anni successivi<sup>19</sup>.

---

riconoscimento all'efficacia del diritto *antitrust* e della sua applicazione, il Rapporto indica, però, alcuni importanti modifiche da apportare ai concetti, alle metodologie e alla stessa dottrina *antitrust*, e ritiene che, in determinate circostanze, vi sia spazio per un intervento di tipo regolamentare. Sul versante dell'adeguamento della disciplina *antitrust*, le proposte concernono, innanzitutto, il controllo delle operazioni di concentrazione, con un particolare riguardo alle acquisizioni di piccole *start-up* con potenzialità competitive e con basi di clientela in rapida crescita (le c.d. *killer acquisitions*) da parte delle grandi piattaforme digitali. Altre importanti proposte vengono suggerite con riguardo all'analisi delle situazioni di abuso della posizione dominante e delle intese suscettibili di limitare la concorrenza. In estrema sintesi, si segnala la necessità di rivedere i "pilastri" dell'analisi *antitrust*, ed esattamente: il concetto di "benessere del consumatore"; la definizione del mercato rilevante, la misurazione del potere di mercato. Con riguardo al primo tema, nel mondo digitale, la categoria del consumatore tende a comprendere sempre più spesso le imprese utilizzatrici, ma, soprattutto, sempre più complessa risulta la misurazione del danno per il consumatore. In relazione al secondo aspetto, si deve sottolineare come, con la trasformazione digitale dei mercati, i confini tra i mercati risultano meno netti e comunque mutevoli, rispetto a quanto sperimentato nella c.d. *old economy*. Di conseguenza, maggiore attenzione deve essere posta sulle teorie del danno (*theories of harm*) e dell'identificazione delle strategie anticoncorrenziali. Da ultimo, riguardo al terzo profilo, il rapporto segnala i *bias* che agiscono dal lato del consumatore, con la propensione a considerare i vantaggi immediati dei servizi offerti dalle piattaforme digitali. Ne deriva una particolare forma di potere di mercato, un potere di intermediazione delle piattaforme, che diventano il partner commerciale inevitabile (*unavoidable trading partner*).

<sup>18</sup> Più di recente, la Commissione accoglie queste sollecitazioni, predisponendo una Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (normativa su un'Europa interoperabile), Bruxelles, 18 novembre 2022 COM(2022)720 final 2022/0379(COD).

<sup>19</sup> Si veda FURMAN *et al.* (2019), *Unlocking digital competition*, in *Report of the Digital Competition Expert Panel*. Si rimanda, inoltre, a GEORGE J. STIGLER CENTER FOR THE STUDY OF THE ECONOMY AND THE STATE (2019), *Report of Committee for the Study of Digital Platforms, Market Structure and Antitrust Subcommittee*, The University of Chicago Booth School of Business. Si veda, da ultimo, anche ACCC, *Digital platforms inquiry – Final Report* (July 2019); CMA – COMPETITION & MARKETS AUTHORITY, *Online platforms and digital advertising*, in *Market Study Final Report*, 1 July 2020; US SUBCOMMITTEE ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW OF THE COMMITTEE ON THE JUDICIARY. *Investigation on competition in digital markets*, 2020; per

Giusto un anno dopo, con la nuova legislatura europea e l'investitura di Ursula von der Leyen alla guida della Commissione europea, interviene il passaggio definitivo da un approccio "minimalista" a una strategia "coordinata" per contrastare il potere delle grandi piattaforme digitali e restituire all'Europa una sovranità digitale<sup>20</sup>.

Nel febbraio 2020, la Commissione presenta la (nuova) strategia contenuta nella Comunicazione *Shaping Europe's digital future*, che non segna una discontinuità assoluta: essa si ricollega, infatti, alle diverse misure che, a partire dalla metà del decennio scorso, la Commissione ha intrapreso in materia di *big data*<sup>21</sup>, protezione dei dati personali, intelligenza artificiale (IA)<sup>22</sup>.

La nuova Strategia per il digitale si caratterizza come processo a più stadi e, nella sua attuale configurazione, poggia su tre pilastri fondamentali<sup>23</sup>. Il DMA, che – presentato in forma di proposta di regolamento nel

la Germania, A. WAMBACH, H. SCHWEITZER, M. SCHALLBRUCH, *A New Competition Framework for the Digital Economy* – Report by the Commission Competition Law 4.0 e, 2019, da ultimo, l'indagine conoscitiva sui Big Data condotta congiuntamente dall'AGCOM, dall'AGCM e dal Garante per la Protezione dei Dati Personali e pubblicata in data 10 febbraio 2020. In aggiunta, il Consiglio Amministrativo per la Difesa Economica ("CADE") in Brasile ha pubblicato, il 17 settembre 2020, il Report "*BRICS in the Digital Economy: Competition Policy in Practice*", durante la Conferenza VI BRICS Competition Conference, che è il risultato del BRICS Working Group on the Competition Issues in the Digital Market, guidato dal CADE.

<sup>20</sup>U. VON DER LEYEN, *Un'Unione più ambiziosa. Il mio programma per l'Europa. Orientamenti politici per la prossima Commissione europea 2019-2024*, 16 luglio 2019.

<sup>21</sup>In materia di *big data*, il primo intervento dell'Unione europea che affronta anche il tema dei dati privati, avviene nel 2014, con la Comunicazione della Commissione "Verso una florida economia basata sui dati", Bruxelles, 2 luglio 2014 COM(2014)442 final.

<sup>22</sup>Si veda Comunicazione della Commissione, "*L'intelligenza artificiale per l'Europa*", COM(2018)237 final, 25 aprile 2018, che illustra un'iniziativa europea per dare impulso alla capacità tecnologica e industriale dell'UE e all'adozione dell'IA in tutti i settori economici, sia privati che pubblici, tenendo conto dei cambiamenti socio-economici apportati dall'IA, soprattutto con riferimento agli impatti sul mercato del lavoro, e della esigenza di garantire un quadro etico e giuridico basato sui valori dell'Unione e coerente con la carta dei diritti fondamentali dell'Unione.

<sup>23</sup>Se si volesse rintracciare un *fil rouge* che illustri la logica sottostante a interventi tanto articolati e complessi, questo andrebbe individuato nella sequenza dati-algoritmi-piattaforme: i dati come risorsa fondamentale dell'economia e della società digitale; gli algoritmi come strumenti capaci di estrarre valore da tali dati (anche per finalità analitiche, predittive e decisionali); le piattaforme come luoghi virtuali nei quali avvengono – intermediati in via algoritmica e con costante profusione di dati, riutilizzati per aumentare il potere delle piattaforme medesime – buona parte degli scambi e delle interazioni sociali contemporanee. Su ciascuno di questi tre nodi si appuntano specifici segmenti di regolazione: Data Governance Act e Data Act si occupano di rimuovere le restrizioni non necessarie alla libera circolazione dei dati, per favorirne accesso e riuso; l'AI Act (e, prima ancora, il GDPR) disciplina l'immissione in commercio e l'utilizzo degli algoritmi di intelligenza artificiale in una prospettiva di compatibilità con il qua-

dicembre 2020 e approvato, nel suo testo definitivo dal Consiglio e dal Parlamento lo scorso 14 settembre 2022 – è preordinato a limitare gli abusi di potere economico degli oligopoli digitali organizzati secondo il modello delle piattaforme<sup>24</sup>. In secondo luogo, il Digital Services Act

dro dei diritti fondamentali europei; il DMA e il DSA assoggettano le piattaforme al rispetto di determinati requisiti sia procedurali sia sostanziali al fine di salvaguardare il funzionamento delle regole di mercato e tutelare gli interessi dei terzi.

<sup>24</sup> Sia consentito rinviare, per una panoramica introduttiva, a G. BRUZZONE, *Verso il Digital Markets Act: obiettivi, strumenti e architettura istituzionale*, in *Riv. reg. merc.*, n. 2, 2021, 323 ss.; F. DONATI, *Verso una nuova regolazione delle piattaforme digitali*, *ivi*, 238 ss.; C. SCHEPISI, *L'enforcement del Digital Markets Act: perché anche i giudici nazionali dovrebbero avere un ruolo fondamentale*, in *Quaderni AISDUE*, n. 1, 2022, 49 ss.; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in *I Post di AISDUE*, 25 febbraio 2021, 30-56; G. MONTI, *The Digital Markets Act – Institutional Design and Suggestions for Improvement*, in *TILEC Discussion Paper*, 22 February 2021; L. ZOBOLI, *Digital Markets Act, una nuova proposta di Regolamento relativa ai mercati digitali*, in *Il Quotidiano Giuridico*, 13 gennaio 2021; V. FALCE, N. FARAONE, *Digital Markets and Competition Law Enforcement. A convergent Approach*, in V. FALCE (eds.), *Competition law enforcement in digital markets. Digital Markets and Competition Law. Interdisciplinary project for European Judges*, Giappichelli, Torino, 2021, 249 ss.; V. FALCE, N. FARAONE, *Mercati Digitali e DMA: note minime in tema di enforcement*, in *Il dir. ind.*, n. 1, 2022, 5 ss.; V. FALCE, *Digital Markets between Regulation and Competition Policy. Converging agendas*, in *European Journal of Privacy Law & Technologies*, n. 1, 2021, 9 ss.; V. FALCE, N. FARAONE, *Digital Markets Act: Profili Istituzionali*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2021, 143 ss. Per uno sguardo alla letteratura internazionale, si rimanda a P. LAROCHE, A. DE STREEL, *The European Digital Markets Act: A Revolution Grounded on Traditions*, in *Journal of European Competition Law & Practice*, n. 12, 2021, 542 ss.; N. PETIT, *The Proposed Digital Markets Act (DMA): A Legal and Policy Review*, *ivi*, 529 ss.; A. LAMADRID DE PABLO, N. BAYÓN FERNÁNDEZ, *Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and How to Fix It*, *ivi*, 576 ss.; R. PODSZUN, P. BONGARTZ, S. LANGENSTEIN, *The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers*, in *Journal of European Consumer and Market Law*, n. 2, 2021, 60 ss.; J. BAKER, *Protecting and Fostering Online Platform Competition: The Role of Antitrust Law*, in *Journal of Competition Law & Economics*, n. 2, 2021, 493 ss.; 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*, n. 1, 2022, 85 ss.; O. ANDRIYCHUK, *Shaping the New Modality of the Digital Markets: The Impact of the DSA/DMA Proposals on Inter-Platform Competition*, in *World Competition*, n. 3, 2021, 261-286; G. COLANGELO, *The European Digital Markets Act and Antitrust Enforcement: A Liaison Dangereuse*, in *European Law Review*, n. 5, 2022, 597 ss. M. POLO, A. SASSANO, *DMA: Digital Markets Act o Digital Markets Armistice*, *ivi*, 501 ss.; M. LIBERTINI, *Il Regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Riv. trim. dir. pubbl.*, fasc. 4, 2022, 1069 ss.; ID., *Digital markets and competition policy. Some remarks on the suitability of the anti-trust toolkit*, in *Orizz. dir. comm.*, 2021, 337 ss. Un dibattito sull'attuale ruolo delle regole *ex ante* per coniugare l'*enforcement ex-post* nei mercati digitali può essere rintracciato anche in CERRE Assessment Paper – The European proposal for a Digital Markets Act: A first assessment (January 2021) (“CERRE DMA Report”); L. CABRAL, J. HAUCAP, G. PARKER, G. PETROPOULOS, T. VALLETTI, M. VAN ALSTYNE, *Eur. Comm'n, The EU Digital Markets Act: A Report from a Panel of Economic Experts*, 2021. Parallelamente, anche negli Stati Uniti, l'American In-

(“DSA”)<sup>25</sup> che aggiorna la direttiva 2000/31/CE sul commercio elettronico, ha predisposto un quadro regolatorio avanzato per il contrasto degli illeciti in rete e la responsabilità per contenuti informativi illeciti e, da ultimo, il Data Governance Act (“DGA”)<sup>26</sup> che disciplina l’accesso ai dati del settore pubblico e introduce meccanismi di incentivazione alla condivisione dei dati in mano privata. Destinate ad integrarsi con tale impianto regolatorio sono due ulteriori proposte normative, la Proposta di regolamento sull’intelligenza artificiale (“AI Act”)<sup>27</sup> e la Proposta di regolamento su accesso e uso dei dati (“Data Act”)<sup>28</sup>.

Tale attivismo sul fronte regolamentare va letto in combinato con le iniziative più esplicitamente di politica industriale, in particolare con gli interventi già in essere o previsti con riferimento ad alcuni mercati digitali: il *cloud*, i microchip<sup>29</sup>, Internet of Things (“IoT”) e la sicurezza informatica<sup>30</sup>.

In conclusione, il ruolo sempre più determinante delle grandi piattaforme digitali per gli assetti e lo sviluppo dei mercati ha indotto l’Europa,

---

novation and Choice Online Act (noto anche come il “Self-Preferencing” Bill), proposto dai senatori Klobuchar e Grassley, si è mosso sul medesimo solco, almeno a livello di ispirazione ideale, delle varie proposte legislative europee. A tal riguardo, si veda Senate of the United States, American Innovation and Choice Online Act – A Bill to provide that certain discriminatory conduct by covered platforms shall be unlawful, and for other purposes, October 18, 2021. Per un’analisi comparativa tra la Proposta europea di DMA e i c.d. US Bills, si veda M. SCHNITZER, J. CRÉMER, D. DINIELLI, A. FLETCHER, P. HEIDHUES, F. SCOTT MORTON, K. SEIM, *International coherence in digital platform regulation: an economic perspective on the US and EU proposals*, in *Yale Tobin Center for Economic Policy, Policy Discussion Paper No. 5* (2021); E. FOX, *Platforms, Power, and the Antitrust Challenge: A Modest Proposal to Narrow the U.S.-Europe Divide*, in *Nebraska Law Review*, 98, 2019, 297 ss.

<sup>25</sup> 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).

<sup>26</sup> Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

<sup>27</sup> Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull’intelligenza artificiale (Legge sull’Intelligenza Artificiale) e modifica alcuni atti legislativi dell’Unione, Bruxelles, 21 aprile 2021 COM(2021)206 final 2021/0106(COD).

<sup>28</sup> Proposta di Regolamento del Parlamento Europeo e del Consiglio riguardante norme armonizzate sull’accesso equo ai dati e sul loro utilizzo (normativa sui dati), Bruxelles, 23 febbraio 2022 COM(2022)68 final 2022/0047(COD).

<sup>29</sup> Proposta di Regolamento del Parlamento Europeo e del Consiglio che istituisce un quadro di misure per rafforzare l’ecosistema europeo dei semiconduttori (normativa sui chip), Bruxelles, 8 febbraio 2022 COM(2022)46 final 2022/0032(COD).

<sup>30</sup> Comunicazione congiunta al Parlamento Europeo e al Consiglio, La strategia dell’UE in materia di cybersicurezza per il decennio digitale, Bruxelles, 16 dicembre 2020 JOIN(2020) 18 final.

ma anche altri Paesi (Stati Uniti, Australia e, ultimamente, la Cina), a rivedere l'approccio finora seguito, fondamentalmente basato sull'applicazione della disciplina *antitrust* per azionare diverse leve: dalla revisione della strumentazione *antitrust* "tradizionale" all'introduzione di una specifica regolazione dei mercati e delle piattaforme digitali, dalla promozione di interventi di politica industriale settoriale alla previsione di un sistema di tassazione delle multinazionali tecnologiche. Nelle pagine che seguono, l'attenzione verrà ad appuntarsi soltanto sul DMA e sulla sua interazione con le norme a tutela della concorrenza europee e nazionali.

### 3. Il cumulo di procedimenti e sanzioni nel Digital Markets Act

Come detto, l'Unione europea è alla vigilia dell'introduzione e della "messa a terra" di un epocale pacchetto di riforme.

Dal momento che il diritto *antitrust* non è stato ritenuto in grado di affrontare efficacemente le sfide e i problemi "strutturali" posti dall'ecosistema delle piattaforme e dall'irrompere onnipresente dell'economia dei dati nel mercato, la Commissione, con l'introduzione del DMA, ha "disegnato" una cornice normativa che integrasse le tradizionali disposizioni a tutela della concorrenza con l'obiettivo di assicurare contendibilità e equità nei mercati digitali<sup>31</sup>. A tal proposito, quantunque, come si vedrà innanzi, gli artt. 101 e 102 TFUE rimangano astrattamente applicabili, la proposta del DMA introduce una nuova serie di obbligazioni *ex ante* per le piattaforme *online* designate come *gatekeeper*<sup>32</sup> ed esonera le autorità competenti dal definire i mercati rilevanti, dal dimostrare eventuali posizioni dominanti e dal misurare potenziali effetti anti-concorrenziali<sup>33</sup>. D'altronde,

---

<sup>31</sup> In tema di *fairness* e *contestability* quali principi ispiratori del DMA, si rimanda, tra gli altri, a G. BRUZZONE, *op. cit.*, 328 ss. e, più in generale, D. GERARD, *Fairness in EU Competition Policy: Significance and Implications*, in *Journal of European Competition Law & Practice*, n. 4, 2018, 211 ss. e N. DUNNE, *Fairness and the Challenge of Making Markets Work Better*, in *Modern Law Review*, n. 2, 2021, 230 ss. Come noto, il dibattito degli ultimi anni ha rivalutato il concetto di *fairness* e di equità, anche con riscontri in diritto positivo (si vedano i Cons. 1 e 6 della direttiva (UE) 2019/1; ma i riferimenti all'equità si rinvengono anche nelle norme originarie del Trattato, in particolare l'art. 102, par. 2, lett. a. Per di più, i riferimenti alla *fair competition* sono stati largamente impiegati nella comunicazione pubblica delle autorità europee, nell'ultimo decennio (si veda *Fairness and competition*, Speech by Commissioner Margrethe Vestager, GCLC Annual Conference, Brussels, 25 January 2018).

<sup>32</sup> Per una panoramica delle obbligazioni cui sono onerati i *gatekeeper* ai sensi del DMA, si veda P. MANZINI, *op. cit.*, 40 ss.

<sup>33</sup> Sotto questo profilo, si spiega perché la base giuridica prescelta è rappresentata dall'art.

nei mercati digitali, la definizione dei mercati rilevanti è sempre stata foriera di accese controversie, tenuto conto della natura conglomerale degli intermediari operanti nei mercati a più versanti e delle caratteristiche strutturali delle transazioni economiche digitali. Non meno farraginoso è parso anche l'individuazione di un chiaro pregiudizio al consumatore proprio perché, ad esempio, alcune piattaforme digitali si basano su modelli c.d. "zero-price" e sull'abbattimento dei costi di ricerca e transazione che caratterizzano tali mercati.

In altri termini, piuttosto che incidere sul "merito" delle norme a tutela della concorrenza, il nuovo regime del DMA è intervenuto su un più generale quadro procedurale e istituzionale al fine di "catturare" condotte puntuali che, in passato, erano state fatte oggetto di specifiche istruttorie *antitrust* da parte della Commissione europea e delle autorità garanti nazionali<sup>34</sup> e che, ora, proprio in ragione di quella farraginosità e scarsa efficacia di cui si dava conto più sopra, necessitano di strumenti più duttili e celeri per essere "disinnescate"<sup>35</sup>.

Il risultato ultimo è stato, quindi, quello di lasciare inalterate le diverse legislazioni nazionali esistenti, e non precludere agli Stati membri la possi-

---

114 TFUE: perché la Commissione, più che intervenire sugli obblighi già esistenti, mira ad introdurre una nuova regolamentazione della materia. In altri termini, si percepisce la diffusa sensazione che, date le peculiarità dei mercati digitali, la "speciale responsabilità" che generalmente incombe sulle imprese dominanti, sia, di fatto, un criterio insufficiente a garantire un effettivo pluralismo del mercato. L'idea di fondo del legislatore europeo sembra, quindi, rinvenibile nella *ratio* di porre taluni obblighi aggiuntivi, in modo da anticipare l'effetto della normativa *antitrust* ed evitare l'insorgenza stessa di condotte preoccupanti dal punto di vista concorrenziale.

<sup>34</sup> Si rimanda *supra* alle note 6-11.

<sup>35</sup> Si rimanda agli autorevoli contributi di stampo accademico e *policy-oriented* citati alla nota 17. Più nello specifico, secondo M. LIBERTINI, *Il Regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, cit., 1069 ss., l'affermazione secondo cui le norme *antitrust* tradizionali sarebbero insufficienti a contenere lo strapotere dei c.d. Big Tech appare destituita di fondamento e tendenzialmente smentita dal moltiplicarsi di procedimenti per abuso di posizione dominante susseguitisi negli ultimi anni, su iniziativa della Commissione e di diverse autorità nazionali. Anzi, secondo l'A., «[i]l vero limite delle norme *antitrust* tradizionali sta dunque, piuttosto, nei profili rimediali e procedurali: esse prevedono interventi solo ex post, con procedimenti lunghi, complessi e costosi, e con la necessità di affrontare dispute interpretative di esito non scontato, ed oneri probatori non indifferenti. È sotto questo profilo che si manifesta la differenza netta del DMA con il diritto *antitrust* e si comprende l'idea della "complementarità" fra i due corpi normativi [...]. L'insufficienza del diritto *antitrust* tradizionale si manifesta, dunque, sotto il profilo organizzativo. Da qui la scelta – certo discutibile ma comunque di grande impatto – di intervenire con un apparato normativo rigido e di immediata applicazione, come quello contenuto nel DMA, che è diverso non solo dal tipico intervento sanzionatorio ex post del diritto *antitrust*, ma anche dalla regolazione di settore tradizionale, che lascia ampia discrezionalità regolamentare alle autorità di settore, nel quadro di principi generali fissati a livello normativo».

bilità di adottare nuove disposizioni di natura legislativa e/o regolamentare potenzialmente divergenti. Con la conseguenza che, “centralizzando” l’attività di *enforcement* del DMA a livello della Commissione europea e non “irreggimentando” l’attività di produzione legislativa degli Stati membri sulle medesime materie (a patto che, idealmente, la nuova normativa trovi applicazione anche per soggetti diversi dai *gatekeeper*), l’effetto ultimo del DMA sarebbe quello di incentivare la proliferazione di legislazioni nazionali parallele, col rischio di una maggiore frammentazione normativa (che è esattamente ciò che si è voluto scongiurare da principio, ponendo come base normativa per l’adozione del DMA proprio l’art. 114 TFUE). È esattamente lo scenario che si è già verificato a seguito dell’entrata in vigore, in data 18 gennaio 2021, della decima modifica della Legge contro le restrizioni della concorrenza (“GWB”), che ha introdotto il nuovo articolo 19(a)<sup>36</sup> ma anche della novella italiana in tema di abuso di dipendenza economica di cui si darà conto *infra*.

---

<sup>36</sup>In data 18 gennaio 2021 è entrata in vigore la decima modifica della Legge contro le restrizioni della concorrenza (Gesetz gegen Wettbewerbsbeschränkungen, GWB), che mira a riformare il quadro precedente al fine di produrre una disciplina proattivamente indirizzata al comparto digitale. La Sezione 19(a) del GWB assoggetta al controllo del Bundeskartellamt un nuovo *genus* di imprese, ossia quelle attive su mercati multilaterali e che rivestono un’importanza primaria per la concorrenza trasversale tra i mercati (“*paramount cross-market significance*”). Queste vengono individuate attraverso un elenco non esaustivo di criteri non cumulativi quali, tra gli altri, una posizione dominante in uno o più mercati, l’accesso ai dati, il potere finanziario e l’integrazione verticale, di modo da permettere al Bundeskartellamt di condurre un’analisi *cross-market* e di prevenire forme di espansione abusiva nei mercati non dominati. Una volta stabilito che un’impresa riveste fondamentale importanza *cross-market*, il Bundeskartellamt può proibirle di porre in essere pratiche ritenute abusive nel particolare contesto quali, tra le altre, ostacolare i concorrenti su mercati in cui l’impresa potrebbe espandere rapidamente la propria posizione, creare barriere all’entrata in un mercato sfruttando i dati raccolti in un altro mercato in cui l’impresa è in una posizione dominante, limitare l’interoperabilità dei prodotti o la portabilità dei dati nonché la *self-preferencing*, ossia, favorire i propri prodotti rispetto a quelli dei concorrenti. Inoltre, lo scorso 5 gennaio 2022, il Bundeskartellamt ha annunciato di voler assoggettare Google e Alphabet ai nuovi obblighi *antitrust* per le imprese che rivestono importanza fondamentale per la concorrenza nei mercati di cui alla Sezione 19(a) GWB (si veda Bundeskartellamt’s press release, Alphabet/Google subject to new abuse control applicable to large digital companies – Bundeskartellamt determines ‘paramount significance across markets’, 5 January 2022). Più di recente, il 4 maggio 2022 e il 6 luglio 2022, il Bundeskartellamt ha formalmente determinato lo *status* di impresa che riveste “importanza fondamentale per la concorrenza tra mercati” per Meta (si veda Bundeskartellamt’s press release, new rules apply to Meta (formerly Facebook) – Bundeskartellamt determines its ‘paramount significance for competition across markets’, 4 May 2022) e per Amazon (si veda Bundeskartellamt’s press release, Amazon now subject to stricter regulations – Bundeskartellamt determines its paramount significance for competition across markets (Section 19a GWB), 6 July 2022). Lo scorso 28 marzo 2023, il Bundeskartellamt ha avviato un’istruttoria nei confronti di Microsoft per determinare se sussiste lo *status* di impresa che riveste “importanza fondamentale per la concorrenza tra merca-

Dal punto di vista operativo, assetto “principe” per l’attuazione di tale dichiarazione d’intenti (e del DMA) è una forte centralizzazione attuativa in capo alla Commissione europea<sup>37</sup>, che, come detto, differenzia nettamente il DMA dall’assetto istituzionale del diritto della concorrenza. Quest’ultimo, sulla scorta del regolamento (CE) di modernizzazione n. 1/2003 (“reg. n. 1/2003”)<sup>38</sup>, è improntato, infatti, a un diffuso decentramento applicativo, che si applica anche ad altri quadri regolatori pro-concorrenziali, come quello delle comunicazioni elettroniche, la cui attuazione è dislocata a livello nazionale per consentire alle autorità di regolazione di modellare l’applicazione delle regole alle circostanze del mercato nazionale e agli operatori aventi dimensione nazionale<sup>39</sup>.

Ciò premesso, che esista, però, un *continuum* ideale tra norme a tutela della concorrenza e DMA è indubbio, al punto che l’ECN (vale a dire, la rete europea delle autorità garanti nazionali) e alcuni Stati membri hanno proposto che le autorità nazionali garanti della concorrenza siano maggiormente coinvolte nel processo di attuazione e applicazione della nuova regolamentazione e che, anzi, siano autorizzate a far rispettare le obbligazioni cui saranno onerati i *gatekeeper* a valle dell’approvazione del DMA. Come detto, tale assunto si poneva alla base della “levata di scudi” del-

---

ti” (si veda Bundeskartellamt’s press release, Examination of Microsoft’s significance for competition across markets, 28 March 2023).

<sup>37</sup> Secondo il DMA, la Commissione europea ha la competenza esclusiva per la designazione dei *gatekeeper*, con il potere di avviare delle indagini di mercato (art. 17) al fine di a) valutare se imprese che soddisfano i parametri quantitativi non soddisfano quelli qualitativi (art. 3.4); b) stabilire se imprese che non soddisfano i criteri quantitativi soddisfino tuttavia quelli qualitativi (art. 3.8) e c) adeguare le soglie quantitative all’art. 3.2 (art. 3.6). La Commissione emana, inoltre, decisioni in cui: d) indica ai *gatekeeper* misure specifiche da tenere per conformarsi agli obblighi regolatori, nel caso in cui la Commissione stessa constati che gli obblighi che l’impresa intenda attuare o abbia già attuato non ne garantiscano l’osservanza (art. 8), e) sospende, in via eccezionale, integralmente o in parte, un obbligo regolatorio su richiesta motivata dal *gatekeeper* (art. 9), f) accerta l’inosservanza degli obblighi regolamentari (art. 29) e irroga ammende monetarie fino al 10% del fatturato annuo (art. 30), g) impone misure cautelari (art. 24) e accetta impegni (art. 25). Inoltre, la Commissione ha il potere esclusivo di h) imporre rimedi comportamentali (o strutturali, se i primi non sono sufficienti) proporzionati alle violazioni commesse e necessari per garantire il rispetto del regolamento, a seguito di un’indagine di mercato ai sensi dell’art. 18 in cui si accetti che il *gatekeeper* abbia violato sistematicamente gli obblighi e abbia così ulteriormente rafforzato o ampliato la sua posizione di *gatekeeper*. Infine, la Commissione è competente in via esclusiva a i) proporre emendamenti al regolamento al fine di aggiornare la lista dei servizi di piattaforma di base, sulla base di un’indagine di mercato a norma dell’art. 19.

<sup>38</sup> Regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l’applicazione delle regole di concorrenza, di cui agli artt. 81 e 82 del Trattato.

<sup>39</sup> Si rimanda la nota 13.

l'ECN nel suo Joint Paper del giugno 2021<sup>40</sup>, ma già prima se ne trovava evidenza in un *paper*, risalente al maggio 2021 (poi “trasfuso” in una lettera ufficiale pubblicata il successivo 7 settembre 2021, che ha impegnato i governi complessivamente), in cui i ministri dell'Economia di Francia, Germania e Olanda, auto-definitisi, non senza enfasi, “Friends of an effective Digital Markets Act”, puntavano l'attenzione sulla necessità di garantire un maggiore “spazio di manovra” alle autorità nazionali di concorrenza in sede di applicazione del DMA, un rafforzamento del loro ruolo, suggerendo l'introduzione di un meccanismo di stretto coordinamento e cooperazione, mutuato dalla complementarietà dell'*enforcement* dell'art. 3, reg. n. 1/2003<sup>41</sup>.

Tale orientamento è stato sigillato definitivamente anche nel testo finale del DMA che, all'art. 38, ha consentito alle autorità nazionali garanti

---

<sup>40</sup> “Joint paper of the heads of the national competition authorities of the European Union, How national competition agencies can strengthen the DMA”. Il documento è stato adottato nel corso della riunione dei direttori generali dell'ECN del 22 giugno 2021.

<sup>41</sup> Germany, France and the Netherlands, Strengthening the Digital Markets Act and its Enforcement, 7 September 2021. Più di recente, lo scorso 13 marzo 2023, il Ministero degli Affari Economici e del Clima dei Paesi Bassi ha pubblicato la prima bozza del regolamento di attuazione, soggetto a consultazione pubblica fino al 10 aprile 2023, per attribuire all'autorità garante della concorrenza olandese il potere di monitorare la *compliance* al DMA nel territorio nazionale (a tal riguardo, si rimanda al seguente *link*: <https://www.internetconsultatie.nl/uitvoeringswetdma/b1#sectie-waarkuntuopreageren>). Tale aggiornamento si pone nel solco di quanto già avvenuto in Ungheria, dove, già a partire dal 1 gennaio 2023, è stata modificata la legge *antitrust* nazionale per conferire poteri investigativi all'autorità garante per la concorrenza nazionale per garantire il rispetto delle disposizioni del DMA (anche qui, si veda il seguente *link*: [https://www.gvh.hu/en/press\\_room/press\\_releases/press-releases-2023/changes-in-competition-law-expanding-gvh-toolbox-and-less-administrative-burden-for-undertakings](https://www.gvh.hu/en/press_room/press_releases/press-releases-2023/changes-in-competition-law-expanding-gvh-toolbox-and-less-administrative-burden-for-undertakings)). Anche la Germania sta riconsiderando di porre mano alla legge *antitrust* nazionale e ciò emerge da un recente documento fatto circolare dal Governo federale lo scorso 27 marzo 2023, dal titolo “DMA Enforcement Priorities”. Sul punto, secondo G. BRUZZONE, *op. cit.*, 337 ss., «la soluzione prospettata dalle autorità di concorrenza degli Stati membri di avvalersi dell'architettura dell'European Competition Network presenta una serie di vantaggi. Anzitutto, questa soluzione consentirebbe di avvalersi da subito di meccanismi di enforcement consolidati, che coinvolgono sia la Commissione attraverso la Direzione generale concorrenza, che le autorità nazionali. Verrebbe così soddisfatta una delle principali esigenze del DMA, ossia quella di agire rapidamente per preservare una concorrenza effettiva nei mercati digitali. Un ulteriore beneficio dell'attribuzione della competenza alla rete delle autorità di concorrenza consiste nel fatto che, disponendo anche degli strumenti *antitrust*, queste autorità potrebbero ottimizzare gli interventi scegliendo, a seconda dei casi, lo strumento più adatto, prevenendo quelle duplicazioni inutili e foriere di contenzioso che spesso caratterizzano i rapporti tra regolazione e concorrenza quando le competenze sono affidate a autorità diverse tra loro. Tra i motivi che suggeriscono di fare riferimento per l'enforcement alla rete della autorità di concorrenza vi è anche la sinergia tra l'obbligo per i gatekeeper, ai sensi dell'art. 12 della proposta di DMA, di informare la Commissione europea di tutti i progetti di operazioni di concentrazione nel settore digitale e il sistema di controllo delle concentrazioni previsto dal regolamento (CE) n. 139/2004».

della concorrenza di effettuare indagini ai sensi del DMA, in stretto coordinamento con la Commissione cui riferisce, da ultimo, i risultati dell'istruttoria, sempre al fine di preservare l'architettura applicativa centralizzata del DMA in capo alla Commissione<sup>42</sup>. Ancor più chiaramente si pronuncia il nuovo art. 37, secondo cui «[l]a Commissione e gli Stati mem-

---

<sup>42</sup> Si legge, infatti, all'art. 38 DMA, rubricato "Cooperazione e coordinamento con le autorità nazionali competenti che applicano le norme in materia di concorrenza": «1. La Commissione e le autorità nazionali competenti degli Stati membri responsabili dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, collaborano e si scambiano informazioni sulle rispettive azioni di esecuzione attraverso la rete europea della concorrenza (ECN). Esse hanno il potere di comunicarsi reciprocamente qualsiasi informazione concernente un elemento di fatto o di diritto, comprese le informazioni riservate. Qualora l'autorità competente non sia membro dell'ECN, la Commissione adotta le disposizioni necessarie per la cooperazione e lo scambio di informazioni sui casi riguardanti l'applicazione del presente regolamento e l'applicazione delle norme nei casi di cui all'articolo 1, paragrafo 6, da parte di tali autorità. La Commissione può stabilire tali disposizioni in un atto di esecuzione, conformemente all'articolo 46, paragrafo 1, lettera l). 2. Qualora un'autorità nazionale competente di uno Stato membro responsabile dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, intenda avviare un'indagine sui gatekeeper sulla base della legislazione nazionale di cui all'articolo 1, paragrafo 6, tale autorità informa la Commissione per iscritto della prima misura formale di indagine, prima dell'avvio di tale misura o immediatamente dopo di esso. Tali informazioni possono essere fornite anche alle autorità nazionali competenti degli altri Stati membri che applicano le norme di cui all'articolo 1, paragrafo 6. 3. Qualora un'autorità nazionale competente di uno Stato membro responsabile dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, intenda imporre obblighi ai gatekeeper sulla base della legislazione nazionale di cui all'articolo 1, paragrafo 6, tale autorità comunica alla Commissione, al più tardi 30 giorni prima della sua adozione, il progetto di misura indicandone i motivi. Nel caso di misure provvisorie, l'autorità nazionale competente di uno Stato membro responsabile dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, comunica alla Commissione il progetto di misure previste quanto prima e al più tardi immediatamente dopo l'adozione di tali misure. Tali informazioni possono essere fornite anche alle autorità nazionali competenti degli altri Stati membri che applicano le norme di cui all'articolo 1, paragrafo 6. 4. I meccanismi di informazione di cui ai paragrafi 2 e 3 non si applicano alle decisioni previste ai sensi delle norme nazionali sulle concentrazioni. 5. Le informazioni scambiate a norma dei paragrafi da 1 a 3 del presente articolo sono scambiate e utilizzate unicamente ai fini del coordinamento dell'applicazione del presente regolamento e delle norme di cui all'articolo 1, paragrafo 6. 6. La Commissione può chiedere alle autorità nazionali competenti degli Stati membri responsabili dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, di sostenere le sue indagini di mercato a norma del presente regolamento. 7. Se dotata della competenza e dei poteri di indagine previsti a tal fine dal diritto nazionale, un'autorità nazionale competente di uno Stato membro responsabile dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, può, di sua iniziativa, svolgere nel suo territorio un'indagine su un caso di possibile non conformità agli articoli 5, 6 e 7 del presente regolamento. Prima di adottare la prima misura formale di indagine, tale autorità ne informa la Commissione per iscritto. L'apertura, da parte della Commissione, di un procedimento a norma dell'articolo 20 preclude alle autorità nazionali competenti degli Stati membri responsabili dell'applicazione delle norme di cui all'articolo 1, paragrafo 6, la possibilità di condurre tale indagine o determina la sua conclusione qualora essa sia già in corso. Tali autorità riferiscono alla Commissione in merito ai risultati dell'indagine al fine di sostenere la Commissione nel suo ruolo di unica autorità preposta all'applicazione del presente regolamento».

*bri operano in stretta collaborazione e coordinano le loro azioni di esecuzione per garantire un'applicazione coerente, efficace e complementare degli strumenti giuridici disponibili applicati ai gatekeeper», ben potendo la stessa «consultare le autorità nazionali, ove opportuno, su qualsiasi questione relativa all'applicazione del [DMA]»<sup>43</sup>.*

Riassumendo, la Commissione europea si trova, dunque, nella posizione privilegiata secondo la quale l'applicazione del diritto della concorrenza avverrà, almeno in linea di principio, in parallelo alla supervisione e all'applicazione del DMA<sup>44</sup> e sarà ben possibile, dunque, che una piattaforma digitale possa essere assoggettata a molteplici procedimenti a valle della commissione della medesima condotta – ciascuno dei quali avviato sulla base di un quadro normativo diverso –, ponendosi così la questione se ciò sia compatibile con il principio del *ne bis in idem*<sup>45</sup>. A più riprese, sia nel

---

<sup>43</sup> Secondo l'art. 37 DMA, rubricato "Cooperazione con le autorità nazionali", «1. La Commissione e gli Stati membri operano in stretta collaborazione e coordinano le loro azioni di esecuzione per garantire un'applicazione coerente, efficace e complementare degli strumenti giuridici disponibili applicati ai gatekeeper ai sensi del presente regolamento. 2. La Commissione può consultare le autorità nazionali, ove opportuno, su qualsiasi questione relativa all'applicazione del presente regolamento». Non v'è dubbio che sia l'art. 38 che l'art. 37, benché non strutturate in maniera altrettanto precisa, siano norme ispirate a quelle dettate dal reg. n. 1/2003, che impone alle autorità nazionali di concorrenza (art. 11) l'obbligo di informare tempestivamente la Commissione dell'avvio di un procedimento di applicazione decentrata delle norme *antitrust* europee. In tal caso, la Commissione ha il potere di avocare a sé il caso e le autorità nazionali sono, comunque, vincolate a non adottare provvedimenti che contrastino con decisioni della Commissione.

<sup>44</sup> In questo scenario, la stessa impresa sarebbe ipoteticamente assoggettata a due istruttorie avviate dalla Commissione europea, la prima ai sensi del DMA e l'altra ai sensi del diritto della concorrenza dell'Unione (artt. 101 e/o 102 TFUE). Tale scenario si risolverà in un mero caso di scuola, una fattispecie puramente teorica. È improbabile, infatti, che la Commissione conduca un'istruttoria avente ad oggetto la medesima condotta sia ai sensi del DMA sia delle norme europee a tutela della concorrenza. Si può ipotizzare che, in tal caso, la Commissione europea faccia ricorso principalmente agli strumenti regolatori del DMA, non foss'altro perché questi ultimi non richiedono che la Commissione definisca i mercati rilevanti, valuti il potere di mercato e dimostri gli effetti anticoncorrenziali. D'altronde, è la genesi stessa della Proposta della Commissione a suggerire, in caso di eventuali *overlapping*, l'adozione degli ampi poteri di regolazione accordati dal DMA (compresi quelli di imporre rimedi comportamentali o strutturali) in luogo delle norme a tutela della concorrenza, se non altro perché – ragionando diversamente – il DMA ne risulterebbe depotenziato ancor prima della sua effettiva entrata in vigore.

<sup>45</sup> Tra i contributi più recenti, sul punto, si rimanda a K. BANIA, *Fitting the Digital Markets Act in the existing legal framework: the myth of the "without prejudice" clause*, in *European Competition Journal*, 2022, 1 ss.; J. VAN DEN BOOM, *What does the Digital Markets Act harmonize? – exploring interactions between the DMA and national competition laws*, *ivi*, 2022, 1 ss.; A. RIBERA MARTINEZ, *An inverse analysis of the digital markets act: applying the Ne bis in idem principle to enforcement*, *ivi*, 2022, 1 ss. Occorre, però, segnalare, che un ulteriore livello di macchinosità è stato introdotto, inoltre, dal considerando 86 del nuovo testo del DMA. Con

testo finale del DMA sia nel documento congiunto pubblicato, lo scorso 22 giugno 2021, dalla rete europea delle autorità garanti della concorrenza, si è ribadito che le ANC (vale a dire, le autorità garanti della concorrenza nazionali) dovrebbero svolgere un ruolo complementare a quello della Commissione, unitamente alla creazione di un meccanismo virtuoso di coordinazione e cooperazione, proprio mutuato dalla rete dell'ECN inaugurata dal reg. n. 1/2003. Ma, ciononostante, tale (benvenuto) accorgimento di politica del diritto non è risultato in grado di sopire tutti i potenziali elementi di conflittualità.

La Commissione europea, ad oggi, ha apparentemente tentato di eludere la questione, appellandosi alla circostanza secondo cui il DMA è strumento regolatorio complementare al diritto della concorrenza e «*lascia [...] impregiudicata l'applicazione: delle norme nazionali che vietano accordi anticoncorrenziali, decisioni delle associazioni di imprese, pratiche concordate*

---

riguardo al tema delle sanzioni e delle penali di mora per il mancato rispetto delle obbligazioni previste dal Regolamento, la Commissione e le autorità nazionali competenti dovranno coordinare i loro sforzi applicativi per garantire il rispetto dei principi di proporzionalità e del *ne bis in idem*. In particolare – continua il considerando 86 –, la Commissione dovrà tener conto di eventuali ammende e sanzioni inflitte alla medesima entità giuridica per gli stessi fatti a seguito di una statuizione divenuta definitiva in un procedimento relativo a una violazione di altre norme dell'Unione o “domestiche”, di modo da garantire che le ammende e le sanzioni complessive inflitte siano parametrizzate alla gravità delle infrazioni commesse. Come detto, tali sforzi di coordinamento saranno indirizzati sia verso eventuali istruttorie *antitrust* avviate nei confronti dei *gatekeeper* a livello dell'Unione sia verso procedimenti avviati dalle autorità garanti nazionali competenti. A riprova di ciò, il nuovo testo del DMA sottolinea che la Commissione europea deve rispettare il principio di leale collaborazione fissato dall'art. 4 TFUE nei rapporti con le autorità nazionali garanti della concorrenza, specialmente allorquando queste ultime supportino (e condividano l'onere del)le istruttorie con i dovuti scambi di informazioni e con la notifica preventiva in sede di avvio di un'istruttoria contro i *gatekeeper* (si vedano i considerando nn. 90, 91 e 98 e gli artt. 37 e 38 del testo finale). Con riguardo alle richieste di informazioni, l'art. 21, par. 5 stabilisce che gli Stati membri dovranno fornire alla Commissione tutte le informazioni necessarie in loro possesso per svolgere i compiti assegnati istituzionalmente alla Commissione ai fini della piena applicazione del DMA. Inoltre, ai sensi dell'art. 26, par. 2, i funzionari delle autorità garanti degli Stati membri collaboreranno al monitoraggio delle obbligazioni e delle misure adottate ai sensi del DMA. Si riporta, qui di seguito, il considerando 86 secondo cui «[è] opportuno che l'osservanza degli obblighi imposti dal presente regolamento sia assicurata mediante ammende e penali di mora. È a tal fine opportuno fissare anche livelli adeguati di ammende e penali di mora, soggette a ragionevoli termini di prescrizione, per l'inosservanza degli obblighi e per la violazione delle norme procedurali, conformemente ai principi di proporzionalità e *ne bis in idem*. È opportuno che la Commissione e le pertinenti autorità nazionali coordinino i loro sforzi di applicazione al fine di garantire il rispetto di tali principi. In particolare, la Commissione dovrebbe tenere conto di eventuali ammende e penali irrogate alla stessa persona giuridica per gli stessi fatti mediante una decisione definitiva nei procedimenti relativi a una violazione di altre norme dell'Unione o nazionali, in modo da garantire che l'importo complessivo delle ammende e delle penali irrogate corrisponda alla gravità delle infrazioni commesse».

*te e abusi di posizione dominante; delle norme nazionali in materia di concorrenza che vietano altre forme di comportamento unilaterale nella misura in cui sono applicate a imprese diverse dai gatekeeper o equivalgono a imporre obblighi aggiuntivi ai gatekeeper [...]*»<sup>46</sup>.

Inoltre, secondo il considerando 10, il DMA «*mira a integrare l'applicazione del diritto della concorrenza*», e, quindi, «*lascia impregiudicati gli articoli 101 e 102 del TFUE, le corrispondenti norme nazionali in materia di concorrenza e altre norme nazionali in materia di concorrenza relative ai comportamenti unilaterali basati su una valutazione caso per caso delle posizioni e dei comportamenti di mercato, compresi i relativi effetti probabili e l'ambito di applicazione preciso del comportamento vietato, e che prevedono la possibilità per le imprese di invocare giustificazioni oggettive di efficienza rispetto al comportamento in questione*».

Analogamente, il considerando 11 del DMA stabilisce che quest'ultimo «*persegue un obiettivo complementare, ma diverso, alla protezione della concorrenza non falsata su un dato mercato, quale definita in termini di diritto della concorrenza, e tale obiettivo consiste nel garantire che i mercati in cui sono presenti gatekeeper siano e rimangano equi e contendibili, indipendentemente dagli effetti reali, potenziali o presunti sulla concorrenza in un dato mercato del comportamento di un dato gatekeeper*», ribadendo che il DMA «*mira pertanto a proteggere un interesse giuridico diverso rispetto a quello protetto da tali norme [di concorrenza] e dovrebbe applicarsi senza pregiudicare l'applicazione di queste ultime*»<sup>47</sup>.

L'art. 1, parr. 5 e 6 (nonché i consideranda 10 e 11) – che impongono una lettura dell'applicazione del DMA “senza pregiudizio” rispetto alle norme a tutela della concorrenza – parrebbero suggerire, quindi, che tutti gli strumenti legislativi che regolano le condotte delle piattaforme e dei *gatekeeper* (sia nell'Unione che a livello nazionale) possano coesistere armoniosamente e si completino a vicenda.

Non solo: dal punto di vista teoretico, una soluzione così congegnata

---

<sup>46</sup> Cfr. art. 1, par. 6, DMA, che aggiunge che «[i]l presente regolamento non pregiudica l'applicazione degli articoli 101 e 102 TFUE».

<sup>47</sup> Parallelamamente, secondo l'art. 1, par. 5, «[a]l fine di evitare la frammentazione del mercato interno, gli Stati membri non impongono ai gatekeeper ulteriori obblighi per mezzo di leggi, regolamenti o disposizioni amministrative allo scopo di garantire l'equità e la contendibilità dei mercati. Nessuna disposizione del presente regolamento impedisce agli Stati membri di imporre obblighi alle imprese, comprese le imprese che forniscono servizi di piattaforma di base, per questioni che non rientrano nell'ambito di applicazione del presente regolamento, purché tali obblighi siano compatibili con il diritto dell'Unione e non derivino dal fatto che le imprese pertinenti hanno lo status di gatekeeper ai sensi del presente regolamento».

avrebbe dovuto “placare” eventuali perplessità circa la possibile duplicazione dei procedimenti, muovendo dall’assunto che i diversi quadri normativi (DMA e regole a tutela della concorrenza, principalmente) presidino e tutelino interessi giuridici diversi.

Sospendendo il giudizio circa la bontà della soluzione “tecnica” individuata dalla Commissione, l’eventualità che la prima indagine sia avviata dalla Commissione sulla base del DMA, mentre la seconda da un’autorità garante di uno Stato membro ai sensi delle norme europee e/o nazionali a tutela della concorrenza rappresenta di gran lunga lo scenario più probabile nella pratica<sup>48</sup>. Tale circostanza potrebbe scaturire dalla tentazione delle autorità garanti nazionali di “affrancarsi” dalla presenza “ingombrante” della regolazione *ex-ante* del DMA e utilizzare la normativa *antitrust* “domestica” (come si diceva, “fatta salva” dai consideranda 10 e 11) per conseguire, così, un risultato più eclatante, in termini di impatto sanzionatorio dell’istruttoria<sup>49</sup>. È esattamente quanto accaduto nel caso Amazon, sanzionato dall’AGCM, lo scorso 30 novembre 2021, per €1,3 miliardi per abuso di posizione dominante *ex art.* 102 TFUE per una condotta abusiva attuata nelle forme del *self-preferencing*<sup>50</sup>.

---

<sup>48</sup> Ad avviso di M. LIBERTINI, *Il Regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, cit., 1069 ss., «[...] non può dirsi dunque che il ruolo delle autorità nazionali sia azzerato (a parte il ruolo ausiliario che possono avere nell’applicazione diretta delle norme del DMA da parte della Commissione)», sottolineando, al tempo stesso, «il rischio di incoerenza fra la disposizione del par. 5 [il riferimento è all’art. 1], che vieta agli Stati membri di “imporre ulteriori obblighi ai gatekeeper”, e le disposizioni del par. 6 [sempre dell’art. 1], che lasciano alle autorità nazionali ampie possibilità di intervento». In ogni caso, il dibattito è ben lungi dal placarsi, nonostante il DMA preveda, all’art. 1, par. 7, che le autorità nazionali (senza distinzioni, quindi sia quelle amministrative sia quelle giudiziarie) non possono adottare decisioni contrastanti con decisioni adottate dalla Commissione in applicazione di norme del DMA. Circostanza confermata anche dal considerando 92, secondo cui occorre garantire che le autorità nazionali, compresi gli organi giurisdizionali nazionali, dispongano di tutte le informazioni necessarie per far sì che le loro decisioni non siano in contrasto con una decisione adottata dalla Commissione.

<sup>49</sup> Se questo è l’orientamento di fondo, non stupisce l’inserimento, nella versione definitiva del DMA, dell’art. 41, rubricato “Richiesta di un’indagine di mercato”, secondo cui tre o più Stati membri possono chiedere alla Commissione di avviare un’indagine di mercato a norma degli artt. 17, 18 e 19 perché ritengono che vi siano motivi ragionevoli per sospettare che un’impresa debba essere designata come *gatekeeper*, perché ritengono che vi siano motivi ragionevoli per sospettare che un *gatekeeper* abbia sistematicamente violato uno o più degli obblighi sanciti dagli artt. 5, 6 e 7 e abbia mantenuto, rafforzato o ampliato la sua posizione di *gatekeeper*, perché ritengono che vi siano motivi ragionevoli per sospettare che: a) uno o più servizi del settore digitale debbano essere aggiunti all’elenco dei servizi di piattaforma di base di cui all’art. 2, punto 2); o b) una o più pratiche non siano affrontate in maniera efficace dal presente regolamento e potrebbero limitare la contendibilità dei servizi di piattaforma di base o essere sleali.

<sup>50</sup> AGCM, caso A528 – FBA Amazon, 30 novembre 2021, in *Boll.* n. 49/2021. L’AGCM ha

La recente casistica dell'AGCM rappresenta, quindi, *in nuce* un banco di prova privilegiato dello “stato di salute” dell'*enforcement antitrust* a livello nazionale nei mercati digitali e un'ulteriore anticipazione della duplicazione di procedimenti cui si assisterà a valle dell'entrata in vigore del DMA<sup>51</sup>.

---

condannato Amazon ad una sanzione superiore a €1,128 miliardi per abuso di posizione dominante, in cui le condotte contestate consistevano in un trattamento preferenziale dei prodotti Amazon e di quelli dei rivenditori indipendenti che si avvalgono dei servizi offerti da Amazon sul mercato “a valle” (in particolare, il riferimento è al servizio denominato Fulfillment by Amazon – FBA). Più nello specifico, secondo l'AGCM, Amazon avrebbe sostanzialmente favorito il proprio servizio di logistica FBA per i venditori attivi sulla piattaforma Amazon.it ai danni degli operatori concorrenti nel mercato e, in secondo luogo, ai venditori terzi che utilizzano FBA non sarebbe stato applicato lo stringente sistema di misurazione delle performance cui Amazon sottopone i venditori non-FBA e il cui mancato superamento può condurre anche alla sospensione dell'account del venditore. Così facendo, Amazon avrebbe danneggiato gli operatori concorrenti di logistica per e-commerce, impedendo loro di proporsi ai venditori online come fornitori di servizi di qualità paragonabile a quella della logistica di Amazon. Per una panoramica sul tema del *self-preferencing*, sia permesso di rinviare a N. FARAONE, *La pronuncia del Tribunale UE nel caso Google Search (Shopping) ovvero la storia della profezia che si auto-avvera: un'anticipazione del futuro mutamento dell'enforcement antitrust nei mercati digitali (anche alla luce del DMA)*, in *Dir. di internet*, n. 1, 2022, 77 ss.; P. MANZINI, *op. cit.*, 48 ss. Si veda, inoltre, B. VESTERDORF, *Theories of Self-Preferencing and Duty to Deal – Two Sides of the Same Coin?*, in *Competition Law & Policy Debate*, n. 1, 2015, 4 ss.; N. PETIT, *Theories of Self-Preferencing Under Article 102 TFEU: A Reply to Bo Vesterdorf*, in *Competition Law & Policy Debate*, n. 3, 2015, 2 ss.; B. EDELMAN, *Does Google Leverage Market Power through Tying and Bundling?*, in *Journal of Competition Law and Economics*, n. 2, 2015, 365 ss.; M. LAO, *Search, Essential Facilities, and the Antitrust Duty to Deal*, in *Northwestern Journal of Technology and Intellectual Property*, n. 5, 2013, 292 ss.; J. RATLIFF, D. RUBINFELD, *Is There a Market for Organic Search Engine Results and Can their Manipulation Give Rise to Antitrust Liability?*, in *Journal of Competition Law and Economics*, n. 3, 2014, 518 ss. Per un'analisi dettagliata e un raffronto della fattispecie del *self-preferencing* con le tradizionali categorie del diritto della concorrenza, si rimanda a P. IBÁÑEZ COLOMO, *Self-Preferencing: Yet Another Epithet in Need of Limiting Principles*, in *World Competition*, n. 4, 2020, 417 ss.; E. HOVENKAMP, *The Antitrust Duty to Deal in the Age of Big Tech*, in *Yale Law Journal*, n. 5, 2022, 1385 ss. Per una prima analisi dell'istruttoria FBA/Amazon, si rimanda a 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. reg. merc.*, n. 2/2022, 478 ss.; F. PETROCELLI, *Il caso FBA Amazon tra pratica legante e self-preferencing (vorrei ma non posso!)*, in *Merc. conc. reg.*, n. 2, 2022, 333.

<sup>51</sup> Il caso sopra riportato (e la correlativa sanzione comminata) dall'AGCM è sovrapponibile, dal punto di vista fattuale e delle condotte contestate in sede di avvio di istruttoria, ai casi avviati dalla Commissione europea Amazon Marketplace (si veda caso AT.40462, Amazon Marketplace, 17 luglio 2019) e Amazon Buy Box (si veda caso AT.40703, Amazon – Buy Box, 10 novembre 2020). Anche in questo caso, secondo la Commissione, i criteri adottati dall'algoritmo avrebbero premiato, a parità delle altre caratteristiche, prodotti di operatori che aderiscono al servizio di logistica Fulfillment by Amazon (FBA), gestito dalla piattaforma stessa. L'indagine Buy Box rappresenta, però, una diramazione del caso Amazon Marketplace, in cui il trattamento preferenziale assume una portata più ampia: i dati sui rivenditori al dettaglio raccolti da Amazon in veste di intermediario (a monte) possono essere utilizzati da quest'ultima per calibrare le offerte dei propri prodotti ai consumatori. Sul parallelismo tra i due procedimenti quel-

## 4. Il caso di scuola del *ne bis in idem*

Si è detto, nel precedente paragrafo, che la dialettica tra DMA e norme europee e nazionali a tutela della concorrenza pone interrogativi di non poco momento relativamente al potenziale materializzarsi di un duplica-

---

lo “domestico” in capo all’AGCM e quelli avviati dalla Commissione, è stato chiamato a pronunciarsi il Tribunale dell’Unione europea, che ha respinto il ricorso di Amazon sulla decisione della Commissione di avvio delle indagini, rispetto alla preesistente istruttoria dell’AGCM sui medesimi fatti (Tribunale dell’Unione europea (Prima Sezione), causa T-19/21, Amazon.com *et al.* c. Commissione, ordinanza del 14 ottobre 2021). In data 21 dicembre 2021, Amazon impugnava tale ordinanza dinanzi alla Corte di giustizia (Causa C-815/21 P), che, lo scorso 14 luglio 2022, ha adottato un’ordinanza che autorizza l’AGCM a intervenire nella causa a sostegno delle conclusioni della Commissione europea. Da ultimo, lo scorso 28 ottobre 2022 (R.G. 1364/2022), il T.A.R. Lazio – dinanzi al quale Amazon proponeva ricorso avverso la sanzione dell’AGCM pari a oltre €1 miliardo – ha sospeso il giudizio sino alla data di pubblicazione della decisione della Corte di giustizia (causa C-815/21 P). In data 14 luglio 2022, Amazon ha presentato impegni nelle istruttorie Buy Box e Marketplace, poi accettati dalla Commissione europea lo scorso 20 dicembre 2022, che sembrano replicare il contenuto del DMA, ponendo ancor più urgenti problemi di coordinamento con lo strumentario di diritto della concorrenza. Quindi, riassumendo, la Commissione europea ha avviato un’indagine ai sensi dell’art. 102 TFUE nei confronti di Amazon per fatti identici a quelli già affrontati in una parallela istruttoria italiana avviata dall’AGCM e conclusasi nel novembre 2021. Delimitando il mercato geografico allo Spazio Economico Europeo (“SEE”) ad eccezione dell’Italia (conseguenza procedurale, quest’ultima, derivante dal precedente avvio dell’istruttoria italiana), la Commissione ha di fatto evitato che l’AGCM deliberasse il “non luogo a procedere” e archiviasse l’istruttoria italiana. Un’ulteriore dimostrazione del cortocircuito che potrebbe materializzarsi a breve è stata fornita, di recente, dal Bundeskartellamt nell’ambito dell’istruttoria avviata il 25 maggio 2021 (Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google’s significance for competition across markets and its data processing terms) in cui si sosteneva che Google condizionasse l’utilizzo dei suoi servizi al consenso degli utenti al trattamento dei loro dati senza fornire loro una reale possibilità di scelta. Nella comunicazione degli addebiti resa lo scorso 11 gennaio 2023 (Statement of objections issued against Google’s data processing terms), il Bundeskartellamt premette che l’istruttoria si basa sulle norme poste a tutela della concorrenza di diritto tedesco (e, nello specifico, sulla Sezione 19(a) del GWB) e che il DMA potrebbe applicarsi senza dubbio a una molteplicità di servizi forniti da Google. D’altro canto, il DMA si applica solo a condizione che siano coinvolti i c.d. servizi di piattaforma di base, ancora oggetto di futura designazione da parte della Commissione europea. Muovendo da tale assunto, secondo il Bundeskartellamt, l’ambito applicativo della Sezione 19(a) del GWB sarebbe più ampio rispetto al DMA. Ciononostante, il Bundeskartellamt rimane in stretto contatto con la Commissione europea. Testualmente, il Bundeskartellamt così si pronuncia: *«In its proceeding, the Bundeskartellamt bases its assessment on German competition law. The European Digital Markets Act (DMA), which is exclusively enforced by the European Commission, is also likely to apply to certain Google services in the future. While the DMA also includes a provision which addresses the processing of data across services, this applies only if so-called core platform services, which still have to be designated by the European Commission, are involved. The present proceeding based on the national provision under Section 19a GWB partially exceeds the future requirements of the DMA. In this regard, the Bundeskartellamt is in close contact with the European Commission»*.

zione di sanzioni e/o di procedimenti e ha “inaugurato” una nuova stagione di conflittualità tra la Commissione europea (incaricata dell’applicazione centralizzata del DMA) e le autorità garanti della concorrenza a livello nazionale (che rimangono titolari della competenza a perseguire le condotte potenzialmente anti-competitive degli attori tecnologici ai sensi del diritto della concorrenza europeo e nazionale).

Faremo, ora, un passo indietro esaminando la giurisprudenza delle Corti europee stratificatasi nel corso degli anni relativamente al principio del *ne bis in idem* per poi farne due avanti contestualizzando il nuovo approccio inaugurato dalla Corte in *bpost*<sup>52</sup> e *Nordzucker*<sup>53</sup>.

È bene premettere, sin d’ora, che la linea evolutiva seguita dalla giurisprudenza della Corte di giustizia ha visto l’imporsi di un doppio binario nell’applicazione del principio in parola, con due interpretazioni antiteti- che a dividersi il campo, con specifico riguardo al requisito dell’*idem*, a seconda che si faccia parola di diritto penale o di diritto *antitrust*.

Nel primo caso, alla luce di quanto previsto dall’art. 54 della Convenzione di Schengen (“CAAS”)<sup>54</sup>, la Corte di giustizia ha chiarito che l’*idem* deve essere inteso quale *idem* fattuale<sup>55</sup>, ossia come riferimento all’identità dei fatti materiali oggetto di valutazione, individuati quali insieme di circostanze concrete inscindibilmente collegate tra loro<sup>56</sup>. Pertanto, ai fini dell’applicazione delle garanzie scaturenti dal principio del *ne bis in idem* in materia penale, la Corte di giustizia richiede che le medesime circostanze di fatto siano riferibili allo stesso soggetto<sup>57</sup>.

<sup>52</sup> CORTE DI GIUSTIZIA UE, Grande Sezione, sentenza 22 marzo 2022, causa C-117/20; Pres. Lenaerts, Rel. Jürimäe, Avv. Gen. Bobek; *bpost* SA c. Autorité belge de la concurrence.

<sup>53</sup> CORTE DI GIUSTIZIA UE, Grande Sezione, sentenza 22 marzo 2022, causa C-151/20; Pres. Lenaerts, Rel. Jürimäe, Avv. Gen. Bobek; Bundeswettbewerbsbehörde c. Nordzucker AG, Südzucker AG, Agrana Zucker GmbH.

<sup>54</sup> La Convenzione è nata nel perimetro del Terzo Pilastro (titolo VI del Trattato sull’Unione europea, relativo alla cooperazione di polizia e giudiziaria in materia penale), caratterizzato da un approccio intergovernativo, ed è stata successivamente “comunitarizzata” con il Protocollo (n. 2) al Trattato di Amsterdam sull’integrazione dell’acquis di Schengen nell’ambito dell’Unione europea.

<sup>55</sup> Nel corso degli anni, in forza dell’art. 50 della Carta di Nizza, tale approccio è stato esteso anche alle sanzioni amministrative di carattere punitivo e di natura “sostanzialmente penale”. Si veda, a tal proposito, Corte EDU, Grande Camera, sentenza 23 novembre 1976, Engel c. Paesi Bassi, ric. nn. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, §§82-83. I criteri Engel sono stati direttamente applicati dal Giudice di Lussemburgo per la prima volta in Corte giust. UE, Grande Sezione, sentenza 5 giugno 2012, causa C-489/10, Lukasz Marcin Bonda, §§37 ss.

<sup>56</sup> Corte giust. UE, sentenza 11 febbraio 2003, causa C-187/01, Gözütek e Brügge; Corte giust. UE, sez. II, sentenza 9 marzo 2006, causa C-436/04, Van Esbroek, §36.

<sup>57</sup> Per un quadro complessivo sulle evoluzioni giurisprudenziali nella definizione del contenu-

All'opposto, nel caso del diritto *antitrust* – che ha mantenuto nel tempo una sua autonomia nell'applicazione del principio in esame, legandola a parametri più stringenti rispetto a quelli elaborati nelle altre aree<sup>58</sup> –, la Corte di giustizia ha, invece, riconosciuto che il requisito dell'*idem* è da ritenersi integrato soltanto nell'ipotesi in cui sia dimostrata la contestuale ricorrenza di tre elementi: l'identità dei fatti, l'unità del contravventore e l'unità dell'interesse giuridico tutelato.

Originariamente elaborato nel caso *Wilhelm et al.*<sup>59</sup>, tale approccio, quello della valorizzazione del requisito dell'interesse giuridico tutelato, è stato successivamente corroborato e “raffinato” nel caso *Aalborg Portland*<sup>60</sup> all'inizio del 2004 e, da ultimo, confermato dalla Corte di giustizia, riunitasi in Grande Sezione, nel caso *Toshiba*<sup>61</sup> (per quanto, in quell'occa-

---

to precettivo del principio del *ne bis in idem*, soprattutto in ambito penale, si veda M. SCOLETTA, *Il principio europeo di ne bis in idem e i modelli punitivi “a doppio binario”*, in C. AMALFITANO, M. D'AMICO, S. LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione Europea nel sistema integrato di tutela*, Giappichelli, Torino, 2022, e già in *Dir. pen. cont. – Riv. trim.*, n. 4, 2021, 180; N. RECCHIA, *L'ennesima stagione del ne bis in idem nel costituzionalismo multilivello: la riaffermazione del suo ubi consistam processuale contro ogni riduzionismo sostanziale*, in *Riv. it. dir. proc. pen.*, 2022, n. 4, in corso di pubblicazione; N. MADIA, *Ne bis in idem europeo e giustizia penale*, Cedam, Milano, *passim*; ID, *Il ne bis in idem europeo nella sua “nuova” veste sostanziale: la sua possibile efficacia anche nell'ambito di un unico procedimento in materia di cumuli punitivi*, in *Arch. pen.*, n. 3, 2019, 1-38; ID., *Ne bis in idem europeo: la definitiva emersione della sua efficacia anche sostanziale in materia di pluralità di sanzioni e proporzionalità della pena*, in *Cass. pen.*, n. 2, 2019, 642-685; L. BIN, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, in *Dir. pen. cont. – Riv. trim.*, n. 3, 2020, 98-141.

<sup>58</sup> Secondo il Tribunale, sentenza 26 ottobre 2017, causa T-704/14, *Marine Harvest c. Commissione*, punto 12, «[...] il principio del *ne bis in idem* si applica nei procedimenti diretti all'irrogazione di ammende in materia di diritto della concorrenza, indipendentemente dalla qualificazione di tali ammende come ammende di natura penale o non penale. Inoltre, in materia di diritto della concorrenza, in cui le ammende sono inflitte dalla Commissione, l'esistenza di una “sentenza” che infligge un'ammenda non è necessaria. [...] è sufficiente che esista una “decisione” precedente non più impugnabile. Pertanto, la sola esistenza di una decisione della Commissione che infligge un'ammenda, che non sia stata contestata nei termini e che, quindi, non sia più impugnabile, è sufficiente per far sì che il principio del *ne bis in idem* possa essere applicato. Tuttavia, il termine “definitiva” che emerge dall'articolo 50 della Carta dei diritti fondamentali ha rilievo anche nel diritto della concorrenza, come risulta dall'espressione “precedente decisione non più impugnabile”».

<sup>59</sup> Corte giust. UE, sentenza 13 febbraio 1969, causa 14/68, *Walt Wilhelm e altri contro Bundeskartellamt*.

<sup>60</sup> Corte giust. UE, sentenza 7 gennaio 2004, cause riunite C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P e C-219/00 P, *Aalborg Portland e altri c. Commissione*. Ma si veda anche Corte giust. UE, sentenza 29 giugno 2006, C-289/04 P, *Showa Denko c. Commissione*; Corte giust. UE, sentenza 29 giugno 2006, C-308/04, *SGL Carbon c. Commissione*.

<sup>61</sup> Corte giust. UE, Grande Sezione, sentenza 14 febbraio 2012, causa C-17/10, *Toshiba Corporation e altri c. Úřad pro ochranu hospodářské soutěže*.

sione, l'Avvocato Generale Kokott si fosse pronunciato a favore dell'abbandono di tale principio) e, più recentemente, nel 2021, nel caso Slovak Telekom<sup>62</sup>.

L'aggiunta dell'elemento dell'identità dell'interesse giuridico tutelato ha suscitato più di una perplessità, dal momento che, a seconda che si versi in materia penale o *antitrust*, ha determinato un restringimento dell'ambito di applicazione del *ne bis in idem*<sup>63</sup>, confinandolo, da strumento eminentemente garantista, a procedura avente un movente sanzionatorio o punitivo<sup>64</sup>.

Parallelamente, anche la Corte EDU è intervenuta in merito alla possibilità di irrogare, rispetto al medesimo fatto, due sanzioni qualificabili, ri-

---

<sup>62</sup> Corte giust. UE, sentenza 25 febbraio 2021, causa C-857/19, Slovak Telekom a.s./Proti monopolný úrad Slovenskej republiky.

<sup>63</sup> A questo punto, non è senza interesse cercare di indagare le ragioni profonde che stanno alla base del descritto statuto speciale riservato alla garanzia del *ne bis in idem* nell'applicazione delle norme *antitrust*. La tenuta della giurisprudenza in Aalborg Portland può spiegarsi con il più generale timore che il pieno riconoscimento della doppia incriminazione possa rappresentare una minaccia al principio di effettività delle norme a tutela della concorrenza. In primo luogo, l'ambito di applicazione della condizione di identità dell'autore del reato potrebbe essere artificialmente ampliata dalla teoria dell'"unità economica", secondo la quale la circostanza che una società controllata abbia una personalità giuridica distinta rispetto alla *holding* non è sufficiente per escludere la possibilità di attribuire automaticamente la sua condotta alla *parent company*. Inoltre, nel diritto *antitrust*, la condizione relativa al *bis* deve essere armonizzata con l'ampia nozione di "infrazione unica e continuata", che consente alle autorità e ai tribunali di prendere in esame una serie di condotte (anche eterogenee tra loro) messe in atto da parte di diverse imprese che rispondano, però, a un complessivo piano distortivo della concorrenza. Più nello specifico, nel nuovo "ordine", le perplessità sopra descritte sarebbero state significativamente attenuate se l'Unione europea avesse applicato alle questioni attinenti al diritto della concorrenza i test "inaugurati" e sviluppati dalla Corte EDU in A & B c. Norvegia (che ha "consacrato" il criterio del «*sufficient connection in space and time*») e dalla Corte di giustizia in Menci, Garlsson Real Estate e Di Puma-Zecca (vale a dire, gli "ulteriori obiettivi di interesse generale" che giustificerebbero "una duplicazione dei procedimenti e delle sanzioni", a condizione che il coordinamento di tali procedimenti sia garantito e che "il rigore e la severità di tutte le sanzioni inflitte" siano proporzionate). In alternativa, il medesimo risultato si sarebbe potuto ottenere tramite una modifica legislativa apposita, eventualmente preceduto da un intervento chiarificatore da parte della Corte di giustizia circa l'ambito di applicazione della giurisprudenza Menci e la sua applicabilità, *mutatis mutandis*, anche in ambito *antitrust*. Per una panoramica di ordine generale, cfr. B. NASCIMBENE, *Il divieto di bis in idem nell'elaborazione della Corte di Giustizia dell'Unione europea*, in *Sistema penale*, n. 4, 2020, 95-108; ID., *Ne bis in idem, diritto internazionale e diritto europeo*, in *Dir. pen. cont.*, 2 maggio 2018. G. DI FEDERICO, *EU Competition Law and the Principle of Ne Bis in Idem*, in *European Public Law*, 2011, 241 ss.; R. NAZZINI, *Fundamental rights beyond legal positivism: rethinking the ne bis in idem principle in EU competition law*, in *Journal of Antitrust Enforcement*, 2014, 270 ss.

<sup>64</sup> Del resto, il passaggio e la transizione da una concezione di *idem* legale ad una nozione material di *idem factum*, fondata sulla concomitante incidenza di un doppio binario punitivo in capo ad un unico fatto storico si erano già compiuti a partire dalla nota sentenza Zolotukhin c. Russia (cfr. Corte EDU, Grande Camera, Zolotukhin c. Russia, 10 febbraio 2009).

spettivamente, come amministrativa (ovvero fiscale), da un lato, e penale, dall'altro, pronunciandosi, quindi, in tema di applicabilità del principio del *ne bis in idem*, previsto dall'art. 4, Protocollo n. 7 CEDU<sup>65</sup>.

La sentenza A. e B. c. Norvegia resa in data 15 novembre 2016 dalla *Grande Chambre* della Corte EDU – che, pur non riguardando direttamente l'Italia, è risultata utile a definire le questioni aperte dalla celeberrima pronuncia Grande Stevens c. Italia<sup>66</sup> – esamina, infatti, l'ipotesi in cui il medesimo episodio di evasione fiscale divenga oggetto di sanzione amministrativa e sia, successivamente, sottoposto a processo penale, arrivando ad escludere, così, che l'imposizione di una duplice sanzione (amministrativa e penale) integri un *bis in idem*<sup>67</sup>. La pronuncia, confermando i criteri già espressi nella sentenza Grande Stevens con riferimento alla valutazione della sussistenza dell'*idem factum* e della natura sostanzialmente penale di sanzioni formalmente amministrative, chiarisce che il principio del *ne bis in idem* non osta, di per sé, a che agli Stati Contraenti prefigurino un "doppio binario sanzionatorio" (amministrativo e penale) con riferimento agli illeciti fiscali<sup>68</sup>. Cosicché, al fine di evitare di incorrere in duplicazioni

---

<sup>65</sup> Anche nell'ordinamento italiano si è posta la questione della compatibilità con la CEDU del doppio binario sanzionatorio in materia tributaria (per le sanzioni penali si vedano artt. 10 ss. del d.lgs. n. 74/2000; per quelle tributarie artt. 13 ss., d.lgs. n. 471/1997). Sul punto si veda, per tutti, F. VIGANÒ, *Omesso versamento di IVA e diretta applicazione delle norme europee in materia di ne bis in idem?*, in *Dir. pen. cont. – Riv. trim.*, 11 luglio 2016. La giurisprudenza italiana, inoltre, ha dubitato della compatibilità del doppio binario in materia tributaria con l'art. 50 CEDU, a partire dalla nota sentenza Åkerberg Fransson della Corte di giustizia (sentenza del 26 febbraio 2013, causa C-617/10, Åklagaren c. Hans Åkerberg Fransson [GC]). Sul punto, cfr. F. VIGANÒ, *Ne bis in idem e omesso versamento dell'IVA: la parola alla Corte di giustizia*, in *Dir. pen. cont. – Riv. trim.*, 28 settembre 2015.

<sup>66</sup> Corte EDU, sentenza 4 marzo 2014, Grande Stevens c. Italia, ricorso n. 18640/10. Si rimanda, per un'analisi della pronuncia, a A. TRIPODI, *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*, in *Dir. pen. cont. – Riv. trim.*, n. 1, 2014, 1-3; B. NASCIBENE, *La sentenza Grande Stevens. Problemi e prospettive*, in *Eurojus.it*, luglio-settembre 2014.

<sup>67</sup> Corte EDU, Grande Camera, sentenza 15 novembre 2016, *A e B c. Norvegia*, ricorsi nn. 24130/11 e 29758/11. La pronuncia ha evidenziato la vicenda di due soggetti accusati in sede penale di frode fiscale per non aver dichiarato i profitti derivanti da alcune transazioni finanziarie operate all'estero. Nei confronti di tali soggetti era stata già irrogata in via definitiva dall'amministrazione tributaria una sanzione formalmente di natura amministrativa consistente in una sovrattassa pari al 30% dell'imposta evasa e i soggetti erano ricorsi alla Corte europea affinché, ravvisata la natura sostanzialmente penale della sanzione amministrativa irrogata, si accertasse l'avvenuta violazione del *ne bis in idem* derivante dai procedimenti penale avviati nei loro confronti per lo stesso fatto.

<sup>68</sup> Secondo il par. 123 della pronuncia, «[...] the object of Article 4 of Protocol No. 7 is to prevent the injustice of a person's being prosecuted or punished twice for the same criminalised

sanzionatorie potenzialmente illegittime, occorre verificare se i due procedimenti – quello amministrativo e quello penale – siano sufficientemente connessi nella sostanza e nel tempo (come recita il par. 131 della pronuncia, «*sufficiently connected in substance and in time*»). A tal proposito, la Corte EDU fornisce un elenco esemplificativo di criteri, tra i quali quello degli scopi in concreto perseguiti dai due procedimenti, della prevedibilità dello sdoppiamento delle procedure, della presenza di meccanismi di coordinamento procedurale e sostanziale tra le autorità intervenienti<sup>69</sup> e, da ultimo, dell'esistenza di meccanismi atti a graduare la complessiva risposta sanzionatoria. In altri termini, si apre la strada a una valutazione “di chiusura” fondata sul principio di proporzionalità del cumulo sanzionatorio (e non già della pluralità di procedimenti)<sup>70</sup>.

Nonostante le critiche mosse alla decisione<sup>71</sup>, la Corte di giustizia ha sostanzialmente ripreso (*melius*, sostanzialmente annacquato) il test della

---

*conduct. It does not, however, outlaw legal systems which take an “integrated” approach to the social wrongdoing in question, and in particular an approach involving parallel stages of legal response to the wrongdoing by different authorities and for different purposes».*

<sup>69</sup> Con riguardo alla sussistenza di idonei meccanismi di coordinamento procedurale e sostanziale tra le autorità intervenienti, la Corte EDU, al par. 132, sottolinea la necessità che, sul piano procedurale, si eviti una duplicazione nella raccolta e nella valutazione delle prove, e che, sul piano sostanziale, la sanzione imposta dal primo giudice sia presa in debita considerazione dal secondo giudice «*so as to prevent that the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall amount of any penalties imposed is proportionate*».

<sup>70</sup> Per un'analisi della torsione in chiave di proporzionalità del principio del *ne bis in idem*, si veda C. SILVA, *La deriva del ne bis in idem verso il canone di proporzionalità*, in *Arch. pen.*, n. 1, 2019, 1-38; F. VIGANÒ, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Giappichelli, Torino, 2021, *passim*. Valorizzano, inoltre, il tema della proporzionalità, tra gli altri, E. BASILE, *Il “doppio binario” sanzionatorio degli abusi di mercato in Italia e la trasfigurazione del ne bis in idem europeo*, in *Giur. comm.*, 2019, 129-141; F. CONSULICH, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, in *Dir. pen. e proc.*, 2018, 949; F. MAZZACUVA, *Il ne bis in idem dimezzato: tra valorizzazione delle istanze di proporzione della sanzione e smarrimento della dimensione processuale*, in *Giur. comm.*, n. 4, 2020, 940.

<sup>71</sup> La Corte EDU ha ulteriormente sviluppato il test scaturente dalla pronuncia A e B c. Norvegia nella sua giurisprudenza successiva, nonostante tale standard sia stato salutato da voci contrastanti che vedevano, nello sforzo argomentativo della Corte, un *overruling* “mascherato” rispetto alle istanze che avevano ispirato la sentenza Grande Stevens, come rilevato dal giudice Pinto de Albuquerque nella sua *dissenting opinion*. Secondo l'opinione dissenziente del giudice Pinto de Albuquerque, ai §§79-80, «*[a]fter turning the rationale of the ne bis in idem principle upside down, the present judgment opens the door to an unprecedented, Leviathan-like punitive policy based on multiple State-pursued proceedings, strategically connected and put in place in order to achieve the maximum possible repressive effect. This policy may turn into a never-ending, vindictive story of two or more sets of proceedings progressively or successively conducted against the same defendant for the same facts, with the prospect of the defendant even being castigated, in*

sentenza A e B c. Norvegia, operando su un quadro concettuale diverso e, quindi, valorizzando unicamente il profilo della proporzionalità del trattamento sanzionatorio cumulativo<sup>72</sup>.

Muovendo dalla pronuncia nel caso Hans Åkerberg<sup>73</sup>, nelle sentenze Menci<sup>74</sup>, Garlsson Real Estate<sup>75</sup>, e Di Puma-Zecca<sup>76</sup>, perché la duplicazione di procedimenti penali e amministrativi per la medesima condotta soddisfi i criteri previsti dall'art. 52, par. 1, Carta di Nizza, è necessario che: (i) la possibilità di un doppio binario sanzionatorio penale-amministrativo sia chiaramente prevista dalla legge; (ii) i procedimenti e le sanzioni abbiano di mira scopi complementari nel comune perseguimento di un interesse generale di importanza tale da legittimare la scelta del doppio binario san-

---

*a retaliatory fashion, for exercising his or her legitimate procedural rights, and especially his or her appeal rights. The combination of criminal penalties and administrative penalties with a criminal nature was specifically rejected by the Court in Grande Stevens and Others, as well as by the Luxembourg Court in Hans Åkerberg Fransson. After the delivery of its death certificate in that Italian case, such an approach is now being resuscitated as a "calibrated" regulatory approach».*

<sup>72</sup> Così realizzando ciò che lo stesso giudice Pinto de Albuquerque ha definito come un esempio di «negative cross-fertilisation between courts»: si rimanda a P. PINTO DE ALBUQUERQUE, L. HYUN-SOO, *The Cross-fertilisation between the Court of Justice of the European Union and the European Court of Human Rights: Reframing the Discussion on Brexit*, in *European Human Rights Law Review* 6, 2018, 571. Infatti, mentre ai sensi dell'art. 15, par. 2, CEDU, la Convenzione non ammette deroga al principio del *ne bis in idem*, al contrario, secondo l'art. 52, par. 1, Carta di Nizza, la garanzia sancita dall'art. 50 della stessa Carta può essere soggetta a limitazioni allorché queste ultime siano previste dalla legge, rispettino l'essenza di tali diritti e siano conformi al principio di proporzionalità. Tale garanzia esprimerebbe però, da un punto di vista dogmatico, non una regola ma un principio, come tale da bilanciare ai sensi dell'art. 52 della Carta. I criteri, che nella giurisprudenza della Corte EDU servivano ad escludere il materializzarsi della regola del *ne bis in idem*, sono, dunque, recuperati dalla Corte di giustizia come elementi che consentono di giustificare l'applicazione di tale principio. La Corte di giustizia si è finora pronunciata su due tipi di limitazioni ai sensi dell'art. 52 della Carta di Nizza. Lasciando, per un momento, sullo sfondo il primo gruppo di eccezioni (relativo alla condizione dell'esecuzione della pena di cui all'art. 54 CAAS alla luce della giurisprudenza Spasic: Corte giust. UE, Grande Sezione, sentenza 27 maggio 2014, causa C-129/14 PPU, Zoran Spasic), il secondo, invece, ha riguardo alla potenziale duplicazione di procedimenti penali e amministrativi.

<sup>73</sup> Corte giust. UE, sentenza 28 febbraio 2013, causa C-617/10, Aklagaren v. Hans Åkerberg Fransson, §34.

<sup>74</sup> Corte giust. UE, sentenza 12 settembre 2017, causa C-524/15, Luca Menci c. Procura della Repubblica, §§41-64. Si veda anche P. DE PASQUALE, *Note a margine delle conclusioni nel caso Menci: la storia del divieto di ne bis in idem non è ancora finita*, in *dirittounioneuropea.eu*, 31 ottobre 2017.

<sup>75</sup> Corte giust. UE, sentenza 20 marzo 2018, causa C-537/16, Garlsson Real Estate SA e altri c. Commissione Nazionale per la Società e la Borsa (CONSOB), §§ 42-62.

<sup>76</sup> Corte giust. UE, sentenze 20 marzo 2018, cause riunite C-596/16 e C-597/16, Enzo Di Puma c. Commissione Nazionale per la Società e la Borsa (CONSOB) e Commissione Nazionale per la Società e la Borsa (CONSOB) c. Antonio Zecca, §§ 38-40.

zionatorio; e (iii) l'ordinamento garantisca un coordinamento tra i procedimenti che limiti "a quanto strettamente necessario" gli oneri per il consociato sottoposto ad un doppio procedimento. Infine, è necessario che l'ordinamento garantisca che la severità del complesso delle sanzioni imposte sia proporzionata rispetto alla gravità dei fatti commessi<sup>77</sup>.

Ricapitolando, a valle della giurisprudenza Menci, Garlsson Real Estate e Di Puma-Zecca, che si è sviluppata sul sentiero già tracciato dalla Corte EDU nella causa A e B c. Norvegia, la Corte di giustizia ha aperto la strada a un rinnovato approccio al tema, inaugurando la possibilità che il cumulo di procedimenti e di sanzioni sia giustificato in caso di perseguimento di un obiettivo di interesse generale, di complementarità degli scopi e di limitazione dell'onere supplementare, in termini sanzionatori e di severità del complesso delle sanzioni comminate, a quanto strettamente necessario<sup>78</sup>. Di conseguenza, il "perimetro di gioco" entro cui il principio del *ne*

---

<sup>77</sup> Come riconosciuto dalla Corte di giustizia in *bpost* (§ 52), un'analisi globale della condizione di proporzionalità e di stretta necessità può essere effettuata in maniera completa solo *ex post*, tenuto conto della natura di alcune circostanze particolari del caso. E, in quest'ultimo passaggio, si annida un'ulteriore nodo problematico della giurisprudenza Menci, come sostenuto in *bpost* nel contesto delle conclusioni dell'avvocato generale Bobek, secondo cui «l'applicazione del principio del *ne bis in idem* cessa di basarsi su un criterio *ex ante* normativamente definito. Esso, diventa, invece, un criterio correttivo *ex post*, che può trovare o meno applicazione a seconda delle circostanze e dell'importo esatto delle sanzioni inflitte. Non si tratta di una tutela contro la duplice incriminazione. Si tratta, semplicemente, di una tutela *ex post* contro il carattere sproporzionato delle sanzioni combinate o cumulate». Secondo la giurisprudenza in Menci – continua l'avvocato generale Bobek – «è soltanto al termine del secondo procedimento che sarà possibile verificare se talune condizioni [...] siano state o meno soddisfatte e, quindi, se il secondo procedimento sia o meno legittimo». In altri termini, Menci (e *bpost*) circoscrive l'ambito di operatività del principio del *ne bis in idem* al fine di tutelare il contenuto essenziale del diritto sancito all'art. 50 della Carta e per impedire la prosecuzione del secondo procedimento (ricordiamo che il principio del *ne bis in idem* impedirebbe non solo il cumulo delle sanzioni, ma anche dei procedimenti), a meno che, ovviamente, non risulti provato che i due procedimenti perseguano il medesimo obiettivo, o che non vi sia coordinamento tra i due procedimenti. In caso contrario, il giudice investito di un potenziale ricorso potrebbe essere restio a sospendere il secondo procedimento, con la conseguenza che l'impresa dovrà attendere la conclusione del secondo procedimento per poi impugnare la seconda sanzione invocando il principio del *ne bis in idem*.

<sup>78</sup> Tali pronunce segnano la definitiva metamorfosi (se non la "deriva": cfr. C. SILVA, *op. cit.*, 1-38) del principio del *ne bis in idem*, destinato a scivolare lungo il piano inclinato dello scrutinio di proporzionalità. Infatti, secondo N. RECCHIA, *Note minime sulle tre recenti sentenze della Corte di giustizia dell'Unione europea in tema di ne bis in idem*, in *www.eurojus.it*, 22 marzo 2018, a seguito del "trittico" di sentenze in esame sfuma definitivamente la possibilità di contestare un doppio binario sanzionatorio alla luce del *ne bis in idem*, che di fatto si riduce a garanzia espressa unicamente sulla carta. Gli scenari sin qui descritti sembrano trovare confermare in due recenti pronunce, Corte giust. UE, sentenza 5 maggio 2022, causa C-570/20, BV e Corte giust. UE, Grande Sezione, sentenza 8 marzo 2022, causa C-205/20, NE. Per un primo commento, si rimanda a F. VIGANÒ, *La proporzionalità della pena tra diritto costituzionale italiano e*

*bis in idem* ha operato è stato variamente declinato, imponendosi, per le questioni afferenti alla tutela della concorrenza, l'analisi dell'interesse giuridico tutelato e, per tutte le restanti fattispecie, l'esistenza del doppio criterio dell'identità della persona e dei fatti materiali, intesi come esistenza di un insieme di circostanze concrete, inscindibilmente collegate tra loro, e la proporzionalità della sanzione.

La giurisprudenza della Corte EDU e della Corte di giustizia “scolpisce”, dunque, un quadro diversificato dei parametri che sostengono l'agibilità del principio del *ne bis in idem*. In questo variegato mosaico di regimi paralleli si collocano sullo sfondo le già citate pronunce in *bpost* e *Nordzucker*, che è opportuno esaminare qui di seguito<sup>79</sup>.

Il primo caso vede protagonista la società *bpost*, storico fornitore di servizi postali in Belgio, sanzionata in successione da due autorità belghe; dapprima, dall'autorità nazionale di regolamentazione settoriale dei servizi postali e successivamente dall'autorità nazionale garante della concorrenza, per abuso di posizione dominante. La *bpost* ha contestato la legittimità di questo secondo procedimento, invocando il principio del *ne bis in idem*<sup>80</sup>. La Cour d'appel di Bruxelles – dinnanzi alla quale la controversia risultava nuovamente incardinata a valle del secondo annullamento “cassato” dalla Cour de Cassation – ha sollevato un rinvio pregiudiziale, chiedendo se la

---

diritto dell'Unione europea: sull'effetto diretto dell'art. 49, paragrafo 3, della Carta alla luce di una recentissima sentenza della Corte di giustizia, in [www.sistemapenale.it](http://www.sistemapenale.it), 26 aprile 2022, 1-19.

<sup>79</sup> Per un commento preliminare, si veda P. DE PASQUALE, *Uno, nessuno e centomila. I criteri di operatività del principio ne bis in idem*, in *Eurojus*, 2022, n. 2, 248 ss.; ID., *Finale di partita per il principio del ne bis in idem? Breve nota alle sentenze bpost e Nordzucker e a.*, in *BlogDUE*, 22 aprile 2022; M. CAPPAL, G. COLANGELO, *La Grande Sezione della Corte di Giustizia elabora (finalmente) un test unico per il ne bis in idem*, in *giustiziainsieme.it*, 13 aprile 2022; ID., *Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets*, in *Common Market Law Review*, n. 2, 2023, 305 ss.; M. SOUSA FERRO, *Analysis: “Bpost and Nordzucker: More Ashes on the Fire of Ne Bis in Idem in EU Antitrust Law”*, in *eu-lawlive.com*, 31 March 2022; P. HARRISON, M. ZDZIEBORSKA, B. WISE, *Navigating ne bis in idem: bpost, Nordzucker and the Digital Markets Act*, in *Competition Law Journal*, n. 2, 2022, 55 ss.; M. MAYR, *Redefining the Ne Bis in Idem Principle in EU Competition Law: bpost and Nordzucker*, in *Journal of European Competition Law & Practice*, n. 8, 2022, 553 ss.; P. VAN CLEYNENBREUGEL, *BPost and Nordzucker: Searching for the Essence of Ne Bis in Idem in European Union Law*, in *European Constitutional Law Review*, n. 2, 2022, 357 ss.; F. RIZZUTO, *Bpost and Nordzucker AG: The End of Competition Law Enforcement Exceptionalism Concerning the Principle of Ne bis In Idem*, in *European Competition and Regulatory Law Review*, n. 2, 2022, 154 ss.

<sup>80</sup> Come ricorda P. DE PASQUALE, *Finale di partita per il principio del ne bis in idem? Breve nota alle sentenze bpost e Nordzucker e a.*, cit., 7 ss., in Italia, una fattispecie, come quella sorta nel caso *bpost*, sarebbe risolta alla luce dell'art. 27, comma 1 *bis*, Codice del Consumo, ai sensi del quale la competenza a perseguire una pratica commerciale scorretta, spetta in via esclusiva, all'AGCM, che deve semplicemente acquisire il parere dell'autorità di regolazione competente.

legittimità del procedimento dinanzi all'autorità nazionale di concorrenza debba essere valutata guardando alla definizione di *idem* sviluppata nella giurisprudenza in materia di concorrenza o se occorre esaminarla alla luce della clausola concernente le limitazioni dei diritti e del criterio stabilito nella giurisprudenza Menci. In altri termini, se considerare rilevante o meno l'interesse giuridico tutelato, come richiesto anche dalla Commissione, intervenuta, peraltro, in qualità di *amicus curiae*.

Nella seconda pronuncia, Nordzucker e a., due società tedesche, produttrici di zucchero e detentrici di una posizione dominante sul relativo mercato, si sono viste contestare, in rapida successione dall'autorità tedesca garante della concorrenza, prima, e da quella austriaca, in un secondo momento, la violazione dell'art. 101 TFUE, apparentemente sulla base degli stessi fatti. La controversia giungeva dinnanzi alla Corte Suprema austriaca, investita in appello dall'autorità garante della concorrenza del procedimento diretto a far dichiarare che la Nordzucker avesse violato il diritto dell'Unione in materia di interesse, nonché il diritto della concorrenza austriaco e ad ottenere l'irrogazione di un'ammenda per la medesima infrazione alla Südzucker, l'altro produttore tedesco di zucchero. Al pari della Corte belga, la Corte Suprema dell'Austria si è avvalsa dell'art. 267 TFUE per rinviare la questione alla Corte di giustizia, ponendo i medesimi quesiti. In particolare, essa ha interrogato la Corte di giustizia in merito al valore da attribuire al criterio dell'interesse giuridico tutelato e se il principio del *ne bis in idem* precluda procedimenti paralleli o successivi in materia di concorrenza in altri Stati membri per quella che sembra essere, almeno in parte, la medesima condotta.

Con due sentenze (quasi) gemelle, la Corte di giustizia ha esteso i criteri Menci alle fattispecie relative alla politica di concorrenza, rendendo univoci i parametri per l'operatività del principio del *ne bis in idem*. Infatti, essa ha sgombrato il campo da ogni ulteriore dubbio, ricordando che, per garantire un'uniforme applicazione dell'art. 50 della Carta, nella constatazione dell'*idem*, la sua giurisprudenza nega rilevanza alla qualificazione giuridica in diritto nazionale dei fatti e all'interesse giuridico tutelato, precisando come ciò valga anche nel settore del diritto della concorrenza dell'Unione<sup>81</sup>. L'aspetto di maggior rilievo sistematico delle due pronunce si esaurisce nell'aver esteso la deroga al *ne bis in idem* all'ipotesi di due procedimenti sanzionatori formalmente amministrativi, ma sostanzialmente penali. Ne discende che il divieto di *bis in idem* opera tra sanzioni penali, tra sanzioni formalmente penali e formalmente amministrative, ma sostanzialmente penali.

---

<sup>81</sup> Sentenza bpost, §§34-35; sentenza Nordzucker, §40.

zialmente penali, e, da ultimo, come nel caso delle due pronunce “gemelle” in *bpost* e *Nordzucker*, anche tra sanzioni formalmente amministrative, come quelle delle autorità indipendenti, ma sostanzialmente penali.

Occorre segnalare, però, che la Corte di giustizia riporta sì ad unità la valutazione circa la deroga al divieto di *bis in idem*, prevedendo che debba rispettare talune condizioni, tra cui quella per cui il secondo procedimento debba perseguire un obiettivo “di interesse generale”, ma senza ricomprendere in tale nozione quella tradizionale di “interesse giuridico tutelato”, come, invece, suggeriva l’avvocato generale Bobek nelle sue conclusioni<sup>82</sup>.

Cionondimeno, la questione appare ben lungi dall’esser risolta, soprattutto in relazione al ruolo che (ancora) giocherebbe il requisito dell’interesse giuridico tutelato. Al punto da chiedersi se la complementarietà tra i diversi scopi di interesse generale perseguiti, che giustificerebbe la deroga al divieto di *bis in idem*, celi, nella sostanza, “sotto mentite spoglie” una diversa modalità di atteggiarsi del criterio dell’interesse giuridico tutelato<sup>83</sup>.

---

<sup>82</sup> Corte giust. UE, Conclusioni dell’avvocato generale Michal Bobek presentato il 2 settembre 2021, causa C-117/20, *bpost SA c. Autorité belge de la concurrence*, §132, in cui si suggerisce «*di rendere l’esame dell’interesse giuridico tutelato e, quindi, dell’obiettivo perseguito, parte dell’analisi dell’idem. È questo elemento che, da solo, consente di decidere, su un piano normativo, in modo chiaro ed ex ante, le ragioni per le quali una determinata condotta è perseguita in procedimenti paralleli o successivi, consentendo di stabilire se lo stesso presunto autore sia punito due volte per gli stessi motivi. Salvo che un esame più approfondito dimostri l’identità degli interessi giuridici tutelati dai due regimi normativi in questione, dovrebbe essere permesso perseguire parallelamente tali interessi anziché dover accettare che uno di essi sia, de facto, cancellato in conseguenza all’applicazione dei criteri Engel e all’ampia nozione dell’idem*». D’altronde, lo stesso l’avvocato generale, al §6, ha descritto il quadro dei versi regimi come «*un mosaico di regimi paralleli frammentato e parzialmente contraddittorio*». Sul punto, si veda, inoltre, P. DE PASQUALE, *Uno, nessuno e centomila. I criteri di operatività del principio ne bis in idem*, cit., 256; M. CAPPALÀ, G. COLANGELO, *op. cit.* Peraltro, anche l’Avvocato generale Sánchez-Bordona, nelle sue Conclusioni rese in data 12 settembre 2017 sul caso *Menci* (Causa C-524/15), al par. 103, aveva suggerito di allineare la giurisprudenza sviluppata nell’ambito *antitrust* con lo standard generale adottato per tutte le altre aree del diritto. Neanche la direttiva ECN+ (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, recepita in Italia con d.lgs. n. 185/2021) ha affrontato propriamente la questione del *ne bis in idem*. Ciò appare ancor più sorprendente, dato che, anni addietro, la Commissione europea aveva sostenuto come l’intervento legislativo fosse l’unico mezzo per risolvere efficacemente la tematica della doppia incriminazione. Si veda EUROPEAN COMMISSION, *Green Paper on Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings*, COM(2005) 696 final.

<sup>83</sup> Come sostenuto dall’avvocato generale Bobek nelle sue Conclusioni, «*[è] interessante notare che, anche nei casi in cui è stato accolto l’approccio dell’idem factum, il criterio dell’interesse giuridico tutelato non è mai realmente scomparso. Al pari di un piccolo camaleonte, esso ha semplicemente assunto colori diversi, attaccandosi ai vari bastoni o rami disponibili all’interno di ciascun filone giurisprudenziale in quel momento esistenti*».

La risposta cambia a seconda delle diverse circostanze fattuali riscontrabili nelle due pronunce. A rigore, se, nel caso *bpost*, i due procedimenti, che hanno ad oggetto distinti interessi generali (la normativa settoriale ha per oggetto la liberalizzazione dei servizi postali, mentre la disciplina *antitrust* persegue, come noto, l'obiettivo di tutelare le dinamiche competitive nel mercato), impongono al giudice di valutare unicamente la proporzionalità del cumulo sanzionatorio in rapporto alla gravità delle infrazioni commesse, nel caso *Nordzucker* la questione appare più delicata, al punto da riportare "alla ribalta" la domanda circa la scomparsa o meno dell'interesse giuridico da tutelare. In *Nordzucker*, considerando che le due autorità garanti hanno, come missione istituzionale, la cura del medesimo interesse generale (vale a dire, garantire il dispiegarsi del più ampio livello di concorrenza nel mercato), il cumulo di procedimenti e sanzioni può essere giustificato soltanto qualora riguardino «*scopi complementari vertenti, eventualmente, su aspetti differenti della medesima condotta di reato interessata*»<sup>84</sup>.

---

<sup>84</sup> Sentenza *Nordzucker*, § 52, che riprende la giurisprudenza Menci, §44. Al punto che, al contrario, «*un cumulo dei procedimenti e delle sanzioni, quando non perseguono scopi complementari vertenti su aspetti differenti del medesimo comportamento ai sensi della giurisprudenza ricordata al punto 52 della presente sentenza, non può, in ogni caso, essere giustificato ai sensi dell'articolo 52, paragrafo 1, della Carta*» (§ 57). Con riguardo a tale aspetto, la Corte di giustizia, in *Nordzucker*, muove dalla constatazione che l'art. 101 TFUE è una disposizione di ordine pubblico che mira a garantire che la concorrenza non sia falsata nel mercato interno. Tenuto conto dell'importanza, riconosciuta anche nella giurisprudenza della Corte di giustizia, di tale obiettivo di interesse generale, un cumulo di procedimenti e di sanzioni di natura equiparabile a quella penale può risultare giustificato qualora tali procedimenti e sanzioni perseguano, in vista di quell'obiettivo, scopi complementari, eventualmente relativi ad aspetti differenti della medesima condotta illecita in questione. Questa ipotesi non ricorre, secondo la Corte, nel caso di procedimenti condotti da autorità garanti della concorrenza degli Stati membri in applicazione dell'art. 101 TFUE e delle corrispondenti norme *antitrust* nazionali. La ragione è connessa all'assetto delineato dal reg. n. 1/2003: in base all'art. 3, par. 1, quando un'autorità nazionale di concorrenza applica la legislazione nazionale in materia di concorrenza a intese che possono pregiudicare il commercio tra Stati membri, essa è tenuta ad applicare anche l'art. 101 TFUE; l'art. 3, par. 2 stabilisce che l'applicazione del diritto nazionale in materia di concorrenza non può comportare il divieto di intese che siano idonee a pregiudicare il commercio tra Stati membri, qualora esse siano compatibili con l'art. 101 (in quanto non comportano restrizioni alla concorrenza ai sensi dell'art. 101, par. 1, TFUE o soddisfano le condizioni dell'art. 101, par. 3, TFUE o ricadono in un regolamento ai sensi dell'art. 101, par. 3, TFUE). Da tali disposizioni si evince che per le intese l'applicazione delle norme nazionali in materia di concorrenza non può condurre a un risultato diverso da quello che deriverebbe dall'applicazione dell'art. 101, par. 1, TFUE. Ne deriva che se due autorità nazionali garanti della concorrenza avviassero procedimenti e irrogassero sanzioni nei confronti degli stessi fatti per assicurare l'osservanza del divieto di intese di cui all'art. 101 TFUE e delle corrispondenti norme del loro rispettivo diritto nazionale, esse perseguirebbero non già scopi complementari vertenti su aspetti differenti del medesimo comportamento, ma lo stesso obiettivo di interesse generale consistente nell'assicurare che la concorrenza nel mercato interno non sia falsata da intese anticoncorrenziali. In tali circostan-

Da qui si spiega l'importanza cruciale delle due pronunce in vista della futura interazione tra il DMA e il diritto della concorrenza dell'Unione e nazionale. E non solo in ragione della nebulosità della distinzione tra interesse generale e interesse giuridico da tutelare. Ma proprio perché l'abbandono di quest'ultimo criterio ha "confuso le acque" e ha aperto la strada al proliferare di ipotesi in cui un'impresa possa essere assoggettata a due procedimenti separati (ad esempio, DMA e diritto nazionale della concorrenza), ciascuno avviato da un'autorità diversa. Con la conseguenza che spetterà al giudice nazionale dirimere la controversia alla luce dei criteri Menci e verificare che i due procedimenti perseguano obiettivi complementari di interesse generale relativi, a seconda dei casi, ad aspetti distinti dello stesso comportamento illecito<sup>85</sup>.

---

ze, secondo la Corte di giustizia, un cumulo di procedimenti e sanzioni non può essere giustificato ai sensi dell'art. 52, par. 1, della Carta.

<sup>85</sup> È proprio quanto, in conclusione, hanno sostenuto M. CAPPALÌ, G. COLANGELO, *op. cit.*, secondo cui «[l']arresto della Grande Sezione ha l'indubbio merito di sgomberare il campo dall'equivoco teorico che ha a lungo investito la nozione di *idem*, declinata per circa due decenni in modo differente a seconda dell'area del diritto europeo interessata (*idem crimen*, nel diritto della concorrenza; *idem factum*, in tutti gli altri settori). Si auspica che questa (lungamente attesa) opera di razionalizzazione possa favorire l'emersione di un *acquis giurisprudenziale* maggiormente coerente e completo. Grazie a queste pronunce, infatti, le esperienze maturate ciascun settore del diritto europeo potranno contribuire allo sviluppo di una matrice condivisa del principio di *ne bis in idem*. Sbaglierebbe, tuttavia, l'interprete a pensare che *bPost* e *Nordzucker* risolvano ogni problema». Si rimanda, inoltre, a P. DE PASQUALE, *Uno, nessuno e centomila. I criteri di operatività del principio *ne bis in idem**, cit., 256 e ID., *Finale di partita per il principio del *ne bis in idem*? Breve nota alle sentenze *bpost* e *Nordzucker* e a.*, cit., 9, secondo cui «[...] l'abbandono del criterio dell'interesse giuridico protetto comporta che, nelle ipotesi in cui un'impresa sia soggetta a due procedimenti separati (*DMA* e diritto nazionale della concorrenza), ciascuno portato avanti da un'autorità diversa, la limitazione del *ne bis in idem* è giustificata soltanto se tali procedimenti perseguono, al fine di raggiungere un obiettivo legittimo di interesse generale, obiettivi complementari relativi, a seconda dei casi, ad aspetti distinti dello stesso comportamento illecito. Complementarietà che, peraltro, è valutabile soltanto *ex post*; cioè nel momento in cui un giudice è chiamato a stabilire se le due autorità hanno effettivamente coordinato i loro procedimenti e se la sanzione eventualmente inflitta nel primo procedimento è stata presa in considerazione nella valutazione della seconda sanzione. Le due sentenze non invertono, quindi, il trend che ha trasformato il principio del *ne bis in idem* da *test ex ante*, definito normativamente, a *test correttivo ex post*, che opera sulla base di criteri circostanziali e accidentali precisati dalla giurisprudenza. E che non impedisce la possibilità di duplicazione di procedimenti e di sanzioni. Neppure si discostano da un approccio casistico e atomizzato, lasciando il giudice privo di una soluzione uniforme dei problemi derivanti in tali ipotesi. Come si è già avuto modo di rilevare, il principio del *ne bis in idem*, interpretato alla luce di un maggiore o minore nesso materiale e temporale tra due procedimenti sanzionatori, ed ora della complementarietà degli obiettivi, presenta così tanti elementi di incertezza e di complessità da affievolire arbitrariamente il diritto delle persone a non essere giudicate né condannate due volte per gli stessi fatti [...]». Da ultimo, dopo la lunga serie di altalenanti interventi giudiziari sinora esaminati a livello della Corte EDU e della Corte di giustizia, il principio di *ne bis in idem* irrompe anche nel palcoscenico della Corte costituzionale. Oggetto specifico di cen-

## 5. La novella dell'abuso di dipendenza economica nei mercati digitali introdotta dal DDL Concorrenza

Nel prossimo futuro, dunque, le grandi piattaforme digitali saranno soggette a diverse cornici normative potenzialmente sovrapponibili all'interno dell'Unione europea, vale a dire: (i) il DMA; (ii) il diritto *antitrust* dell'Unione; e (iii) le norme nazionali in materia di concorrenza (comprese le norme a tutela della concorrenza specificamente “congegnate” per i mercati digitali)<sup>86</sup>.

Oltre a quelli citati, è verosimile attendersi un altro scenario di potenziale conflitto e di cortocircuito con l'art. 29 del DDL 2469 – legge annuale per il mercato e la concorrenza 2021 (ora divenuto art. 33, nel testo approvato in Senato lo scorso 30 maggio 2022 e “sfociato” nella legge 5 agosto 2022, n. 118, entrata in vigore lo scorso 27 agosto)<sup>87</sup>, che ha integrato

---

sura da parte della Corte costituzionale, con la recentissima sentenza n. 149/2022 resa in data 10 maggio 2022, è stato il meccanismo di doppio binario sanzionatorio previsto dalla legge n. 633 del 22 aprile 1941 in materia di diritto d'autore, un sottosistema punitivo meno soggetto all'attenzione dagli operatori del diritto e dagli interpreti rispetto al doppio binario vigente in materia di abusi di mercato nonché con riguardo alla materia sanzionatoria tributaria. Si veda, per una prima analisi della pronuncia, M. SCOLETTA, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, in *www.sistemapenale.it*, 23 giugno 2022; J. DELLA VALENTINA, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection*, *ivi*, 24 novembre 2022.

<sup>86</sup> Si veda K. BANIA, *op. cit.*, 33-34, secondo cui «[r]ecent developments in the field of competition law showcase that the implementation of the DMA may trigger the ne bis in idem principle in subsequent competition proceedings. The example of the P2B Regulation depicts that the DMA may render certain rules devoid of purpose. In such cases, despite the “without prejudice” clause, the DMA would not necessarily complement existing rules. Depending on the case, the conflict under consideration could undermine the overall regulatory framework for protecting businesses and consumers against problematic platform conduct. All in all, contrary to the intention of the legislator, the DMA may not necessarily be compatible with other instruments. At the outset, this may not necessarily harm businesses and end users protected by other regulatory tools. [...] A word of caution is in order. This paper has focused on instruments that form part of the existing framework. How the DMA is placed in the overall structure is an exercise that should go beyond resolving the tension between those instruments and the DMA, for an avalanche of legislative proposals for platforms is currently taking place. Absent reflection on (and resolution of) this matter will undermine legal certainty and the objectives of the emerging regulatory regime for harmful platform practices».

<sup>87</sup> Tale proposta di riforma/integrazione prende le mosse dalla segnalazione inviata dall'AGCM al Governo, nell'ambito dei suoi poteri di *advocacy*, in data 22 marzo 2021 al fine della predisposizione del disegno di legge annuale per il mercato e la concorrenza (AS1730). Al punto C della sezione VII della segnalazione, rubricata “I poteri dell'Autorità e le modifiche alla Legge n. 287/90”, l'AGCM propone un nuovo statuto dell'abuso di dipendenza economica nel

l'istituto dell'abuso di dipendenza economica, introducendo all'art. 9, legge 18 giugno 1998, n. 192 (d'ora in avanti, la "legge sulla subfornitura" o "legge n. 192/1998"):

(i) una presunzione superabile – e, come tale, non assoluta – di dipendenza economica nel caso di impresa che utilizza servizi di intermediazione forniti da una piattaforma digitale che abbia un ruolo determinante per raggiungere utenti finali o fornitori, anche in termini di effetti di rete o di disponibilità dei dati (inserendo un nuovo comma 1-*bis*)<sup>88</sup>;

(ii) un elenco (non vincolante) di pratiche abusive realizzate dalle piattaforme digitali che possono integrare un abuso di dipendenza economica, modificando *ex novo* il comma 2 (fornire informazioni o dati insufficienti

---

contesto delle piattaforme digitali, nei termini che seguono: «L'Autorità auspica un'integrazione dell'articolo 9 della legge 18 giugno 1998, n. 192, volta a rendere le previsioni relative all'abuso di dipendenza economica più appropriate ed efficaci rispetto alle caratteristiche e, in particolare, al potere di intermediazione delle grandi piattaforme digitali. La modifica proposta riguarda l'introduzione di una presunzione relativa di dipendenza economica nelle relazioni commerciali con un'impresa che offre i servizi di intermediazione di una piattaforma digitale, allorché quest'ultima abbia un ruolo determinante per raggiungere utenti finali e/o fornitori, anche in termini di effetti di rete e/o di disponibilità dei dati. Trattandosi di una presunzione relativa, è sempre possibile per la piattaforma dimostrare che non sussiste la dipendenza economica per le imprese terze. La proposta di modifica si completa con l'indicazione esemplificativa di alcune pratiche che possono integrare un abuso di dipendenza economica da parte delle piattaforme. In tal modo si intende fornire una prima indicazione delle condotte vietate, cosicché, anche sotto il profilo della certezza giuridica, le piattaforme possano più facilmente definire e orientare il proprio comportamento nelle relazioni commerciali con le imprese terze che utilizzano i loro servizi di intermediazione».

<sup>88</sup> Ciò è in linea con i principi di difesa e al contraddittorio propri del nostro ordinamento, in quanto la presunzione introdotta dalla norma è superabile, fornendo prova dell'assenza dello stato di dipendenza economica del soggetto che si rivolge alla piattaforma con posizione predominante (per esempio per accessibilità a fonti alternative sul mercato). Occorre evidenziare, però, che un eventuale accertamento positivo della dipendenza non equivarrebbe, di per sé, a un giudizio di abusività della condotta indagata, giacché, in tal caso, andrà ulteriormente indagata la reale possibilità, per la parte che abbia subito l'abuso, «di reperire sul mercato alternative soddisfacenti» e, per l'impresa in posizione di dominanza, «di determinare, nei rapporti commerciali con un'altra impresa, un eccessivo squilibrio di diritti e di obblighi», così come previsto dall'art. 9, comma 1, legge n. 192/1998. L'opzione a favore di una tecnica presuntiva, in alternativa a quella fondata sulla dimostrazione della dipendenza economica, riflette la valenza onnivora delle tecnologie informatiche utilizzate dagli operatori che operano su mercati a più versanti. Si delinea, quindi, una presunzione relativa di dipendenza economica, programmata in via istituzionale, di natura algoritmica, ossia derivante dalla capacità di processare una molteplicità di dati e di concentrare i processi cognitivi, anche mediante sistemi di intelligenza artificiale, che diventano sempre più indispensabili per le attività produttive e distributive delle imprese. In questo scenario, la tecnica presuntiva tende ad agevolare il contenzioso, atteso che la presunzione relativa può essere ribaltata soltanto da una prova contraria sugli effettivi rapporti di forza tra le imprese e sulla possibilità di ricorrere a soluzioni alternative senza dover affrontare costi insormontabili.

in merito all'ambito o alla qualità del servizio erogato e nel richiedere indebite prestazioni unilaterali non giustificate dalla natura o dal contenuto dell'attività svolta, ovvero nell'adottare pratiche che inibiscono od ostacolano l'utilizzo di diverso fornitore per il medesimo servizio, anche attraverso l'applicazione di condizioni unilaterali o costi aggiuntivi non previsti dagli accordi contrattuali o dalle licenze in essere). Dunque, la norma integra l'elenco (non tassativo) delle pratiche abusive, arricchendolo di ipotesi, formulate sì in termini generali, ma che appaiono suggerite dall'esperienza dei rapporti tra le grandi piattaforme digitali e le imprese che si avvalgono dei loro servizi di intermediazione<sup>89</sup>.

---

<sup>89</sup> Non è questa la sede per soffermarci oltre sul tema, ma è opportuno ricordare che la presunzione introdotta nella nuova novella del DDL Concorrenza non è ignota ad altre fattispecie del diritto europeo (specialmente – e con la maggiore forza della presunzione assoluta – sui ritardi nei pagamenti). Nel digitale, pur non ricorrendo alla presunzione, vi sono comunque analoghe discipline nazionali avanzate e di maggior tutela anche (o specificamente rivolte) verso le grandi piattaforme. Su analoghe discipline di maggior tutela in Germania è stata introdotta una nuova forma di dipendenza economica nei mercati a due versanti: un'impresa che fornisce servizi essenziali di intermediazione è anche soggetta al divieto di discriminazione se non ci sono possibilità e operatori alternativi per sostituire il servizio di intermediazioni originariamente fornito. In Germania, insomma, lo stesso utilizzatore dovrà provare la situazione di predominanza nei suoi confronti e l'assenza di alternative ragionevoli e disponibili. In Italia, invece, l'utilizzatore, tipicamente piccola e media impresa, dovrà provare la situazione di predominanza nei suoi confronti, ciò che passa per l'assenza di alternative ragionevoli per il proprio business, mentre all'operatore sarà consentito individuare l'esistenza di altre possibili e oggettive alternative sul mercato, così superando la presunzione di dominanza. Altrettanto può dirsi per Francia e Belgio, dove sono state introdotte misure specifiche in materia di dipendenza economica: queste, per la portata generale che rivestono, si estendono ovviamente anche alle piattaforme digitali. Più in generale la presunzione spinge le grandi piattaforme che hanno un ruolo predominante ad adottare *ex ante* condizioni contrattuali eque e non discriminatorie nei confronti delle imprese, potendo poi agevolmente dimostrare in un eventuale giudizio la legittimità dei loro comportamenti; anziché far gravare l'onere della prova sull'impresa, soggetto più debole, che generalmente è costretta ad accettare condizioni discriminatorie per non perdere l'occasione di stare sulla piattaforma. A tal riguardo, si veda il nuovo art. 18, par. 3(b), GWB, che introduce una nuova forma di dipendenza economica nei mercati a due versanti (un'impresa che fornisce servizi essenziali di intermediazione è anche soggetta al divieto di discriminazione se non ci sono possibilità e operatori alternativi per sostituire il servizio di intermediazioni originariamente fornito). Inoltre, il Belgio ha recentemente adottato nuove disposizioni che vietano l'abuso di dipendenza economica: in particolare, una legge del 4 aprile 2019, entrata in vigore il 22 agosto 2020, ha introdotto l'articolo IV.2/1 nel Codice di diritto economico belga (Code of Economic Law – “CEL”). Anche in Francia, l'abuso di dipendenza economica è espressamente contemplato dall'art. L 420-2 del Codice di commercio francese (French Commercial Code – “FCC”). Più nello specifico, secondo la nuova formulazione dell'art. 20, par. 1 e 1(a), GWB, l'abuso di posizione dominante «shall also apply to undertakings acting as intermediaries on multi-sided markets to the extent that other undertakings are dependent on their intermediary services for accessing supply and sales markets in such a way that sufficient and reasonable alternatives do not exist» e, soprattutto, «[d]ependence [...] may also arise from the fact that an undertaking is de-

L'art. 9, legge 18 giugno 1998, n. 192 ha introdotto nel nostro ordinamento l'istituto della dipendenza economica<sup>90</sup>, stabilendo che:

---

*pendent on accessing data controlled by another undertaking in order to carry out its own activities*». Inoltre, l'art. L420-2 francese prevede che: «Est prohibée, dans les conditions prévues à l'article L. 420-1, l'exploitation abusive par une entreprise ou un groupe d'entreprises d'une position dominante sur le marché intérieur ou une partie substantielle de celui-ci. Ces abus peuvent notamment consister en refus de vente, en ventes liées ou en conditions de vente discriminatoires ainsi que dans la rupture de relations commerciales établies, au seul motif que le partenaire refuse de se soumettre à des conditions commerciales injustifiées. Est en outre prohibée, dès lors qu'elle est susceptible d'affecter le fonctionnement ou la structure de la concurrence, l'exploitation abusive par une entreprise ou un groupe d'entreprises de l'état de dépendance économique dans lequel se trouve à son égard une entreprise cliente ou fournisseur. Ces abus peuvent notamment consister en refus de vente, en ventes liées, en pratiques discriminatoires visées aux articles L. 442-1 à L. 442-3 ou en accords de gamme». Quanto al Belgio: «Est interdit, sans qu'une décision préalable ne soit nécessaire à cet effet, le fait pour une ou plusieurs entreprises d'exploiter de façon abusive une position dominante sur le marché belge concerné ou dans une partie substantielle de celui-ci. Ces pratiques abusives peuvent notamment consister à: 1° imposer de façon directe ou indirecte des prix d'achat ou de vente non équitables ou d'autres conditions de transaction non équitables; 2° limiter la production, les débouchés ou le développement technique au préjudice des consommateurs; 3° appliquer à l'égard de partenaires commerciaux des conditions inégales à des prestations équivalentes, en leur infligeant de ce fait un désavantage dans la concurrence; 4° subordonner la conclusion de contrats à l'acceptation, par les partenaires, de prestations supplémentaires qui, par leur autre ou selon les usages commerciaux, n'ont pas de lien avec l'objet de ces contrats».

<sup>90</sup>M.R. MAUGERI, *Abuso di dipendenza economica e autonomia privata*, Giuffrè, Milano, 2003, *passim*; ID., *Subfornitura e abuso di dipendenza economica. Fra diritto civile e diritto alla concorrenza*, Giappichelli, Torino, 2022, *passim*; P. FABBIO, *L'abuso di dipendenza economica*, Giuffrè, Milano, 2006, 9 ss.; ID., *Abuso di dipendenza economica*, in A. CATRICALÀ, E. GABRIELLI (a cura di), *I contratti nella concorrenza*, in Tratt. contratti Rescigno-Gabrielli, 2011, 271 ss.; V. FALCE, M. MAUGERI, *Indotto, concorrenza e mercato: il caso della subfornitura*, in *Anal. giur. econ.*, n. 2, 2011, 273 ss.; C. OSTI, *L'abuso di dipendenza economica*, in *Merc. conc. reg.*, n. 1, 1999, 9 ss.; G. DI LORENZO, *Abuso di dipendenza economica e contratto nullo*, Cedam, Padova, 2009, *passim*; R. NATOLI, *L'abuso di dipendenza economica. Il contratto e il mercato*, Jovene, Napoli, 2004, *passim*; A. VILLELLA, *Abuso di dipendenza economica ed obbligo a contrarre*, Edizioni Scientifiche Italiane, Napoli, 2009, *passim*. Per un'analisi a livello comparato, in dottrina, V. FALCE, *Abuse of economic dependence and competition law remedies: a sound interpretation of the Italian Regulation*, in *European Competition Law Review*, n. 2, 2015, 71 ss.; ID., *The Italian regulation against the abuse of economic dependence at the crossroads*, in F. DI PORTO, R. PODSZUN (eds.), *Abusive Practices in Competition Law*, Edward Elgar, 2018. Più in generale, il divieto di abuso di dipendenza economica riflette le preoccupazioni scaturenti dall'asimmetria del potere contrattuale nell'ambito delle relazioni commerciali, la quale è vista come foriera di potenziali termini e condizioni contrattuali iniqui. In quest'ottica, le disposizioni che vietano l'abuso di dipendenza economica mirano a proteggere il contraente debole nei confronti del *partner* commerciale che, in considerazione delle caratteristiche del contratto, potrebbe sfruttare a proprio vantaggio una posizione di potere contrattuale. In particolare, lo *status* di dipendenza economica richiede la dimostrazione di significative barriere all'uscita dalla relazione commerciale in corso, ossia della mancanza sul mercato per la parte debole di alternative soddisfacenti a quel determinato *partner* contrattuale. La dipendenza economica è, infatti, principal-

– È vietato l'abuso da parte di una o più imprese dello stato di dipendenza economica nel quale versi una impresa cliente o fornitrice nei suoi o nei loro confronti.

– Sussiste una situazione di dipendenza economica quando un'impresa subisce, nei rapporti commerciali con un'altra impresa, un eccessivo squilibrio di diritti e di obblighi, che la controparte è, dunque, in grado di determinare<sup>91</sup>.

– L'abuso, che esprime lo sfruttamento illecito della posizione di forza rivestita, può consistere nel rifiuto di vendere o nel rifiuto di comprare, nella imposizione di condizioni contrattuali ingiustificatamente gravose o discriminatorie, nella interruzione arbitraria delle relazioni commerciali in atto<sup>92</sup>.

– La competenza all'accertamento dell'illecito è del giudice civile per i profili privatistici, cui si aggiunge, nel caso di impatto significativo dell'abuso sul mercato nazionale, la competenza dell'AGCM (indipendentemente dalla posizione di dominanza occupata sul mercato rilevante dalla controparte, ai sensi della legge n. 287/1990).

È, quindi, di tutta evidenza che potrebbe proporsi un ulteriore scenario di sovrapposizione, se non di cumulo, tra le disposizioni del DMA e la novella riguardante l'abuso di dipendenza economica.

---

mente il risultato di rilevanti costi di conversione (*switching costs*) che imprigionano la parte debole in una relazione commerciale, non consentendole di individuare adeguate soluzioni alternative. In questo senso, per dare contenuto alla disposizione in esame non può non farsi riferimento alla teoria economica dei costi di transazione, la quale ha illustrato come il governo delle relazioni contrattuali sia fortemente influenzato dall'eventuale presenza di investimenti specifici (*transaction-specific investments*) che una parte può essere chiamata a sostenere in ragione della natura del contratto e/o delle condizioni pattuite. È l'entità degli investimenti specifici a determinare la condizione di dipendenza economica e la "prigione" (*lock-in*) del contraente debole. Si considerano tali solo quegli investimenti che, non essendo suscettibili di riconversione, andrebbero perduti qualora la relazione contrattuale in corso dovesse interrompersi. Di conseguenza, maggiori saranno gli investimenti specifici sostenuti da una parte, maggiore sarà il potere contrattuale della controparte e la possibilità per quest'ultima di imporre condizioni contrattuali squilibrate ed inique (*hold-up*).

<sup>91</sup> Art. 9, comma 1: «È vietato l'abuso da parte di una o più imprese dello stato di dipendenza economica nel quale si trova, nei suoi o nei loro riguardi, una impresa cliente o fornitrice. Si considera dipendenza economica la situazione in cui una impresa sia in grado di determinare, nei rapporti commerciali con un'altra impresa, un eccessivo squilibrio di diritti e di obblighi. La dipendenza economica è valutata tenendo conto anche della reale possibilità per la parte che abbia subito l'abuso di reperire sul mercato alternative soddisfacenti».

<sup>92</sup> Art. 9, comma 2: «L'abuso può anche consistere nel rifiuto di vendere o nel rifiuto di comprare, nella imposizione di condizioni contrattuali ingiustificatamente gravose o discriminatorie, nella interruzione arbitraria delle relazioni commerciali in atto».

Occorre, perciò, interrogarsi circa la sorte delle condotte in ipotesi integranti un potenziale abuso di dipendenza economica a seguito dell'avvio di un procedimento ai sensi del DMA.

Ebbene, è di tutta evidenza come il DMA, le norme a tutela della concorrenza e l'abuso di dipendenza economica presidino e mirino a salvaguardare interessi tra loro difforni, dal ché dovrebbe discenderne la pacifica applicazione parallela. Come noto, mentre l'abuso di posizione dominante, rilevante per integrare qualsiasi fattispecie *antitrust*, comporta la necessità di delimitare anzitutto il mercato rilevante, l'abuso di dipendenza economica attribuisce rilievo non alla posizione dominante di un'impresa sul mercato, ma all'abuso e allo squilibrio delle imprese nell'ambito di un rapporto negoziale<sup>93</sup>. E, del resto, secondo l'art. 9 della legge sulla subfornitura si considera «*dipendenza economica la situazione in cui una impresa sia in grado di determinare nei rapporti commerciali con un'altra impresa un eccessivo squilibrio di diritti e di obblighi*»<sup>94</sup>.

In altre parole, mentre le norme a tutela della concorrenza sono disposizioni generali dirette a tutelare il processo concorrenziale in relazione all'assetto di mercato, la norma relativa alla dipendenza economica, prevista nella disciplina della subfornitura nelle attività produttive (e, dunque, anche la riformulazione derivante dal DDL Concorrenza con le relative aggiunte ora approvate), costituisce una regola inerente alla disciplina dei rapporti contrattuali fra le parti, con finalità che possono prescindere dalla loro incidenza sui meccanismi concorrenziali<sup>95</sup>. Senza contare che il DMA

---

<sup>93</sup> Sul punto, si veda M. LIBERTINI, *Posizione dominante individuale e posizione dominante collettiva*, in *Riv. dir. comm.*, n. 1, 2003, 543 ss.; V. FALCE, *Rapporti asimmetrici tra imprese e soluzioni pro-concorrenziali. Note minime su evoluzione normative e giurisprudenziale*, in *Riv. dir. ind.*, n. 4-5, 2021, 189 ss.; G. COLANGELO, *L'abuso di dipendenza economica tra disciplina della concorrenza e diritto dei contratti. Un'analisi economica e comparata*, Giappichelli, Torino, 2004, *passim*. Per queste ragioni, la situazione di dipendenza economica è anche descritta come potere di mercato relativo, in contrapposizione alla posizione di potere di mercato assoluto che caratterizza la posizione dominante, ossia una delle soglie principali che giustifica l'applicazione del diritto della concorrenza. In sintesi, nella dipendenza economica l'indagine mira a valutare l'uso di un potere economico nell'ambito di una relazione contrattuale (e, dunque, nei confronti di uno specifico partner commerciale), anziché sull'intero mercato (e, dunque, nei confronti di qualsiasi operatore economico).

<sup>94</sup> Non è decisivo, invece, che l'abuso di dipendenza economica sia prevista dal legislatore espressamente con riguardo solo alla fattispecie della subfornitura nelle attività produttive, poiché, per giurisprudenza consolidata, esso rappresenta un principio generale (si veda, tra le altre, Cass., Sez. Un., sentenza 25 novembre 2011, n. 24906; Cass. civ., sez. III, sentenza 23 luglio 2014, n. 16787).

<sup>95</sup> Si veda, ancora, Trib. Milano, sentenza 6 dicembre 2017, R.G. 25998/2015; Trib. Bergamo, Sez. IV, sentenza 4 gennaio 2017, R.G. n. 6591/2016.

persegue ancora un'ulteriore differente finalità, quella di assicurare la "contestabilità" e la *fairness* nei mercati digitali. Tre moventi di interesse pubblico differenti, dunque, che, a rigore, ne giustificano e ne legittimano l'applicazione parallela e l'eventuale cumulo di sanzioni<sup>96</sup>.

Ebbene, è proprio quello che pare esser accaduto con il nuovo comma 2 dell'art. 9 della legge sulla subfornitura, con l'inserimento di ulteriori obbligazioni aggiuntive, potenzialmente integranti un abuso di dipendenza economica, non ricollegabili al ruolo "pivotale" di *gatekeeping* di tali operatori (e, quindi, come detto, non rientranti nel perimetro di applicazione del DMA).

## 6. Conclusioni

A partire dal 2023, la riforma epocale del DMA, da "cantiere aperto", diventerà pienamente operativa e si vedrà sul campo se le obbligazioni imposte ai *gatekeeper* ai sensi degli artt. 5-7 DMA rimpiazzeranno, nell'applicazione pratica dell'*enforcement antitrust*, gli artt. 101 e 102 TFUE oppure se – memore del considerando 86 – la Commissione utilizzerà il DMA come strumento di regolamentazione davvero complementare al diritto della concorrenza (europeo e domestico).

Ciò premesso, il presente contributo ha inteso ripercorrere le linee di-

---

<sup>96</sup> Per una conclusione in tal senso, si rimanda a V. FALCE, *L'abuso di dipendenza economica nel digitale. Perché no?*, in *Filodiritto*, 5 maggio 2022 secondo cui «[q]uanto all'altra obiezione, secondo cui con il DMA non ci sia più necessità di introdurre l'art. 29 del DDL Concorrenza, va precisato che Digital Markets Act e dipendenza economica sono discipline diverse che perseguono fini diversi. Il DMA è teso a garantire la contendibilità dei mercati attraverso obblighi e divieti. Non solo il DMA si rivolge solo a pochi gatekeeper ma soprattutto in caso di violazioni, gli utilizzatori finali non godono di alcuna tutela, perché il DMA è disciplina di diritto pubblico e non di diritto privato. Insomma, l'istituto della dipendenza completa il DMA anziché sovrapporsi ad esso (un po' come l'azione di classe rispetto all'illecito antitrust), consentendo di accedere alla giustizia civile o amministrativa se un diritto esiste e questo è stato violato. Né infine c'è sovrapposizione o contrasto formale, perché il DMA chiarisce da subito (come è ovvio) che la regolazione UE non incide, né interferisce sulla disciplina nazionale e men che meno su quella a tutela della concorrenza e dell'abuso di dipendenza economica». In risposta a talune critiche giunte dagli operatori del settore con riguardo a una presunta eccessiva indeterminazione dei casi ai quali si applica la norma e del suo futuro *enforcement*, il nuovo testo approvato dal Senato ha compiuto significativi passi in avanti, prevedendo, all'art. 33, comma 3, l'adozione di linee guida da parte della Presidenza del Consiglio dei ministri, d'intesa con il Ministero della giustizia e sentita l'AGCM, «dirette a facilitare l'applicazione delle disposizioni [...], in coerenza con i principi della normativa europea, anche al fine di prevenire il contenzioso e favorire buone pratiche di mercato in materia di concorrenza e libero esercizio dell'attività economica».

rettrici di un percorso tortuoso, che origina da una nuova strategia industriale per l'Europa, passa attraverso le insidie che si annidano nel rapporto tra la regolazione del DMA e le norme a tutela della concorrenza europee e nazionali e culmina, attraverso una disamina giurisprudenziale del principio del *ne bis in idem*, con le “storiche” (a loro modo) pronunce della Corte di giustizia nei casi *bpost* e *Nordzucker*.

Come ribadito nel corso del presente contributo, lo stesso “cortocircuito” logico palesatosi nel rapporto tra DMA e norme *antitrust* (europee e “domestiche”) si è presentato con l'approvazione dell'art. 33 del DDL Concorrenza in materia di abuso di dipendenza economica nei mercati digitali, dinanzi al quale si è tentato di argomentare che, in verità, il DMA e la disciplina della dipendenza economica perseguono fini diversi e, anziché sovrapporsi, si completano vicendevolmente.

Ciononostante, per quanto la Corte di giustizia in *bpost* e *Nordzucker* abbia fornito istruzioni mediamente particolareggiate, il nodo è ben lungi dall'esser dipanato e ci si attende che, a valle dell'entrata in vigore del DMA, quello del potenziale cumulo di procedimenti e di sanzioni – e, quindi, del rapporto tra concorrenza e regolazione – costituirà un terreno fertile per l'avvio di lunghi contenziosi.

Silvia Giudici

# Intelligenza artificiale e diritti di proprietà industriale e intellettuale. Spunti preliminari

SOMMARIO: 1. Introduzione. – 2. L’apporto creativo. – 3. La titolarità. – 4. Conclusioni.

## 1. Introduzione

La disciplina della proprietà industriale ed intellettuale è sin dalle sue origini inscindibilmente connessa allo sviluppo delle nuove tecnologie, non solo perché la *ratio* del sistema brevettuale è proprio quella di incentivare, con la concessione di un premiale diritto di esclusiva, il progresso tecnologico e la sua diffusione, ma anche perché l’effettività della tutela può essere messa in crisi proprio dall’uso diffuso delle nuove tecnologie.

Si assiste così ad un inesorabile e continuo tentativo del legislatore internazionale, europeo e nazionale di adattare il sistema normativo della proprietà industriale ed intellettuale al progressivo evolversi dello sviluppo tecnologico, con l’estensione (proprio al fine di incentivare l’innovazione) del sistema brevettuale (o di sistemi affini) a tutti i nuovi settori<sup>1</sup>, e con importanti modifiche alla legislazione sul diritto d’autore, al fine di contrastare gli attacchi della tecnologia digitale e della comunicazione globale alla effettività della tutela autorale.

Si discute oggi, in particolare dei c.d. sistemi di “Intelligenza Artificiale”, di quelle macchine cioè che, sempre più, sono in grado di sostituire l’intelligenza e la creatività umana.

---

<sup>1</sup> Non solo a partire dai Trips è stato previsto che “*possono costituire oggetto di brevetto le invenzioni, di prodotto o di procedimento, in tutti i campi della tecnologia*” (art. 27 Trips), ma progressivamente la protezione è stata estesa e adattata a nuove creazioni intellettuali (si pensi, a mero titolo esemplificativo, alle topografie di prodotti a semiconduttori e alle invenzioni biotecnologiche).

Va tuttavia, preliminarmente, ricordato che gli investimenti sull'intelligenza artificiale e sul digitale sono essenziali per il Paese, per l'innovazione e per la competitività delle imprese che vi operano, e che le imprese trovano un importante incentivo ad investire nei mezzi che concorrono a produrre innovazione (e quindi anche nei sistemi di Intelligenza Artificiale o attraverso l'Intelligenza artificiale) proprio nel sistema brevettuale che garantisce appunto un'esclusiva sui frutti dell'attività di ricerca e sviluppo, non solo con riferimento alla macchina intelligente ma anche con riferimento al risultato derivante dall'uso della macchina intelligente.

## 2. L'apporto creativo

Ed invero, il tema dell'Intelligenza artificiale è particolarmente sentito e dibattuto, soprattutto con riferimento alla fase della produzione di "beni" astrattamente proteggibili con il diritto della proprietà industriale e intellettuale poiché la c.d. Intelligenza Artificiale e i sistemi di Intelligenza Artificiale hanno iniziato ad influenzare il processo creativo dei beni protetti, giungendo addirittura a crearli in modo autonomo.

Tradizionalmente, tuttavia, l'apporto "creativo" dell'uomo è sempre stato considerato essenziale nella ideazione e creazione delle opere dell'ingegno suscettibili di protezione attraverso i diversi istituti della proprietà industriale e intellettuale, ma oggi si sta sempre più assistendo alla creazione di "opere", astrattamente proteggibili dal diritto d'autore o dal diritto brevettuale, da parte dell'Intelligenza Artificiale o, comunque, attraverso l'apporto, essenziale, determinante e talvolta autonomo, della Intelligenza Artificiale.

Ed allora il dogma in base al quale le "opere dell'ingegno" (siano esse invenzioni vere e proprie o opere protette dal diritto d'autore) sono create dall'uomo e appartengono al suo autore, viene posto in discussione.

Le criticità maggiormente toccano la disciplina del diritto d'autore, del c.d. "*copyright*", fortemente incentrata sulla "creatività" dell'opera attribuibile al soggetto umano che ne ha dato origine: la Corte di Giustizia ha infatti ripetutamente affermato che l'opera è proteggibile dal diritto d'autore solo se dotata di "carattere creativo" e quindi solo se riflette la personalità del suo autore. Il problema della attribuzione del diritto su un'opera *computer generated*, e cioè creata non dall'uomo avvalendosi di un computer programmato, ma esclusivamente dal computer, ha indotto autorevole dottrina<sup>2</sup>

---

<sup>2</sup> Cfr. G. SENA, *Intelligenza artificiale, opere dell'ingegno e diritti di proprietà industriale e in-*

a ritenere che l'opera *computer generated* cade immediatamente, per sua natura, in pubblico dominio e su di essa neppure può sorgere un diritto di esclusiva.

### 3. La titolarità

Il tema della titolarità dei diritti acquista però una grandissima importanza nel caso di vere e proprie invenzioni, intese come soluzioni di un problema tecnico, create, o meglio interamente generate, dalla Intelligenza Artificiale<sup>3</sup>: l'impresa ha evidentemente interesse ad investire sull'Intelligenza Artificiale (e cioè sul mezzo che produce innovazione) solo se il sistema brevettuale garantisce poi all'imprenditore, che ha sopportato il costo spesso ingente della ricerca, un'esclusiva sui frutti dell'attività di ricerca e sviluppo.

Probabilmente in questo caso sarebbe quantomeno opportuno giungere a risultati diversi rispetto a quelli a cui si giunge inesorabilmente in materia di *copyright*.

Il Codice della proprietà industriale stabilisce che “*il diritto morale di essere riconosciuto autore dell'invenzione può essere fatto valere dall'inventore e dopo la sua morte, dal coniuge e dai discendenti fino al secondo grado; in loro mancanza o dopo la loro morte, dai genitori e dagli altri ascendenti e in mancanza, o dopo la morte anche di questi, dai parenti fino al quarto grado*” (art. 62 c.p.i.), con la precisazione che alla domanda di brevetto nazionale deve essere unita “*la designazione dell'inventore*” (cfr. art. 160.3, lett. c), c.p.i.). Parimenti, la Convenzione di Monaco prevede che “*L'inventore ha il diritto, nei riguardi del titolare della domanda di brevetto europeo o del brevetto europeo, di essere designato come tale presso l'Ufficio europeo dei brevetti*” (art. 62 EPC 2000), che “*La domanda di brevetto europeo deve comprendere la designazione dell'inventore*” e, infine, che “*Se il richiedente non è l'inventore o l'unico inventore, la designazione deve contenere una dichiarazione indicante in quale modo il richiedente ha acquisito il diritto al brevetto*” (art. 81 EPC 2000).

Il diritto morale, anche nel sistema brevettuale, sembrerebbe dover appartenere ad una “persona fisica”, ma se bene si osserva da un lato tale di-

---

tellezzuale, in *Riv. dir. ind.*, 2020, I, 325. Cfr. anche G. SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, *ivi*, 2019, I, 253 ss.

<sup>3</sup> Cfr. G. SENA, *Invenzioni brevettabili e intelligenza artificiale*, in *Riv. dir. ind.*, 2020, I, 151 ss.

ritto si estrinseca nel solo diritto di essere indicato come autore dell'invenzione nella domanda o nel brevetto, diritto che può essere fatto valere, come precisa la Convenzione di Monaco, nei confronti del richiedente o del titolare del brevetto. D'altro canto il diritto morale non riveste certo nel sistema brevettuale l'importanza che assume invece nella disciplina sul *copyright*.

Nel sistema brevettuale infatti, benché gli artt. 63.2 c.p.i. e 60 EPC2000 stabiliscano che “*il diritto al brevetto spetta all'autore dell'invenzione e ai suoi aventi causa*” riconducendo così anche il diritto al brevetto ad una persona fisica, importanza determinante per la risoluzione della questione sulla titolarità dei diritti, assume la *ratio* del sistema, che si ripercuote anche sulle norme sulle invenzioni dei dipendenti (artt. 64 e 65 c.p.i.) dalle quali si desume che il diritto di esclusiva spetta a colui che ha sopportato il costo e il rischio <sup>4</sup> dell'attività di ricerca e sviluppo.

La mancata indicazione dell'inventore (o l'indicazione come inventore di una macchina) dovrebbe dunque presentare conseguenze solo nell'ambito della procedura amministrativa di concessione, portando semmai al rigetto della domanda di brevetto, dato che non è prevista l'ipotesi della nullità del brevetto, eventualmente concesso, per mancata designazione dell'inventore o per designazione come inventore di una macchina e che le cause di nullità del brevetto sono da ritenersi tassative.

Questa considerazione vale sia con riguardo alla normativa nazionale, sia con riguardo alla normativa della Convenzione di Monaco.

E vale – a mio avviso – di regola e salvo eccezioni, anche con riferimento alla norma che prevede la nullità del brevetto “*usurato*”.

Si tratta cioè di una mera irregolarità formale che potrebbe portare – come di fatto è avvenuto nel noto caso DABUS<sup>5</sup> – al rigetto della domanda di brevetto.

<sup>4</sup> Vedi sul punto G. SENA, *I diritti sulle invenzioni e sui modelli di utilità*, Milano, 2011, 172 ss.

<sup>5</sup> Sul caso DABUS, cfr. A. LUZZATI, *L'innovazione artificiale al vaglio dell'Ufficio Brevetti Europeo. Prime riflessioni sulla compatibilità del sistema brevettuale con le invenzioni dell'imminente futuro*, in *Riv. dir. ind.*, 2020, II, 256, in nota a Divisione di esame EPO, 27 gennaio 2020.

DABUS è un sistema di Intelligenza Artificiale ideato da Stephen Thaler che è in grado di creare nuove idee, analizzarle e, soprattutto, individuare idee nuove ed utili. In particolare DABUS ha creato alcune invenzioni che nulla avevano a che fare con le competenze dell'ideatore del sistema (Thaler, appunto). La società dell'inventore della macchina ha depositato due domande di brevetto volte a proteggere le invenzioni create da DABUS, inizialmente non indicando il nome dell'inventore poi, su richiesta degli Uffici, indicando come inventore il sistema di Intelligenza Artificiale al quale è stato dato appunto il nome di DABUS.

Alcuni uffici (come l'EPO, l'Ufficio UK, l'Ufficio brevetti americano) hanno ritenuto essenziale l'indicazione di una persona umana (che sola può essere titolare di diritti, mentre invece

Il rigetto della domanda normalmente ha però conseguenze fortemente negative per il richiedente (e quindi per l'impresa che ha sopportato inutilmente, o comunque anche a vantaggio dei concorrenti, il costo e il rischio economico della ricerca).

Come noto, infatti, per i primi 18 mesi decorrenti dal deposito la domanda di brevetto rimane in regime di segretezza; se dunque la decisione di rigetto venisse emessa prima del decorso dei 18 mesi, il richiedente (l'imprenditore della ricerca, che ha investito nelle nuove tecnologie produttive di nuove invenzioni) -se consentito dalla tipologia dell'invenzione- potrebbe optare per la tutela del segreto, ai sensi degli artt. 98 e 99 c.p.i. Se invece la decisione di rigetto venisse emessa – come accaduto nel caso DABUS – dopo la pubblicazione della domanda, il richiedente perderebbe ogni forma di protezione della sua invenzione essendo divenuta l'invenzione di pubblico dominio.

Ciò determinerebbe un forte disincentivo per l'impresa ad investire in sistemi di Intelligenza Artificiale, produttivi di nuove invenzioni o condurrebbe al risultato di incentivare l'espansione della tutela del segreto.

Evidentemente, il rischio del rigetto della domanda di brevetto è nella pratica superabile con l'indicazione, come inventore, di una persona fisica (appartenente alla impresa della ricerca, richiedente il brevetto) atteso che gli Uffici (in particolare l'UIBM e l'EPO) non controllano la corretta designazione dell'inventore, che, come sopra detto, può essere contestata solo dall'effettivo autore dell'invenzione nei confronti del richiedente e del titolare.

## **4. Conclusioni**

Il vero problema che pone l'Intelligenza Artificiale utilizzata per la soluzione di problemi tecnici è però forse un altro, e cioè la “definizione di persona esperta del ramo”, problema che riguarda tanto le invenzioni autonomamente generate dalla Intelligenza Artificiale, quanto le invenzioni generate dall'Intelligenza Artificiale su input dell'uomo.

Nella normativa brevettuale il legislatore fa spesso riferimento al “tecnico medio del ramo” e la costruzione di tale figura assume una importanza fondamentale soprattutto con riferimento alla validità del brevetto.

L'invenzione, infatti, per essere validamente brevettabile deve essere

---

una macchina non ha capacità giuridica) ed hanno quindi rigettato il brevetto; altri invece come l'Ufficio brevetti Sudafricano e quello Australiano (con decisione poi riformata in secondo grado), hanno concesso il relativo brevetto.

non solo “nuova”, e cioè non compresa nello stato della tecnica *ex artt.* 46 c.p.i. e 54 EPC 2000, ma deve essere anche dotata di “attività inventiva”.

Gli artt. 48 c.p.i. e 56 EPC 2000 stabiliscono che un’invenzione è considerata come implicante un’attività inventiva “*se per una persona esperta del ramo, essa non risulta in modo evidente dallo stato della tecnica*”.

Inoltre la figura del tecnico medio del ramo rappresenta il parametro per valutare la sufficiente descrizione dell’invenzione (che deve essere esposta in modo sufficientemente chiaro e completo perché una persona esperta del ramo possa attuarla).

La mancanza di altezza inventiva e l’insufficienza della descrizione (entrambe parametrata alla figura del tecnico medio) sono non solo motivi di rigetto della domanda in sede amministrativa ma addirittura le più importanti e discusse cause di nullità del brevetto.

Mi chiedo dunque come si potrà costruire “*la figura del tecnico medio del ramo*” e il bagaglio delle “*sue conoscenze*”<sup>6</sup> in caso di invenzioni che siano state generate dalla macchina con e soprattutto senza alcun apporto dell’uomo.

Questa è – io credo – la principale questione che dovrà essere affrontata e risolta dall’interprete.

---

<sup>6</sup>Per alcune interessanti riflessioni su questi temi cfr. soprattutto M. LIBERTINI, *I prodotti inventivi dell’intelligenza artificiale*, in *Intelligenza artificiale e diritto. Una rivoluzione?*, Astrid, 2022.

Emanuela Arezzo

## La tutela dei prodotti dell'IA tramite diritto d'autore e i diritti connessi

SOMMARIO: 1. Introduzione. – 2. Possono i prodotti dell'IA considerarsi opere dell'ingegno? – 3. I prodotti dell'IA e il requisito della creatività nelle opere dell'ingegno. – 4. Può l'IA considerarsi “autore”? – 5. Assenza di una giustificazione a sostegno della tesi che intende concedere alla macchina intelligente le fattispecie esclusive tipiche del diritto d'autore. – 6. Può l'inventore/autore dell'IA vantare una qualche prerogativa verso i prodotti dell'IA? e in tal caso a che titolo. – 6.1. I prodotti realizzati dall'IA e le diverse tesi che giustificano l'attribuzione dei relativi diritti all'essere umano. – 6.1.1. La dottrina maggioritaria: valorizzazione dell'apporto creativo umano nella fase di strutturazione e predisposizione dell'IA. – 6.1.2. La dottrina che valorizza l'apporto creativo dell'utente. – 7. Una proposta *de jure condendo* di regolamentazione della tutela dell'IA e dei suoi prodotti tramite il diritto d'autore e i diritti connessi.

### 1. Introduzione

C'era grande attesa alla Biennale di Venezia 2022 per il debutto di Ai-Da, cyborg pittrice creata dal gallerista Aidan Meller, che si è esibita con un'esposizione intitolata *Saltare nel Metaverso*, composta da una serie di “opere” ispirate alla Divina Commedia (da una prima installazione intitolata *Fiori sulle rive del Lete*, con fiori in 3D realizzati sulla base di schizzi prodotti da AI-DA, sino ad autoritratti con gli occhi cuciti che simboleggiano il destino degli invidiosi). AI-DA – che ha sembianze umane, ma con un braccio metallico – ha poi anche prodotto quattro ritratti dal vivo, durante la mostra stessa<sup>1</sup>.

---

<sup>1</sup>V. MAZZONI, *La Biennale di Venezia apre le porte ai Robot. Attesa la partecipazione dell'umanoide Ai-Da e le sue performance*, 4 aprile 2022, <https://insideart.eu/2022/04/04/ai-da/>; L. IPPOLITO, *Ai-Da, a Venezia la robot-artista con ritratti e opere ispirate a Dante*, 4 aprile 2022, <https://www.corriere.it/video-articoli/2022/04/04/ai-da-veneziana-robot-artista-ritratti-opere->

AI-DA è l'esempio di come oggi i sistemi di IA<sup>2</sup> abbiano raggiunto un livello di complessità e di sofisticazione tale da riuscire, grazie alle direttive impartite dal programmatore, non solo ad interagire con l'uomo, eseguendo istruzioni ovvero fornendo informazioni, bensì anche a "creare" beni che prima non esistevano e, per quanto qui ci occupa, esteriormente comparabili ad opere dell'ingegno<sup>3</sup>. Parleremo in questo caso di IA «creativa»,

---

ispirate-dante/1ef0e378-b438-11ec-a8ea-1989748a429c.shtml?&appunica=true&app\_v1=true, (entrambi consultati da ultimo il giorno 11 aprile 2022).

<sup>2</sup>Le definizioni di IA abbondano in letteratura. La più calzante pare quella suggerita dalla Commissione europea, secondo cui «Artificial intelligence (Ai) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. Ai-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or Ai can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)». Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Sull'intelligenza artificiale per l'Europa, 25 aprile 2018, n. 237, § 1, consultabile in <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF>.

<sup>3</sup>Pensiamo ad Aaron, prodotto di intelligenza artificiale creato da Harold Cohen, pittore ed esperto in computer-generated art, in grado di creare opere figurative su tela e anche disegni. Per un approfondimento consultare il sito <https://www.wired.com/2001/05/aaron-art-from-the-machine/>. Altro esempio è il progetto biennale intitolato «The Next Rembrandt», sviluppato da Microsoft in collaborazione con la società finanziaria Ing, la Delft University of Technology e due musei d'arte olandesi: Mauritshuis e Rembrandthuis. Questo team ha sviluppato una serie di algoritmi che ha permesso al programma di apprendere in modo automatico lo stile dell'artista olandese, analizzando le sue opere, e così di produrre e stampare in 3D un ritratto che rispecchia lo stile di Rembrandt. Cfr. <https://www.nextrembrandt.com/>. E ancora, prodotto derivato dall'IA paragonabile ad un'opera dell'ingegno è il «Compte de Bellamy», ritratto in stile pittorico compreso tra il XIV e il XX secolo, creato utilizzando il sistema informatico Gan, dal collettivo Obvious a Parigi. Vedi <https://obvious-art.com/portfolio/edmond-de-belamy/>. Le opere generate dall'intelligenza artificiale non si esauriscono solamente nell'arte pittorica; ed infatti possiamo individuare opere prodotte dall'IA afferenti ad altri campi artistici. Ad esempio il romanzo «The day a computer wrote a novel» scritto da un software creato nel 2015 dal Sato-Matsuzaki Laboratory, un gruppo di ricerca dell'Università di Nagoya, che ha utilizzato la generazione automatica del testo basata sulla memorizzazione di parametri strutturali individuati in oltre 1.000 racconti e saggi. Cfr. <http://kotoba.nuee.nagoya-u.ac.jp/sc/gw2015>. Nel campo della composizione musicale troviamo l'opera «Transits into an Abyss» scritta dall'intelligenza artificiale «IAMUS» che è in grado di produrre musica classica. V. <http://www.bbc.com/news/technology-20889644>. Le varie composizioni di IAMUS sono state poi eseguite dalla London Symphony Orchestra nel concerto dal titolo «Can machine be creative?» v. <https://www.youtube.com/watch?v=JOKslCT8DZU>. Possiamo annoverare anche una sceneggiatura dal titolo «Sunspring» prodotto dal software «Benjamin» in seguito diventato un cortometraggio (con il regista Oscar Shape) classificandosi tra i migliori dieci nel festival cinematografico annuale di fantascienza a Londra. V. <https://www.focus.it/cultura/arte/sunspring-cortometraggio-creato-da-Intelligenza>

proprio per distinguerla dalle più tradizionali macchine e sistemi di IA (che sono peraltro forse i più diffusi) che si propongono semplicemente di interagire con l'uomo offrendo un certo tipo di servizio (si pensi, ad esempio, a Siri, agli assistenti di acquisti virtuali, ad Alexa). Chiaramente, l'IA (chiamiamola) «non creativa» si pone come prodotto a sé stante, caratterizzato dalla tipologia di funzionalità/servizio che offre (in questo non differenziandosi da un più banale software), e non ha attratto particolare attenzione in dottrina, sembrando abbastanza lineare la sua riconduzione entro paradigmi proprietari noti. Per contro, i giuristi sono stati massimamente attratti dal tema della eventuale protezione – tramite il diritto d'autore – da tributare a quei beni intangibili prodotti dalla IA, in ragione della loro somiglianza alle creazioni intellettuali<sup>4</sup>.

La trattazione partirà dall'esame di una serie di interrogativi volti a comprendere se i prodotti della macchina IA siano o meno sussumibili all'interno del paradigma autoriale classico. Ripercorrendo le categorie del diritto d'autore e tentando di applicarle ai prodotti dell'IA, l'autore proporrà infine una soluzione di protezione alternativa per tali beni che paiono in tutto e per tutto assimilabili ad opere dell'ingegno.

## 2. Possono i prodotti dell'IA considerarsi opere dell'ingegno?

La Convenzione di Berna per la protezione delle opere letterarie e artistiche, all'art. 2, comma 1, definisce come opere dell'ingegno “[...] tutte le produzioni nel campo letterario, scientifico e artistico [...]”. L'oggetto della tutela viene, dunque, definito in luce dell'appartenenza al campo della letteratura, della scienza e dell'arte e, per voluta scelta, prescinde dal modo

---

artificiale#:~:text=Il%20cortometraggio%20di%20fantascienza%20Sunspring,e%20ha%20prodotto%20una%20sceneggiatura.

<sup>4</sup> Viceversa, il tema non sembra porsi nel caso in cui l'IA sia ascrivibile al genere delle c.d. «partly-generative machine», ossia in quei casi in cui la macchina intelligente ammonta a niente di più che un toolkit, sebbene molto sofisticato, utilizzato dall'essere umano, sotto suoi precipui input, per realizzare un'opera dell'ingegno. Così G. FROSIO, *L'IDautore inesistente: una tesi techno-giuridica contro la tutela dell'opera generata dall'intelligenza artificiale*, in *AIDA*, 2020, 54 che richiama la distinzione a sua volta fatta da R. DENICOLA, *Ex Machina: Copyright Protection for Computer-Generated Works*, in *69 Rutgers University L. Rev.* 2016, 269 ss. Ed infatti sono molti gli esempi in cui l'opera dell'ingegno viene prodotta dalla macchina (hardware o software: si pensi indifferentemente ad un programma di videoscrittura o ad una macchina fotografica), nonostante nessuno metta in dubbio che essa funga da semplice strumento che permette il dispiegarsi della creatività umana. Sul punto J.C. GINSBURG, L.A. BUDIARDJO, *Authors and Machines*, in *34 Berkeley Tech. L. J.*, 2019, 428.

o dalla forma di espressione o rappresentazione dell'opera<sup>5</sup>. Segue, immediatamente dopo, una lista di opere assai eterogenea che va dalle opere drammatiche a quelle coreografiche, ivi comprese quelle pantomimiche, le composizioni musicali e molto altro. La medesima impostazione è stata seguita dal legislatore italiano il quale ha sancito all'art. 2575 c.c. il principio (ribadito ulteriormente all'art. 1 l.a.) per cui sono protette dal diritto d'autore le opere che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia; e rimandando alla legge speciale l'enucleazione, meramente esemplificativa, delle tipologie di opere che il legislatore intende proteggere<sup>6</sup>.

Tuttavia, la dottrina più autorevole ha da sempre ritenuto canone generale della disciplina autoriale il principio per cui la protezione si appunta unicamente sulla forma espressiva, anche detta rappresentativa, dell'opera, lasciando impregiudicato il suo contenuto e le idee personali dell'autore ovvero i fatti ivi espressi<sup>7</sup>.

Il principio della c.d. dicotomia tra idea ed espressione, oggi sancito a chiare lettere all'art. 9.2 dell'accordo TRIPs e all'art. 2 WTC<sup>8</sup>, ha il pregio

<sup>5</sup>La Convenzione di Berna non fa riferimento all'elemento della creatività, specificando per contro che è rimandata alle legislazioni degli Stati aderenti la facoltà di condizionare la tutela delle opere al requisito della fissazione (la *fixation* tipica degli ordinamenti anglosassoni) su un supporto materiale (art. 2, n. 2). Sul punto v. *infra* § 2.

<sup>6</sup>Sulla valenza meramente esemplificativa, nel nostro ordinamento, dell'elencazione ivi contenuta, per tutti, v. G. GHIDINI, *Profili evolutivi del diritto industriale, Innovazione – Creatività – Informazione, Dinamiche conflittuali, esperienze di condivisione*, 3<sup>a</sup> ed., Giuffrè, Milano, 2015, 205 ss. Così non è, per contro, nel sistema anglosassone dove la lista di opere dell'ingegno enucleate alla section 1, comma 1 del Copyright, Designs and Patents Act del 1988 ha carattere esaustivo. Diffusamente sull'argomento v. W. CORNISH, D. LLEWELYN, T. APLIN, *Intellectual Property: Patents, Copyright, Trademarks and Allied Rights*, 9<sup>a</sup> ed., Sweet & Maxwell, London, 2019, 439 ss.

<sup>7</sup>Sul punto v. MUSSO, per il quale oggetto del diritto d'autore è l'opera nella sua forma espressiva o rappresentativa. V. A. MUSSO, *Diritto d'autore sulle opere dell'ingegno letterarie e artistiche, Art. 2575-2583 c.c.*, *Commentario del Codice Civile Scialoja-Branca*, Zanichelli, Bologna, 2008, 13; M. BERTANI, *Diritto d'autore europeo*, in *Quaderni di AIDA*, Giappichelli, Torino, 2011, 107, secondo il quale l'accesso alla tutela sarebbe consentito "ai soli esiti creativi *esteriorizzati*, in quanto trasfusi in un artefatto culturale separato dalla persona dell'autore" (corsivo mio). Analogamente, per AUTERI il diritto d'autore consente di proteggere l'opera solo "in quanto rappresentazione della realtà o espressione di opinioni, idee e sentimenti", P. AUTERI in *Diritto Industriale, proprietà intellettuale e concorrenza*, 6<sup>a</sup> ed., Giappichelli, Torino, 2020, 635.

<sup>8</sup>Appare tuttavia assai singolare che nonostante, si diceva, il principio della dicotomia tra espressione/idea (che nelle norme internazionali estende il divieto ai procedimenti, ai metodi di funzionamento o ai concetti matematici in quanto tali) sia pienamente riconosciuto dalla dottrina come principio ordinatore della materia, nella legislazione nazionale esso ha trovato esplicita codificazione solo con riferimento a determinate categorie di opere (segnatamente: i programmi

chiarire qual è l'oggetto della protezione autoriale, da intendersi come l'*espressione*, la *rappresentazione* di una certa idea suggellata in una determinata *forma*<sup>9</sup>. Un assunto, quest'ultimo, oggi accolto anche dalla giurisprudenza europea allorquando ribadisce che la creazione intellettuale deve vestirsi di una precipua forma espressiva, che la renda identificabile "con sufficiente precisione e obiettività"<sup>10</sup>, potendo la qualificazione di opera dell'ingegno tributarsi unicamente "[...] agli elementi che sono espressione di una siffatta creazione intellettuale"<sup>11</sup>.

Tornando al tema di questo studio, da un punto di vista meramente ontologico sembrerebbe che i prodotti dell'IA possano certamente rientrare

---

per elaboratore elettronico e le banche di dati). Diffusamente in argomento v. G. DORE, *Plagio e diritto d'autore, un'analisi comparata e interdisciplinare*, Wolters Kluwer-Cedam, Milano, 2021, 50 ss.

<sup>9</sup>Sul punto, per tutti, V. M. DE SANCTIS, *Il diritto di autore, Del diritto di autore sulle opere dell'ingegno letterarie e artistiche*, artt. 2575-2583, in *Il cod. civ. comm.*, a cura di P. Schlesinger, F.D. Busnelli, Giuffrè, Milano, 2012, 30, secondo cui il carattere creativo quale requisito di proteggibilità va necessariamente riferito «... alla *forma rappresentativa* che tutte le opere dell'ingegno possiedono e comunque devono possedere», essendo esse «... comunicazioni di informazioni circa il pensiero in proposito del loro autore».

<sup>10</sup>Cfr. CGUE, 13 novembre 2018, in causa C-310/17, *Levola Hengelo c. Smilde Foods BV*, (in seguito per brevità, *Levola*, C-310/17), § 40. Confermata poi anche da: CGUE 12 settembre 2019, in causa C-683/17, *Cofemel – Sociedade de Vestuário SA c. G-Star Raw CV*, (in seguito per brevità, *Cofemel*, C-683/17), §§ 29, 32-33. Interessante notare che la necessità di circoscrivere in maniera «precisa e obiettiva» quale sia «l'espressione oggetto della tutela» autoriale – che riporta immediatamente alla memoria l'appena citato art. 7 c.p.i. – è stata espressamente ricondotta dalla Corte vuoi all'esigenza di assicurare un più efficace *enforcement* dei diritti – consentendo alle autorità preposte a garantirne la tutela una più immediata identificazione della creazione intellettuale protetta – vuoi alla necessità di tutti gli individui (ivi compresi in particolar modo gli operatori economici) di poter individuare con precisione «[...] what is the subject matter of protection which third parties, especially competitors, enjoy» (*Levola*, C-310/17, § 41). *Razionale*, quest'ultimo, che ugualmente ricorda il contemporaneo di interessi suggellato all'art. 52, comma 3, c.p.i. dove il legislatore italiano (in ossequio a quanto disposto dall'art. 1 del Protocollo interpretativo dell'art. 69 della Convenzione sul Brevetto Europeo) impone che l'interpretazione del brevetto garantisca al contempo un'equa protezione al suo titolare ed una ragionevole sicurezza giuridica ai terzi. Sia consentito rinviare sul punto a E. AREZZO, *Ambito di estensione della protezione brevettuale e titolarità dei diritti*, in *Proprietà Intellettuale – Segni distintivi, brevetti, diritto d'autore*, a cura di G. Olivieri, A. Genovese, Utet Giuridica, Torino, 2021, 513.

<sup>11</sup>V. *Levola*, C-310/17, § 37. Si noti, peraltro, come la circostanza che l'opera prenda una forma espressiva che la renda percepibile e identificabile con un sufficiente grado di precisione non implica che tale forma sia parimenti permanente, e dunque fissata su di un supporto tangibile (*Levola*, C-310/17, § 40). Ed invero, solo per taluni tipi di opere il supporto permane parte integrante dell'opera stessa. Su questo tema v. F. BENATTI, *Diritto d'autore e supporto dell'opera*, in *Quaderni di AIDA*, n. 30, Giappichelli, Torino, 2020, 84 ss., che esplora il ruolo del supporto quale elemento fondante dell'opera con particolare riferimento al fenomeno della *Street Art*.

nel *genus* delle opere dell'ingegno, dal momento che solitamente prendono le sembianze di creazioni intellettuali che per un verso appartengono a quei campi dell'arte e della cultura tradizionalmente protetti dal diritto d'autore e, per altro verso, sono inconfutabilmente dotate di forma rappresentativa: si pensi nuovamente ai dipinti di Aaron o ai ritratti di AI-DA. Ed invero, in molti hanno sottolineato l'impossibilità di distinguere, all'atto pratico, l'opera realizzata dall'autore umano rispetto a quella realizzata dalla macchina intelligente<sup>12</sup>.

Il quadro, tuttavia, non è completo. Le legislazioni dei Paesi aderenti richiedono espressamente che l'opera dell'ingegno proteggibile dal diritto d'autore sia altresì dotata di carattere creativo (ovvero dell'originalità, negli ordinamenti anglosassoni) e rappresenti il frutto del lavoro intellettuale del suo autore<sup>13</sup>: elementi, questi ultimi, che spesso nell'analisi sia della dottrina, sia della giurisprudenza, tendono a sovrapporsi con la nozione stessa di opera proteggibile, quasi a diventare sfumature di un concetto unitario<sup>14</sup>.

### 3. I prodotti dell'IA e il requisito della creatività nelle opere dell'ingegno

Nell'ordinamento italiano i beni intangibili proteggibili per il tramite del diritto d'autore sono quelli che appartengono alla letteratura, alla mu-

---

<sup>12</sup> Così R. DENICOLA, *Ex Machina: Copyright Protection for Computer-Generated Works*, cit., *supra* nota 4, 2016, 272; R. YU, *The Machine Author: What Level Of Copyright Protection Is Appropriate For Fully Independent Computer-Generated Works?*, in *University of Pennsylvania Law Review* 165, 2017, 1257; J.C. GINSBURG, L.A. BUDIARDJO, *Authors and Machines*, cit., *supra* nota 4, 2019, 401 ss.

<sup>13</sup> Cfr. artt. 2575 c.c. e 1, comma 1, l.a. con riferimento al requisito della creatività e artt. 2576 c.c. e 6 l.a. ove si specifica che la fattispecie costitutiva del diritto è data dalla creazione dell'opera «quale particolare espressione del lavoro intellettuale».

<sup>14</sup> Cfr. in dottrina Fabiani, per il quale i requisiti dell'opera dell'ingegno "... perché possa costituire oggetto del diritto d'autore, sono, *oltre che il carattere creativo*, l'appartenenza ad uno dei campi dell'arte e della cultura [...] e la concretezza di espressione". M. FABIANI, *Diritto d'autore e diritti degli artisti interpreti o esecutori*, Giuffrè, Milano, 2004, 39. Per DE SANCTIS, il carattere creativo è il requisito che le opere dell'ingegno debbono possedere insieme alla forma espressiva "nella quale la creatività si deve estrinsecare" (per essere protette ai sensi dell'art. 2575 c.c.). V. M. DE SANCTIS, *Il diritto di autore, Del diritto di autore sulle opere dell'ingegno letterarie e artistiche*, artt. 2575-2583, cit. *supra* nota 9, 2012, 31. Analogamente AUTERI, secondo il quale la definizione di opera dell'ingegno protetta dal diritto d'autore permette anche di chiarire il significato del requisito del carattere creativo che l'opera deve possedere per meritare la protezione autoriale. P. AUTERI, in *Diritto Industriale, proprietà intellettuale e concorrenza*, cit. *supra* nota 7, 2020, 639.

sica, alle arti figurative, all'architettura, al teatro ed alla cinematografia (e in particolare quelle che, nello specifico, prendono le sembianze di una delle opere elencate all'art. 2 l.a.), in qualunque modo o forma espressi, e a condizione che siano dotati di carattere creativo<sup>15</sup>.

Il requisito della creatività nel diritto d'autore italiano è stato storicamente inteso come espressione del lavoro intellettuale dell'uomo<sup>16</sup>. L'opera deve essere il risultato dell'attività intellettuale dell'autore, cui spettano i diritti esclusivi in ragione dell'atto creativo (art. 2576 c.c.)<sup>17</sup>, e deve ulteriormente riflettere la sua personale impronta<sup>18</sup>. In questo senso parlandosi anche di creatività intesa come originalità o individualità dell'opera<sup>19</sup>.

---

<sup>15</sup> La legge italiana – che più dettagliatamente descrive le forme artistiche, menzionando il teatro, la cinematografia, l'architettura – aggiunge l'elemento della creatività. Le opere protette dalla legge sul diritto d'autore, recita l'art. 1 l.a. (che riprende l'art. 2575 c.c.) sono quelle dotate di carattere creativo.

<sup>16</sup> Cfr. art. 2576 c.c. e art. 6 l.a. In questo senso G. OPPO, *Creazione ed esclusiva nel diritto industriale*, in *Riv. dir. comm.*, 5-6, 1964, 191. Più di recente MUSSO, per il quale l'art. 2576 c.c., con il suo riferimento alla creazione dell'opera quale "particolare espressione del lavoro intellettuale" costituirebbe un indissolubile cerniera tra l'elemento della creazione personale dell'opera dell'ingegno da parte del suo autore, di cui all'art. 2575 c.c., ed il titolo di acquisto (originario) del diritto in capo al soggetto autore, ex art. 2580 c.c. (in ragione della creazione), A. MUSSO, *Diritto d'autore sulle opere dell'ingegno letterarie e artistiche*, cit., *supra* nota 7, 2008, 126.

<sup>17</sup> Poiché ogni ideazione proviene, per definizione, da un atto creativo del suo autore del quale reca l'impronta, essa sarà soggettivamente nuova nel senso di differente rispetto a tutte le altre opere dell'ingegno esistenti (diversità che, ovviamente, si rapporta alla differente maniera di espressione e non all'oggetto di tale rappresentazione che può ben essere noto alla collettività). Così P. AUTERI, *Diritto Industriale, proprietà intellettuale e concorrenza*, cit. *supra* nota 7, 2020, 497). In questa accezione, la novità soggettiva rappresenta un profilo importante che connota il (più ampio) requisito della creatività. Così: M. ARE, *L'oggetto del diritto di autore*, Giuffrè, Milano, 1963, 52. Appare a tutt'oggi controversa, invece, l'idea che la tutela autoriale richieda altresì prova della c.d. novità oggettiva dell'opera, come riteneva un tempo autorevole dottrina, in particolare: M. ARE, *op. cit.*, 53; T. ASCARELLI, *Teoria della concorrenza e dei beni immateriali*, Giuffrè, Milano, 1960, 705; P. GRECO, P. VERCELLONE, *I diritti sulle opere dell'ingegno*, Utet Giuridica, Torino, 1974, 47 ss. Oggi sembra propendere per questa tesi M. BERTANI, *Diritto d'autore europeo*, cit. *supra* nota 7, 2011, 126 ss., per il quale siffatta concezione del requisito della creatività avrebbe il pregio di risolvere situazioni problematiche, quali il caso degli incontri fortuiti, ripristinando un maggior livello di certezza del diritto.

<sup>18</sup> Sul punto v. VITT. M. DE SANCTIS, *Il carattere creativo delle opere dell'ingegno*, Giuffrè, Milano, 1971, 38, per il quale il requisito si considera soddisfatto lì dove la creazione rappresenti «il "riflesso" della personalità stessa dell'autore in quanto è la immagine dei tratti caratteristici di quest'ultimo in un determinato momento e in una determinata direzione sedimentati in un quid oggettivo che cristallizza in un certo senso la configurazione dinamica dell'individuo». Analogamente sul punto, ancor prima, STOLFI, *Il diritto d'autore*, Società Editrice Libreria, 1932, 518 ss.

<sup>19</sup> Così P. AUTERI, in *Diritto Industriale, proprietà intellettuale e concorrenza*, cit. *supra* nota 7, 2020, 639. Si tratta, dunque, di una sfumatura concettuale che si differenzia dalla nozione

Questa seconda sfumatura del concetto di creatività sembra essere stata accolta dal legislatore eurounitario che lo ha declinato per l'appunto secondo il parametro dell'"author's own intellectual creation" (parlando specificamente di originalità, con riferimento a software, banche dati<sup>20</sup> e fotografie)<sup>21</sup>. Parametro poi accolto anche dalla giurisprudenza europea che, a partire dalla ben nota pronuncia *Infopaq*, si è proposta di estendere il requisito della originalità intesa quale "risultato della creazione intellettuale dell'autore" a tutte le tipologie di creazioni<sup>22</sup> intellettuali<sup>23</sup>.

---

anglosassone di originalità in cui il termine viene inteso come sinonimo di provenienza, origine dell'opera da parte del suo autore: nozione che porta a ritenere soddisfatto il requisito ogniqualvolta la creazione sia riconducibile ad un certo autore, il quale l'abbia concepita in via del tutto indipendente (*leggi*: senza copiare). Impianto che, a sua volta, porta a giustificare la dottrina della c.d. *independent creation*, sulla scorta della quale creazioni financo identiche non saranno considerate contraffattorie là dove gli autori (*recte*: il secondo autore) siano in grado di dimostrare di averle concepite in maniera autonoma. Per tutti v. M.A. LEAFFER, *Understanding Copyright Law*, 2004, 59 e 408.

<sup>20</sup> Definiti da P. FRASSI "creazioni utili" per evidenziare la loro connotazione tipicamente funzionale. V. P.A.E. FRASSI, *Creazioni utili e diritto d'autore, Programmi per elaboratore e raccolte di dati*, Giuffrè, Milano, 1997.

<sup>21</sup> Cfr. art. 1, comma 3, direttiva 2009/24/Ce, del Parlamento europeo e del Consiglio del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore, in G.U. L. 111 del 5 maggio 2009; art. 3, comma 1, direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, in G.U. L. 077 del 27 marzo 1996; art. 6, direttiva 2006/116/Ce del Parlamento europeo e del Consiglio del 12 dicembre 2006, concernente la durata di protezione del diritto d'autore e di alcuni diritti connessi, in G.U. L. 372 del 27 dicembre 2006, p. 12 (con riferimento alle opere fotografiche). V. da ultimo anche l'art. 14 direttiva (UE) 2019/790 del Parlamento Europeo e del Consiglio del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale che modifica le direttive 96/9/CE e 2001/29/CE in CDSM Directive, in G.U. L. 130 del 17 maggio 2019, 82, (con riferimento alle opere delle arti visive di dominio pubblico).

<sup>22</sup> Cfr. CGUE 16 luglio 2009, in causa C-5/08, *Infopaq International c. Danske Dagblades Forening*, in *Racc.*, pag. I-6569, § 37.

<sup>23</sup> Sul punto A. KUR, T. DREIER, *European Intellectual Property Law – Text, Cases & Materials*, Edward Elgar Publishing, Cheltenham, 2013, 291 ss., notando in proposito come la CGUE abbia così ceduto alla tentazione di colmare quei vuoti normativi ancora largamente presenti nel panorama del diritto d'autore europeo. Ed invero, come opportunamente notato dalla dottrina antecedente ad *Infopaq*, l'introduzione di una specifica nozione di originalità solo per taluni beni intellettuali, seppur ampiamente giustificata da una forte esigenza di armonizzazione circa il trattamento (e forse ancor prima di riconoscimento della tutela) tributato a taluni tipi di opere, portava con sé il rischio di rompere l'unità del sistema (così R. CASAS VALLES, *The requirement of originality*, in *Research Handbook on the Future of EU Copyright*, a cura di E. Derclaye, Edward Elgar Publishing, Cheltenham, 2009, 103 e 132). L'arresto della Corte in *Infopaq* va dunque inquadrato come un primo e importante riconoscimento da parte della Corte della necessità di adottare un unico concetto di originalità (unitamente, si vedrà, ad un'unica nozione di opera dell'ingegno) valido in tutti i Paesi dell'UE e trasversale a tutte le diverse tipologie di opere dell'ingegno (cfr. P. FABBIO, *Opere protette e requisiti di tutela nel diritto d'autore*

Ne è così scaturito un arresto giurisprudenziale che, partendo dall'elemento della creazione intellettuale dell'autore intesa come riflesso del suo spirito creativo, ha gradualmente sviluppato la nozione di creatività intorno al parametro della libertà di scelta, disposizione e combinazione degli elementi che vanno a comporre la forma rappresentativa dell'opera<sup>24</sup>, ergendolo a canone generale dell'intera disciplina autoriale<sup>25</sup>. In questa prospettiva, ha chiarito la Corte, l'elemento della creatività è da escludersi tutte le volte in cui l'autore si trovi ad essere per un qualsivoglia motivo costretto entro specifici parametri o regole, il cui rispetto gli impone una certa via, privandolo di discrezionalità<sup>26</sup>.

---

UE, in *AIDA*, 2016, 293 ss.), sebbene sia impossibile dimenticare che la nozione di creazione intellettuale propria del suo autore avesse, in realtà, sfumature assai eterogenee all'interno delle tre direttive in cui fu inizialmente introdotta. Sul punto Q.R.N. RAMALHO, *Originality redux: an analysis of the originality requirement in AI-generated works*, in *AIDA*, 2018, 26 ss.; E. ROSATI, *Originality in EU Copyright*, Edward Elgar Publishing, Cheltenham, 2013, 63. M. VAN ECHOUD, P.B. HUGENHOLTZ, S. VAN GOMPEL, L. GUIBAULT, N. HELBERGER, *Harmonizing European Copyright Law. The Challenges of better law making*, Kluwer Law International, 2009, 41.

<sup>24</sup> Si ricordi, peraltro, come anche siffatta concezione di creatività, riferita alla precipua scelta e disposizione di materiale (anche di per sé costituito da elementi non proteggibili) è stata per introdotta con riferimento alla disciplina delle banche dati creative (art. 3, direttiva 96/9), trovando il suo antecedente nella tutela delle opere collettive (v. art. 3 l.a.).

<sup>25</sup> Si ricordi, invero, che in *Infopaq* la questione concerneva la tutelabilità a mezzo di diritto d'autore di frammenti di opera estremamente esigui (ossia estratti di ben undici parole). La Corte si pronunciava nel senso della proteggibilità di tali estratti là dove mediante la scelta, la disposizione e la combinazione di semplici parole, ancorché singolarmente non tutelabili, l'autore fosse in grado di esprimere il suo spirito creativo in maniera originale, ottenendo un risultato che costituisse una creazione intellettuale. *Infopaq*, C-5/08, cit., § 45. Il principio per cui il diritto d'autore si applica ogni qualvolta l'opera "[...] costituisca una creazione intellettuale dell'autore che ne riflette la personalità e si manifesta attraverso le scelte libere e creative di quest'ultimo [...]" è stato riaffermato poi dalla Corte in molti altri casi successivi. Cfr. CGUE, 12 settembre 2019, in causa C-683/17, *Cofemel – Sociedade de Vestuário SA c. G-Star Raw CV*; CGUE, 13 novembre 2018, in causa C-310/17, *Levola Hengelo c. Smilde Foods BV*, (in seguito per brevità, CGUE, C-310/17); CGUE, 7 agosto 2018, in causa C-161/17, *Land Nordrhein-Westfalen c. Dirk Renckhoff*; CGUE, 1 marzo 2012, in causa C-604/10, *Football Dataco e altri c. Yahoo! UK Ltd e altri*; CGUE, 1° dicembre 2011, in causa C-145/10, *Eva-Maria Painer c. Standard VerlagsGmbH e altri*; CGUE 4 ottobre 2011, nelle cause riunite C-403/08 e C-429/08, *Joined Cases Football Association Premier League Ltd e altri c. QC Leisure e altri, e Karen Murphy c Media Protection Services Ltd*, (in seguito per brevità: *Football Association Premier League*, C-403/08 e C-429/08), § 97.

<sup>26</sup> Come nel caso degli incontri sportivi, per i quali la Corte ha escluso la tutelabilità a mezzo di diritto d'autore (si noti: pur lasciando aperta la via dei diritti connessi), ritenendo che questi ultimi «[...] non possono essere considerati quali creazioni intellettuali qualificabili come opere ai sensi della direttiva sul diritto d'autore [...]» in quanto «disciplinati dalle regole del gioco, che non lasciano margine per la libertà creativa ai sensi del diritto d'autore». Cfr. CGUE, *Football Association Premier League*, nelle cause C-403/08 e C-429/08, cit., § 98. E dunque riconducendo l'impossibilità di rientrare nella categoria delle opere protette da diritto d'autore all'a-

Alla luce del quadro così delineato, e abbracciando la nozione di creatività intesa come frutto di scelte libere e individuali dell'autore, attraverso cui questi imprime all'opera la sua personale impronta, e ancora, di riflesso, come assenza di un qualunque condizionamento che possa dettare in qualche modo la via all'autore, riconducendolo all'interno di binari precostituiti, diversi autori hanno ritenuto di escludere che la macchina sia in grado di "creare" alla stessa maniera in cui farebbe un autore umano, e questo per due ordini di ragioni. In primo luogo, perché la macchina non sarebbe in grado di scegliere tra un numero infinito di possibilità, seppure enormemente vasto per la mente umana<sup>27</sup>. La macchina intelligente, invece, anche quella basata sulle più sofisticate tecniche di *machine learning*, dove il livello di autonomia decisionale è tale da rendere imprevedibile il risultato creativo cui perverrà, si muove sempre lungo il binario predefinito dall'autore e creerà sempre secondo il criterio e seguendo i parametri

---

senza del requisito della creatività. Sull'elemento della creatività inteso come anche sinonimo di discrezionalità v. M. BERTANI, *Diritto d'autore europeo*, cit. *supra* nota 7, 2011, 122, per il quale la protezione di diritto d'autore sarebbe riservata unicamente alle opere dell'ingegno che possiedono il requisito, normativamente previsto, dell'idoneità dell'opera a denotare carattere creativo e, allo stesso tempo, l'elemento della discrezionalità, descritta come la circostanza che le forme non siano «necessitate» rispetto al contenuto ideativo o informativo che debbono esprimere. Sul punto v. anche CASAS VALLES per il quale il requisito della creatività comprende vuoi la sfumatura della provenienza dell'opera dal suo autore, vuoi soprattutto quella di risultare dalla libertà di scelta tra diverse forme espressive possibili. Cfr. R. CASAS VALLES, *The requirement of originality*, in *Research Handbook on the Future of EU Copyright*, a cura di E. Derclaye, Edward Elgar Publishing, Cheltenham, 2009, 113.

<sup>27</sup> In tal senso v. G. ROSSI, *L'intelligenza artificiale e la definizione di opera dell'ingegno*, in *AIDA*, 2018, 275, 276, secondo il quale «il risultato nuovo ed originale non rappresenta affatto un esito della creatività del sistema, ma semplicemente del fatto che questo ha dato applicazione all'algoritmo». S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – The Human-Like Authors are Already Here – A New Model*, in *Mich. St. L. Rev.*, 2017, 691, per il quale la legislazione attuale sul diritto d'autore non è in grado di abbracciare il tipo di produzione e creatività espresso dall'IA. A conclusioni analoghe giungono anche altri autori secondo i quali alcune IA, in particolare quelle basate sui meccanismi di deep learning, sarebbero sì capaci di compiere innumerevoli scelte in totale autonomia; ciononostante, il risultato cui pervengono non sarebbe originale nell'accezione richiesta dal diritto d'autore. Cfr. K. HRISTOV, *Artificial Intelligence and the Copyright Dilemma*, in 57 *IDEA*, 3, 2017, 436 ss.; D.J. GERVAIS, *The Machine as Author*, in 105 *Iowa L. Rev.*, 2019/1, 52, per il quale tali beni sarebbero destinati a cadere nel public domain. Una posizione intermedia è sostenuta da BRIDY, la quale pur ritenendo impensabile attribuire alla macchina la titolarità dei diritti sui beni intangibili prodotti, ritiene impossibile negare natura creativa alle opere prodotte dall'IA. V. BRIDY, *Coding Creativity: Copyright and the Artificially Intelligent Author*, in 5 *Stan. Tech. L. Rev.* 1, 2012, 26. Si spinge in là F. BANTERLE, *Ownership of inventions created by Artificial Intelligence*, in *AIDA*, 2018, 71, per il quale le macchine di IA sarebbero capaci di esprimere scelte creative in via del tutto autonoma e le loro creazioni sarebbero, dunque, opere dell'ingegno da proteggere con il copyright.

con cui è stato impostato il suo arricchimento informativo<sup>28</sup>. Aaron, ad esempio, sarà certamente in grado di dipingere un quadro raffigurante un soggetto che Cohen non aveva immaginato, ma lo ritrarrà sempre seguendo lo stile ed il tocco dell'autore. Analogamente, il New Rembrandt Project produrrà una innumerevole serie di nuovi dipinti, tutti in perfetto stile Rembrandt. In secondo luogo, diversamente dall'essere umano l'apparato programmato, per quanto intelligente, non sarebbe in grado di riflettere una sua personalità<sup>29</sup> (che non possiede) ed imprimere il suo tocco nelle opere prodotte<sup>30</sup> (trasmetterebbe, semmai, i tratti tipici delle creazioni di cui si compone il dataset sul quale è stato addestrato)<sup>31</sup>.

Di conseguenza, pur prendendo le sembianze di beni che appaiono in

---

<sup>28</sup> Cfr. A. RAMALHO, *Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems*, in *Journal of Internet Law*, 2017/1, 3 ss., che individua l'assenza di capacità creativa della macchina intelligente nella sua mancanza di immaginazione, affermando che l'IA può rappresentare solo ciò che le è stato impartito attraverso un insieme di regole astratte individuate dal programmatore, non essendo il software capace di modificare lo stile delle creazioni che andrà a comporre se non appositamente riprogrammato dall'uomo. Considerazioni analoghe sono state espresse da G. ROSSI, *L'intelligenza artificiale e la definizione di opera dell'ingegno*, cit. *supra* nota 27, 2018, 276, per il quale nemmeno la più sofisticata macchina capace di auto-apprendere potrebbe dirsi capace di creare, poiché «il suo agire sarà sempre delimitato, in modo invalicabile, dalla base dati di partenza e dall'algoritmo». Così anche J.C. GINSBURG, L.A. BUDIARDJO, *Authors and Machines*, cit., *supra* nota 4, 2019, 402 ss. Sul punto v. anche le riflessioni di D.L. BURK, *Thirty-Six Views of Copyright Authorship, by Jackson Pollock*, in *58 Hous. L. Rev.*, 2020, 263 e 266, secondo cui i prodotti dell'IA, quand'anche rappresentino creazioni uniche e completamente imprevedibili, sono sempre il risultato diretto del procedimento attuato dalla macchina che ovviamente è il frutto del lavoro intellettuale dell'uomo.

<sup>29</sup> Con riferimento al tema dell'IA v. F. ROSSI, *L'intelligenza artificiale e la definizione di opera dell'ingegno*, cit., *supra* nota 27, 2018, 275, il quale evoca un nesso di causalità tra autore e opera. Analogamente D.J. GERVAIS, *The Machine as Author*, cit., *supra* nota 27, 2019, 52, parla di "causation of originality". V. anche G. FROSIO, *L'(I)Autore inesistente: una tesi tecnologica contro la tutela dell'opera generata dall'intelligenza artificiale*, cit., *supra* nota 4, 2020, 74 il quale rileva che per permettere la protezione autoriale della "creatività algoritmica" si dovrebbe mutare l'interpretazione soggettiva e antropocentrica esistente nella nozione di originalità, sostituendola con un approccio formale e oggettivo.

<sup>30</sup> Così A. MUSSO, *Diritto d'autore sulle opere dell'ingegno letterarie e artistiche*, cit., *supra* nota 7, 2008, 126 ss., per il quale l'elemento della creatività quale espressione del lavoro intellettuale dell'autore deve necessariamente manifestarsi sotto forma di personale impronta di costui nell'opera dell'ingegno: impronta che verrebbe completamente a mancare nel caso dell'intelligenza artificiale, dove l'atto creativo verrebbe integralmente delegato a programmi, ancorché molto sofisticati.

<sup>31</sup> Su questo punto concorda anche G. SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, in *Riv. dir. ind.*, 1, 2019, 270 ss. Cfr. anche M. ANTIKAINEN, *Copyright Protection and AI-Generated Works – A Fight We Have Already Lost?*, in *AIDA*, 2018, 257, il quale dubita che un sistema di IA possa possedere una sua personalità ovvero più banalmente, sia in grado di compiere scelte che possano dirsi genuinamente libere e creative.

tutto e per tutto assimilabili alle opere dell'ingegno, non è chiaro se nel caso di prodotti dell'IA il requisito della creatività possa ritenersi integrato.

#### 4. Può l'IA considerarsi "autore"?

Le riflessioni da ultimo formulate inducono a chiedersi se il requisito della creatività dell'opera, così come da ultimo tratteggiato dalla Corte di Giustizia, presupponga o meno, quale suo corollario, la circostanza che l'opera proteggitibile sia necessariamente e unicamente quella creata da un essere umano<sup>32</sup>.

A ben vedere, se sussistono certamente in materia situazioni in cui l'ordinamento ammette la nascita dei diritti (si badi, patrimoniali!) in capo a persone giuridiche<sup>33</sup> ovvero a soggetti diversi dall'autore<sup>34</sup>, l'architettura

---

<sup>32</sup> Va certamente in questa direzione la prassi del Copyright Office nord-americano che ha rifiutato la registrazione di opere il cui autore risultasse essere una macchina e ha suggellato tale principio in apposite "Best Practices", ove spiega che "[...] the Office will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author [...]". Cfr. Copyrightable Authorship: What Can Be Registered U.S. Copyright Office, Compendium of U.S Copyright Office Practices, 3<sup>a</sup> ed., 2021, § 300, § 313.2., consultabile all'indirizzo <https://copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf>. Ancora, alla sezione 306 (intitolata "The Human Authorship Requirement"), specificava che "[...] Copyright Office will register an original work of authorship, provided that the work was created by a human being. The copyright law only protects "the fruits of intellectual labor" that "are founded in the creative powers of the mind" Trade-Mark Cases, 100 U.S. 82, 94 (1879), cfr. <https://supreme.justia.com/cases/federal/us/100/82/>. Because copyright law is limited to "original intellectual conceptions of the author," the Office will refuse to register a claim if it determines that a human being did not create the work."

<sup>33</sup> Cfr. art. 3, direttiva 2009/24/Ce del Parlamento europeo e del Consiglio del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore, in G.U. L. 111 del 5 maggio 2009, 16 ss., ove si specifica che "La tutela è riconosciuta a tutte le persone fisiche o giuridiche aventi i requisiti previsti dalla legislazione nazionale sul diritto di autore applicata alle opere letterarie". La medesima direttiva, all'art. 2, comma 3, prevede l'attribuzione di tutti i diritti economici sul programma creato dal dipendente ("nell'esecuzione delle sue mansioni o su istruzioni del suo datore di lavoro") al datore di lavoro (che, si badi, ben potrebbe essere una persona giuridica). La disposizione è stata recepita all'art. 12 *bis* della legge italiana sul diritto d'autore che l'ha poi estesa anche alle banche di dati, nonostante la rispettiva direttiva non avesse suggellato *expressis verbis* un analogo principio (un rimando era, tuttavia, contenuto al considerando n. 29). Sul punto F. GIOIA, *I soggetti dei diritti*, in *AIDA*, 2002, 80 ss. Ed invero taluna dottrina riterrebbe il principio applicabile a tutte le creazioni intellettuali concepite dal lavoratore dipendente, allorquando egli crei l'opera durante lo svolgimento delle proprie mansioni lavorative ovvero sulla scorta delle istruzioni impartite dal datore di lavoro. V. L.C. UBERTAZZI, *I diritti d'autore e connessi*, nei *Quaderni di AIDA*, Giuffrè, Milano, 2003, 41 ss.; M. BERTANI, *Diritto d'autore europeo*, cit., *supra* nota 7, 2011, 86 ss., in particolare 89.

<sup>34</sup> La dottrina maggioritaria ritiene che nel caso di opera su commessa, ove oggetto del contratto sia precipuamente l'attività creativa, i diritti patrimoniali vengono acquistati a titolo deri-

del diritto d'autore italiano ed eurounitario sembrano presupporre che la creazione proteggibile sia per l'appunto quella creata dall'essere umano<sup>35</sup>. Basti pensare al termine di durata della protezione, il cui computo tipicamente decorre a partire dalla morte dell'autore (art. 25 l.a.), e ai diritti morali, che si giustificano alla luce di un profondo legame tra creatore e opera, che di quest'ultimo riflette il personalissimo tratto creativo<sup>36</sup>. Ed è cer-

---

vativo dal committente. Cfr. VITT. M. DE SANCTIS, *Il carattere creativo dell'opera dell'ingegno*, cit., *supra* nota 18, 1971, 164.

<sup>35</sup> Sul punto M. BERTANI, *Diritto d'autore europeo*, cit., *supra* nota 7, 2011, 75, secondo il quale l'appartenenza originaria dei diritti d'autore può spettare unicamente a persone fisiche, presupponendo un atto di creatività intellettuale che altri soggetti (es. le persone giuridiche) non sono in grado di compiere. Analogamente V. FALCE, *La modernizzazione del diritto d'autore*, Giappichelli, Torino, 2012, 79; A. MUSSO, *L'impatto dell'ambiente digitale su modelli e categorie dei diritti d'autore e connessi*, in *Riv. trim. dir. e proc. civ.*, 2018/I, 503, per il quale la personalità fisica dell'autore permane quale requisito imprescindibile di protezione. Come già espresso in A. MUSSO, *Diritto d'autore sulle opere dell'ingegno letterarie e artistiche*, cit., *supra* nota 7, 2008, 126, ove l'Autore spiega che il carattere di creazione personale dell'opera dell'ingegno da parte del suo autore, conformemente alla natura personale e "spirituale" dell'istituto negli ordinamenti continentali, impedisce l'attribuzione (perlomeno a titolo originario) del diritto d'autore alle persone giuridiche e ad eventuali entità artificiali. Sul punto v. anche E. ROSATI, *Originality in EU Copyright*, Edward Elgar Publishing, Cheltenham, 2013, 57 ss., la quale pur cogliendo i limiti connessi alla nozione di antropocentrica *authorship*, conclude tuttavia che là dove essa venisse espunta dalla disciplina autoriale, quest'ultima si trasformerebbe in una mera protezione dell'investimento lavorativo, con la conseguenza che il diritto si tramuterebbe in una mera pretesa compensatoria per lo sforzo intellettuale profuso. E ancora A. RAMALHO, *Intellectual Property Protection for AI-generated Creations. Europe, The United States, Australia and Japan*, Routledge, 2021, 30 ss.; J. PILA, P. TORREMANS, *European Intellectual Property Law*, 2ª ed., Oxford University Press, Oxford, 2019, 249, definendo le opere protette dal diritto d'autore "... intangible expressions of a person meriting the title 'author'". L'opinione sembra essere condivisa anche dal Parlamento europeo. Cfr. Risoluzione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, testo approvato il 20 ottobre 2020, consultabile all'indirizzo [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_IT.pdf), dove, dopo avere espresso scetticismo sulla possibilità di attribuire protezione autoriale ai prodotti dell'IA, § 15 dove si evidenzia che "le opere prodotte autonomamente da agenti artificiali e robot potrebbero non essere ammissibili alla protezione del diritto d'autore, al fine di rispettare il principio di originalità, che è legato a una persona fisica, e dal momento che il concetto di "creazione intellettuale" riguarda la personalità dell'autore".

<sup>36</sup> V. art. 6 e 20 l.a. Per quanto concerne il panorama internazionale, autorevole dottrina ritiene che, nonostante manchi un espresso riferimento nella Convenzione di Berna, lo *jus conventionis* sia inequivocabilmente fondato sulla concezione antropocentrica dell'autore quale creatore dell'opera. Così A. DIETZ, *The Concept of Author under the Berne Convention*, in *R.I.D.A.*, 1993, 2, 10 ss.; S. RICKETSON, *People or Machines: The Berne Convention and the Changing Concept of Authorship, People or Machines: The Berne Convention and the Changing Concept of Authorship*, in *Col. VLA J.L. & the Arts. vol. 16*, 1992, 1, 8 ss. (qui facendo espressamente agli artt. 7, comma 1 e 6 *bis* della Convenzione di Berna relativamente al termine di durata dei diritti e al diritto morale), 21 ss., 36; P. GOLDSTEIN, P.B. HUGENHOLTZ, *International Copyright – Principles, Law, and Practice*, 3ª ed., Oxford, 2013, 191; L.C. UBERTAZZI, *La di-*

tamente la strettissima connessione tra l'autore e la propria creazione intellettuale che giustifica il recente orientamento di quella dottrina che vorrebbe elevare il diritto d'autore al rango di diritto fondamentale<sup>37</sup>. Non solo. Se la legge non è esplicita circa l'elemento antropico che connota il requisito della creatività, per altro verso sancisce chiaramente che il diritto di pubblicare l'opera e di utilizzarla economicamente in ogni forma e modo spetta all'autore, per l'atto stesso della creazione<sup>38</sup>.

Alla luce di quanto detto, e anche là dove si concordasse con chi ritiene che l'IA sia in grado di creare, allo stesso modo di quanto faccia l'essere umano<sup>39</sup>, che si possa immaginare di attribuire la qualità di autore ad una macchina sembra arduo e nemmeno, per certi versi, desiderabile (specie in assenza di una definizione comunemente accolta di cosa possa intendersi per IA)<sup>40</sup>. La macchina intelligente, infatti, non solo non possiede una sua personalità, in grado di riflettersi sull'opera, ma è altresì priva di personalità giuridica e capacità di agire<sup>41</sup>. Questi due aspetti, che non saranno og-

---

*sciplina UE dei diritti morali d'autore*, in *AIDA*, 2016, 374 ss.; ANTIKAINEN, *Copyright Protection and AI-Generated Works – A Fight We Have Already Lost?*, in *AIDA*, 2018, 243 ss.

<sup>37</sup> Si ricordi, invero, che già la Dichiarazione Universale sui Diritti Umani del 1948 all'art. 27, comma 2, statuisce che ogni individuo ha diritto alla protezione dei propri interessi morali e materiali scaturenti da una qualunque tipologia di produzione scientifica, letteraria o artistica di cui sia l'autore. In dottrina, per tutti, v. C. GEIGER, *Copyright's fundamental rights dimension at EU level*, in *Research Handbook on the Future of EU Copyright*, a cura di E. Derclaye, Edward Elgar Publishing, Cheltenham, 2009, 27.

<sup>38</sup> Cfr. art. 2577, comma 1, c.c. e art. 12, commi 1 e 2, l.a.

<sup>39</sup> Cfr. S. GUIZZARDI, *La protezione d'autore dell'opera dell'ingegno creata dall'Intelligenza Artificiale*, in *AIDA*, 2018, 58 (nota 38), la quale ritiene che il processo di creazione di un'opera dell'ingegno interamente demandata alla tecnologia non possa di per sé, per il solo fatto di essere posto in essere dall'IA, dirsi vincolato e dunque talmente predeterminato nel suo esito finale da privare di creatività il risultato finale di tali processi. Posizioni per certi versi analoghe sono state formulate anche da SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, cit., *supra* nota 31, 2019, 273 ss., per il quale se è vero che l'IA non opera in maniera svincolata da qualunque regola, il grado di libertà che essa è in grado di esprimere – nel rispetto del sistema di regole che presidiano il suo funzionamento – sarebbe in linea generale analogo al tipo di creatività che contraddistingue un essere umano.

<sup>40</sup> In questo senso si è espresso anche il Parlamento europeo nella recente Risoluzione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale, cit., dove, dopo avere espresso scetticismo sulla possibilità di attribuire protezione autoriale ai prodotti dell'IA, nel § 15 l'organo raccomanda che la titolarità di eventuali diritti sia eventualmente assegnata soltanto alle persone fisiche o giuridiche che hanno creato l'opera in modo lecito.

<sup>41</sup> Vedi G. FROSIO, *L'(I)Autore inesistente: una tesi tecno-giuridica contro la tutela dell'opera generata dall'intelligenza artificiale*, cit., *supra* nota 4, 2020, 63, per il quale senza personalità giuridica, l'IA non potrebbe comunque né ricevere la titolarità dei diritti d'autore sui prodotti creativi in grado di generare, né fare valere tali diritti contro terzi. Analoghe riflessioni sono state avanzate da M. SENFTLEBEN, L. BUIJTELAAR, *Robot Creativity: An Incentive-Based Neighbou-*

getto di approfondimento in questo saggio, assumono in realtà un rilievo preponderante. L'entità priva di capacità giuridica, invero, difficilmente potrà ritenersi centro di imputazione di diritti e prerogative economiche, per non menzionare le responsabilità per le eventuali violazioni derivanti dalla circolazione, in senso ampio, delle opere prodotte dall'IA. Considerazioni analoghe debbono farsi per il soggetto privo di capacità di agire che sarà invece astrattamente configurabile come titolare dei diritti, e che tuttavia gli sarà precluso esercitare in prima persona. Nel caso della macchina intelligente appare ovvio che essa manchi di entrambi gli elementi. Non solo. Come si dirà meglio in appresso, essa non è in grado, autonomamente, né di sfruttare sapientemente i suoi prodotti (scegliendo, ad esempio, i risultati migliori, valutando le modalità di sfruttamento commerciale più consone, ecc.), né di rispondere in alcun modo degli eventuali danni cagionati (per quanto qui ci occupa) dalla commercializzazione di tali beni <sup>42</sup>.

## **5. Assenza di una giustificazione a sostegno della tesi che intende concedere alla macchina intelligente le fattispecie esclusive tipiche del diritto d'autore**

Ancora, sembra anche chiaro che nel caso delle opere prodotte dall'IA le giustificazioni tipiche dell'esclusiva autoriale non trovano ragion d'essere. L'IA non nutre alcun sentimento verso le proprie opere, né imprime la sua personalità sull'opera. Non abbisogna, quindi, di alcun diritto morale <sup>43</sup>. Parimenti, l'IA non si "affatica"/impegna/affanna nel produrre. Essa

---

*ring Rights Approach*, in *European Intellectual Property Review*, 2020/I, 14, consultabile all'indirizzo <https://www.researchgate.net/publication/344777560>. Sul punto si vedano anche le riflessioni di SENA per il quale proprio l'assenza di capacità giuridica in capo all'IA le impedisce di divenire titolare dei diritti, restando inconfutato che sia quest'ultima l'autore delle sue creazioni. V. G. SENA, *Intelligenza artificiale, opere dell'ingegno e diritti di proprietà industriale e intellettuale*, in *Riv. dir. ind.*, 2020/I, 327.

<sup>42</sup> Si pensi al caso in cui i prodotti dell'IA rappresentino una contraffazione di altro diritto d'autore. Come farebbe l'autore dell'opera contraffatta a chiamare in giudizio l'IA? Vedi sul punto D.J. GERVAIS, *The Machine as Author*, cit., *supra* nota 27, 2019, 37 ss., il quale insiste sullo stretto legame tra authorship/rights attribuiti all'autore dell'opera e responsibility verso le proprie creazioni. Analogamente: M. SENFTLEBEN, L. BUIJTELAAR, *Robot Creativity: An Incentive-Based Neighbouring Rights Approach*, cit., *supra* nota 41, 2020, 15, consultabile all'indirizzo <https://www.researchgate.net/publication/344777560>.

<sup>43</sup> Così S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – The Human-Like Authors are Already Here – A New Model*, cit., *supra* nota 27, 2017, 689.

produrrà incessantemente, a meno che qualcuno non “spenga il bottone”<sup>44</sup>. Di conseguenza, essa non avrà bisogno di alcuna ricompensa per il lavoro intellettuale (che, appunto, non compie), né ambirà ad alcuna forma di riconoscimento o premio economico per continuare a creare<sup>45</sup>.

Da ultimo, non può non notarsi come, quand’anche le si venisse riconosciuta la titolarità dei diritti sui beni intangibili prodotti, l’IA non sarebbe in grado di trarne profitto e, soprattutto di godere di tali profitti.

Per contro, la prospettiva di poter monetizzare i frutti derivanti dallo sfruttamento economico delle opere dell’IA interessa molto all’uomo.

Quest’ultima riflessione ci porta forse a porci una diversa domanda da quella inizialmente formulata. Perché in effetti, e a ben vedere, dietro la retorica della possibilità di riconoscere alla macchina la qualità di autore<sup>46</sup>, si nasconde forse l’esigenza di individuare un soggetto, propriamente una persona fisica o giuridica, cui imputare la titolarità dei diritti sulle opere generate dall’IA – posto che questa, si ricorda, non ha capacità giuridica, né capacità di agire<sup>47</sup>. Più opportuno, allora, porre una diversa domanda e interrogarsi sulla possibilità di attribuire i diritti d’autore sulle opere prodotte dall’IA direttamente all’essere umano che potrebbe essere a) l’ideatore della IA stessa (così intendendo non solo colui che ha predisposto il software di funzionamento, ma anche il soggetto che ha successivamente introdotto i parametri che l’IA utilizzerà per creare ovvero per apprendere,

<sup>44</sup> Così M. PERRY, T. MARGONI, *From music tracks to Google maps: Who owns computer-generated works?*, in *Computer Law & Security Review*, 2010, 628. Si chiede, peraltro, D.J. GERVAIS, *The Machine as Author*, cit., *supra* nota 27, 2019, 9, se la proliferazione di prodotti artistici dell’IA che scaturirebbe a seguito del riconoscimento di un diritto esclusivo su tali beni sia il tipo di «progresso» che la Costituzione americana intendeva promuovere (o se per contro sia una forma inferiore di produzione artistica rispetto a quella umana).

<sup>45</sup> K. HRISTOV, *Artificial Intelligence and the Copyright Dilemma*, cit., *supra* nota 27, 2017, 444. SAMUELSON sostiene che non ha senso attribuire diritti esclusivi alle macchine, dal momento che esse non hanno bisogno di un incentivo per generare output. P. SAMUELSON, *Allocating Ownership Rights in Computer-Generated Works*, in *University of Pittsburgh Law Review*, 47, 1986, 1185, 1199. Cfr. D.J. GERVAIS, *The Machine as Author*, cit., *supra* nota 27, 2019, 60.

<sup>46</sup> Si veda, ad esempio, R. PEARLMAN, *Recognizing Artificial Intelligence (AI) as Authors and Inventors under U.S. Intellectual Property Law*, in *Richmond Journal of Law & Technology* 24, 2, 2018/1, 29, il quale si esprime per l’attribuzione all’IA della qualità di autore, per poi immediatamente andare alla ricerca della persona fisica o giuridica cui imputare lo sfruttamento patrimoniale dei diritti stessi.

<sup>47</sup> In tal senso J. GINSBURG, J. BUDIARDJO, *Authors and Machines*, cit., *supra* nota 4, 2019, 352, secondo i quali la giusta domanda da porsi (escludendo che possa riconoscersi in capo all’IA la capacità di creare e dunque considerarsi autore nell’accezione autoriale del termine) concerne quale peso attribuire alle rivendicazioni di creatività che l’uomo asserisce di avere con riferimento sia alla preparazione sia all’utilizzo della macchina che crea.

nonché colui che ha poi nutrito l'IA con determinati dati e curato l'opera di affinamento del risultato prodotto)<sup>48</sup>; in alternativa b) all'utilizzatore effettivo dell'IA, che con l'IA dialoga e talvolta interagisce dando input che guideranno la messa a punto del prodotto creativo finale<sup>49</sup>, o ancora c) immaginare un sistema di titolarità congiunta dei diritti in capo ad entrambi, o d) da ultimo uno scenario in cui i diritti non spettino a nessuno<sup>50</sup>.

## 6. Può l'inventore/autore dell'IA vantare una qualche prerogativa verso i prodotti dell'IA? e in tal caso a che titolo

Può il creatore dell'IA vantare una qualche prerogativa verso i prodotti creati autonomamente dall'IA? Anche questo quesito in realtà ne sottende due: il primo concerne il se l'autore, in ragione degli input creativi con cui ha forgiato l'IA, e sulla scorta dei quali l'IA a sua volta sarà in grado di creare, possa vantare una qualche prerogativa sui beni prodotti dall'IA. Il secondo quesito concerne, per contro, il tema degli incentivi ad innovare. Ci si chiede, cioè, se il creatore dell'IA, che già può disporre di diritti esclusivi sull'IA in quanto tale, non dimentichiamolo, abbia necessità di appropriarsi anche dei frutti dell'IA<sup>51</sup>.

---

<sup>48</sup> Sulla pluralità di soggetti che prendono parte al processo creativo dell'IA v. S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era*, cit., *supra* nota 27, 2017, 692 ss.

<sup>49</sup> Favorevole a questa tesi parrebbe S. GUIZZARDI, *La protezione d'autore dell'opera dell'ingegno creata dall'Intelligenza Artificiale*, cit., 59 ss. Anche S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era*, cit., *supra* nota 27, 2017, 712 ss., per il quale l'utilizzatore dell'IA sarebbe il soggetto più opportunamente deputato a detenere i diritti sulle opere prodotte dalla macchina che ha commissionato e, parimenti, ad essere ritenuto responsabile per le eventuali violazioni (per quanto qui ci occupa, di diritto d'autore) derivanti dallo sfruttamento commerciale di siffatte opere.

<sup>50</sup> Questa la tesi abbracciata da G. SENA, *Intelligenza artificiale, opere dell'ingegno e diritti di proprietà industriale e intellettuale*, cit. *supra* nota 41, 2020, 329 ss., per l'ipotesi in cui manchi una qualsivoglia connessione tra l'opera realizzata dalla macchina e l'autore dell'IA (dunque nell'ipotesi di una creazione realizzata in via totalmente indipendente dall'IA). In questo caso, secondo l'Autore, mancherebbe il conflitto di interessi intersoggettivo (ossia la presenza di più soggetti umani portatori di interessi contrapposti) che giustifica l'attribuzione di un diritto. A conclusioni analoghe giunge RAMALHO, la quale però motiva l'assenza di protezione nella circostanza che le creazioni dell'IA non soddisfano il requisito della creatività il quale presuppone vuoi la presenza di scelte libere e creative, vuoi il compimento di tali scelte da parte di un autore umano. Siffatti prodotti sono, quindi, destinati a cadere nel *public domain*. A. RAMALHO, *Intellectual Property Protection for AI-generated Creations. Europe, The United States, Australia and Japan*, cit., *supra* nota 35, 2021, 27 ss.

<sup>51</sup> Sulla necessità di porsi tali interrogativi v. J.C. GINSBURG, *People Not Machines: Author-*

## 6.1. I prodotti realizzati dall'IA e le diverse tesi che giustificano l'attribuzione dei relativi diritti all'essere umano

Come evidenziato in precedenza, il ciclo produttivo relativo alla messa a punto dell'IA è intimamente connesso al ciclo produttivo dei beni realizzati dall'IA, essendo alcune delle fasi del primo specificatamente tese a modellare il *modus creandi* della macchina e dunque tali da influire direttamente sul gradiente di creatività dei prodotti che essa andrà a realizzare. Ora, ai fini del nostro tema interessa comprendere in quali di quelle fasi sopra descritte l'intervento umano risulti essere maggiormente incisivo, al punto da riverberarsi sulla creatività delle eventuali opere prodotte dall'IA<sup>52</sup>, e così da giustificare l'attribuzione dei diritti di sfruttamento di queste direttamente in capo a tale soggetto.

Fra i diversi stadi di creazione sopra illustrati quelli che possono denotare un contributo creativo tale da riflettersi sulle opere prodotte dall'IA sono essenzialmente la fase di programmazione e di addestramento dell'IA e la fase di c.d. refinement.

### 6.1.1. La dottrina maggioritaria: valorizzazione dell'apporto creativo umano nella fase di strutturazione e predisposizione dell'IA

La dottrina maggioritaria tende a valorizzare l'impatto creativo sui prodotti dell'IA fornito dall'essere umano durante le prime due fasi ossia il

---

*ship and What It Means in the Berne Convention*, in *IIC*, vol. 48, 2018, 131 ss. Contrari all'attribuzione di ulteriori diritti esclusivi in capo all'autore dell'IA sono G. SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, cit., *supra* nota 31, 2019, 282, che ammonisce contro una "innecessaria superfetazione degli incentivi economici" in favore degli sviluppatori dell'IA. Analogamente G. FROSIO, *L'(I)Autore inesistente: una tesi tecno-giuridica contro la tutela dell'opera generata dall'intelligenza artificiale*, cit., *supra* nota 4, 2020, 81, ritenendo che un'ulteriore ricompensa allo sviluppatore dell'IA, sotto forma di diritti esclusivi sulle creazioni dell'IA, potrebbe favorire l'insorgere di una sorta di «copy right-trolling», che porterebbe per contro ad una riduzione all'incentivo del programmatore a sviluppare nuovi programmi o migliorare quegli esistenti. In senso contrario, sostenendo cioè che la sola tutela sull'IA in quanto prodotto di per sé non sarebbe sufficiente a stimolare l'incentivo all'innovazione v. K. HRISTOV, *Artificial Intelligence and the Copyright Dilemma*, cit., *supra* nota 27, 2017, 439, per il quale l'assenza di tutela sui prodotti finirebbe per scoraggiare gli incentivi a creare nuove macchine di IA. Così si era anche espresso C.R. DAVIS, *An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property*, in *27 Computer L. & Security Rev.*, 2011, 612.

<sup>52</sup> Ed invero, l'analisi giuridica, osservando, deve incentrarsi sulla verifica dell'apporto umano nel ciclo produttivo dell'IA al fine di determinare se quest'ultimo possa impartire un gradiente di creatività sufficiente a determinare la protezione dei prodotti generati dall'IA. *Ibidem*.

momento in cui, attraverso istruzioni informatiche, il/i programmatore/i allestisce/scono il processo creativo della macchina<sup>53</sup>. La via dovrebbe essere allora, più semplicemente, quella di attribuire i diritti di sfruttamento sui beni prodotti dall'IA in capo a quel soggetto (*recte* a quei soggetti) che è responsabile di avere impartito, nelle diverse fasi del processo produttivo (di realizzazione della macchina intelligente), quegli input creativi che la caratterizzano vuoi come prodotto in sé, vuoi nelle sue capacità creative<sup>54</sup>. Si ritiene, infatti, che siffatta creatività certamente sia in grado di riverberarsi sul prodotto realizzato dall'IA, dal momento che tali istruzioni incidono profondamente sul *modus agendi* dell'IA<sup>55</sup>.

---

<sup>53</sup> Vedi J. GRIMMELMANN, *There's No Such Thing as a Computer-Authored Work – And It's a Good Thing, Too*, in 39 *Columbia Journal of Law & the Arts*, 2016, 412. Vedi anche P. SAMUELSON, *Allocating Ownership Rights in Computer-Generated Works*, cit., *supra* nota 45, 1986, 1205, pur propendendo per una diversa soluzione, sottolinea come, perlomeno in prima battuta, appaia chiaro che il contributo dato dal programmatore verso il bene generato dall'IA (anche se lei parlava di “generator program”) sembra spesso essere quello più sostanziale e significativo. Cfr. anche J. GINSBURG, J. BUDIARDJO, *Authors and Machines*, cit., *supra* nota 4, 2019, 401 ss., i quali, pur riconoscendo che i prodotti dell'IA sembrano in tutto e per tutto “creativi” e assai simili ad opere generate dall'essere umano, mettono in guardia dall'attribuire il valore espressivo dei prodotti alla macchina che li ha generati, dal momento che ogni qualsivoglia “creatività” nell'output prodotto dall'IA è direttamente attribuibile al codice scritto dal programmatore che l'ha disegnata e roduta (*trained*) o alle istruzioni impartite dall'utente che sta utilizzando la macchina. Si veda in tal senso anche il Libro Bianco sull'Intelligenza Artificiale della Commissione dove si spiega che: «In case of machine learning techniques, which constitute a subset of AI, algorithms are trained to enter certain patterns based on a set of data in order to determine the actions needed to achieve a given goal. Algorithms may continue to learn when in use. While AI-based products can act autonomously by perceiving their environment and without following a pre-determined set of instructions, their behaviour is largely defined and constrained by its developers. Humans determine and programme the goals, which an AI system should optimise for». V. EC, *White paper on Artificial Intelligence – A European approach to excellence and trust*, 19 February 2020, all'indirizzo [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf), 16.

<sup>54</sup> In questo senso v. anche P.B. HUGENHOLTZ *et al.*, *Trends and Developments in Artificial Intelligence Challenges*, in *Final Report, European Commission*, 2020, 76 e 83, consultabile all'indirizzo [https://www.ivir.nl/publicaties/download/Trends\\_and\\_Developments\\_in\\_Artificial\\_Intelligence-1.pdf](https://www.ivir.nl/publicaties/download/Trends_and_Developments_in_Artificial_Intelligence-1.pdf), secondo i quali il diritto d'autore europeo, così come interpretato dalla Corte di Giustizia, lascerebbe margine per la protezione dei beni prodotti dall'IA in una vasta gamma di campi creativi. Ed infatti, fin tanto che tali prodotti sono in grado di riflettere le scelte creative compiute dall'essere umano in un qualsivoglia stadio della catena creativa (“at any stage o the production process” nelle parole degli Autori), essi sono tali da poter beneficiare della protezione autoriale.

<sup>55</sup> Sul punto v. J. GINSBURG, J. BUDIARDJO, *Authors and Machines*, cit., *supra* nota 4, 2019, 407 ss., secondo i quali anche nel caso delle macchine self-learning, dotate dei più sofisticati programmi di auto-apprendimento, la macchina pur sempre procede sulla scorta delle informazioni inizialmente impartite dal suo programmatore. Analogamente si esprime F. ROSSI, *L'intelligenza artificiale e la definizione di opera dell'ingegno*, cit., *supra* nota 27, 2018, 276, il quale osserva che il momento chiave è pur sempre quello della predisposizione dell'algoritmo, ossia del

Tale impostazione, tuttavia, di fatto considererebbe la macchina intelligente alla stregua di un qualsivoglia altro strumento tecnologico (come può essere una macchina fotografica, capace di mettere a fuoco l'immagine e di applicare i filtri migliori per ogni contesto, secondo le preferenze impartite dal suo proprietario). Ed è stata aspramente criticata da quanti, per contro, evidenziano le peculiarità delle più sofisticate macchine di IA, e cioè quelle basate su modelli di auto-apprendimento (tramite algoritmi di *machine-learning*) che emulano le sinapsi e i metodi del ragionamento induttivo tipico del cervello umano, dove i processi di calcolo interni raggiungono una complessità tale da sfuggire alla comprensione dello stesso programmatore<sup>56</sup>. Sempre secondo questo indirizzo, la conseguente non prevedibilità da parte dell'autore del preciso risultato finale che la macchina è in grado di raggiungere spezzerebbe il legame creativo tra autore (si badi: dell'IA in quanto tale) e il prodotto generato dalla macchina intelligente, facendo venir meno l'elemento dell'originalità dell'opera intesa come lavoro intellettuale ascrivibile al suo autore umano<sup>57</sup>. Anche questo

---

percorso logico che il sistema seguirà per rielaborare il materiale di base fino a giungere alla messa a punto di un risultato originale. Scenario che non cambia, secondo l'autore, nemmeno nel caso di sistemi self learning, in quanto il loro agire sarà sempre limitato, in maniera incontrovertibile, dalla base di dati di partenza e dall'algoritmo di programmazione. Una posizione contraria è stata, per contro, espressa da S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era*, cit., *supra* nota 27, 2017, 693 ss., per il quale nessuno dei soggetti che prende parte al processo creativo dell'IA sarebbe in grado di poter vantare una qualche prerogativa giuridica sui beni prodotti dalla macchina intelligente.

<sup>56</sup> Sul punto v., *ex multis*, OTTOLIA, il quale distingue tra sistemi «opachi», anche detti *black box*, dove le regole in funzione delle quali il software prende le proprie decisioni sono in larga misura sviluppate dalla stessa macchina intelligente e non sono, di conseguenza, pienamente conoscibili dall'uomo; ed i sistemi «trasparenti», o c.d. *clear box*, dove invece le regole di funzionamento del software sono interamente predeterminate dall'uomo secondo specifici parametri e, di conseguenza, non solo integralmente conoscibili, ma anche modificabili dall'uomo. Cfr. A. OTTOLIA, *Big Data e Innovazione Computazionale*, in *Quaderni di AIDA*, 2020, 11 ss. Per una disamina degli aspetti di funzionamento delle diverse tipologie di IA v. M. CAPPARELLI, *Le invenzioni dell'intelligenza artificiale: questioni aperte di tutela autoriale e brevettabilità*, in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, 346 ss.

<sup>57</sup> Così D.J. GERVAIS, *The Machine as Author*, cit., *supra* nota 27, 2019, 6 ss., il quale eloquentemente puntualizza come "... The automated decision-making feature of deep learning machines [...] adds unpredictability [...] and in doing so it breaks the causal link between humans (the author of the code and the user of the machine) and the output". Sul punto concorda K. HRISTOV, *Artificial Intelligence and the Copyright Dilemma*, cit., *supra* nota 27, 2017, 436 ss., per il quale la macchina intelligente che sia totalmente autonoma nella creazione produce risultati casuali la cui paternità, di conseguenza, non può essere attribuita al programmatore. Secondo HRISTOV, ciò porterebbe alla conseguente caduta nel dominio pubblico di tutte le opere prodotte dall'IA. Vedi anche M. SENFLEBEN, L. BUIJTELAAR, *Robot Creativity: An Incentive-Based Neighbouring Rights Approach*, cit., *supra* nota 41, 2020, 9 ss.

punto, tuttavia, è assai controverso. A ben vedere, infatti, l'elemento della c.d. “*nondeterministic creation*” non è fenomeno del tutto nuovo nella storia diritto d'autore, e non mancano esempi in cui si tende a ritenere integrati i requisiti di protezione anche là dove il processo creativo si sia in tutto o in parte avvalso di strumenti che introducono un gradiente di imponderabilità del risultato creativo finale<sup>58</sup>: ciò però a condizione che l'autore avesse deliberatamente scelto di abbracciare e far suo l'elemento che causa indeterminatezza<sup>59</sup>.

Una conferma in tal senso pare potersi cogliere anche in quella giurisprudenza, principalmente anglosassone<sup>60</sup>, in materia di videogiochi dove si è sempre negata all'utilizzatore la titolarità sulle immagini prodotte a video come risultato degli input impartiti durante il gioco, dal momento che le creazioni così ottenute sono intrinseche allo stesso software, avendo il programmatore (astrattamente) previsto ogni possibile futura combinazione<sup>61</sup>.

---

<sup>58</sup> Vedi J. GRIMMELMANN, *There's No Such Thing as a Computer-Authored Work*, cit., *supra* nota 53, 2016, *passim*, per il quale il tema non pone problematiche nuove rispetto a quanto non accada normalmente nel caso di opere dell'ingegno prodotte con l'aiuto, più o meno sensibile, di un computer o di altro elemento che aggiunga indeterminatezza al procedimento creativo. GRIMMELMANN fa riferimento al *Musikalisches Würfelspiel* (*gioco dei dadi musicali*) pubblicato nel 1792 ed attribuito a MOZART, dove disponendo su un tavolo una serie di frammenti musicali e utilizzando poi dei dadi per estrarre a sorte i frammenti era possibile comporre dei minuetti sempre nuovi. Riporta l'autore come, nel passato, nessuno mai avesse pensato di attribuirsi la paternità delle opere musicali derivanti dal gioco, così come nessuno mai ha pensato di poter attribuire la paternità ai dadi stessi. Altro esempio cui l'autore fa riferimento sono le opere pittoriche di Jackson Pollock (cui pure si riferisce D. Burk nel saggio citato alla nota in appresso), noto esponente del c.d. *action painting*, realizzate con la tecnica del «dripping». Anche in questo caso, sebbene nelle opere fosse presente un forte elemento di indeterminatezza, legato alla tecnica pittorica utilizzata, nessuno ha mai messo in dubbio la paternità dei dipinti.

<sup>59</sup> Sulla rilevanza dell'elemento della *volition* come fattore di causazione nel diritto d'autore v. D.L. BURK, *Thirty-Six Views of Copyright Authorship, by Jackson Pollock*, cit., *supra* nota 28, 2020, 268.

<sup>60</sup> U.S. District Court for the Northern District of Illinois, 10 marzo 1982, 704 F.2d 1009, *Case Midway Mfg. Co. c. Artic Int'l, Inc.*, consultabile all'indirizzo <https://law.justia.com/cases/federal/district-courts/FSupp/547/999/1478912/>. La corte ha sostenuto che “playing a video game is more like changing channels on a television than it is like writing a novel or painting a picture. The player ... does not have control over the sequence of images that appears on the video game screen. He cannot create any sequence he wants out of the images stored on the game's circuit boards. The most he can do is choose one of the limited number of sequences the game allows him to choose”. V. anche United States Court of Appeals, Second Circuit, 20 January 1982, 669 F.2d 852, *Stern Elecs, Inc. c. Kaufman*, <https://openjurist.org/669/f2d/852/stern-electronics-inc-v-kaufman>.

<sup>61</sup> Cfr. tuttavia J.C. GINSBURG, *People Not Machines: Authorship and What It Means in the Berne Convention*, cit., *supra* nota 51, 2018, 131, 423 ss., la quale ritiene che il “possible anticipation test” (incentrato sul se “the upstream creator has sufficiently “bounded” the downstream

### 6.1.2. La dottrina che valorizza l'apporto creativo dell'utente

Un diverso filone di pensiero ha, per contro, valorizzato il peso del contributo creativo umano nella fase c.d. di *refinement*, intesa sia come stadio finale di perfezionamento dell'opera, con modifiche o aggiunte da parte dell'autore, sia come fase di selezione e scelta (tra le tante possibili opzioni) di quel risultato che maggiormente incarna l'estro creativo dell'autore e può, di conseguenza, essere destinato alla disseminazione<sup>62</sup>. Ed invero, come già osservato, l'IA non sarebbe in grado, senza l'intervento umano, di selezionare quali opere destinare al mercato (né tantomeno di diffonderle e trarne profitto). Si pensi, nel caso di Aaron, alla scelta effettuata da Cohen relativamente a quali dipinti destinare al mercato o ancora, nel caso di programmi di traduzione ovvero di produzione di testi, alle revisioni apportate dall'autore prima di licenziare il testo definitivo<sup>63</sup>.

Queste riflessioni, si diceva, hanno spinto parte della dottrina a ritenere preponderante il ruolo creativo dell'eventuale utilizzatore dell'IA, in tutti quei casi in cui la macchina intelligente non sia pensata per uso personale ed esclusivo del suo autore (come nel caso di Aaron), ma sia invece riservata al mercato e dunque concessa in licenza o financo ceduta ad un terzo. In queste ipotesi, colui che legittimamente utilizza il prodotto IA, per effetto del contratto, subentrerà all'autore dell'IA nella fase di *refinement* del-

---

creator's role ...” e se “... the upstream creator *could have anticipated* what the downstream user would do to *complete* the work”) sarebbe certo utile nei casi di videogiochi più semplici come Space Invader, Pac Man, Tetris o Candy Crush in cui il programmatore ha potuto prevedere tutti i possibili risultati di gioco. Parrebbe invero inadeguato, per contro, per videogiochi più complessi, come ad esempio *Minecraft*, nel quale gli sviluppatori del programma forniscono una serie di elementi predefiniti (ossia gli strumenti con cui i giocatori possono costruire gli ambienti in cui si svolgerà il gioco), ma dove l'apporto creativo dell'utente è massimo e i risultati cui perviene sono di conseguenza imprevedibili al momento della programmazione del gioco stesso.

<sup>62</sup> Vedi, tuttavia, *contra* M.J. ANTIKAINEN, *Copyright Protection and AI-Generated Works – A Fight We Have Already Lost?*, in *AIDA*, 2018, 258 ss., per il quale spesso il ruolo dell'utilizzatore della macchina si limita al solo comando iniziale («pushing a button») e dunque anche quando il risultato prodotto dalla macchina dovesse avere una qualche valenza estetica, tale bene non potrebbe considerarsi una creazione intellettuale del suo autore, mancando il tocco personale di quest'ultimo nell'opera.

<sup>63</sup> Ciò, si badi, anche là dove “[...] the Ai system has played a significant or even predominant role in the entire creative process”. Cfr. P.B. HUGENHOLTZ *et al.*, *Trends and Developments in Artificial Intelligence Challenges*, cit., *supra* nota 54, 2020, 76 e 83, dove si aggiunge che anche nel caso di prodotti con caratteristiche del tutto imprevedibili per l'autore dell'IA, in ragione delle tecniche di machine learning impiegate, il ruolo di quest'ultimo tornerebbe comunque a divenire prevalente nella fase finale di “redazione” («redaction») dell'opera, che richiede diversi input creativi.

l'opera e si inserirà nella catena creativa, seppur solo limitatamente a tale stadio<sup>64</sup>. D'altra parte, come ha giustamente enfatizzato la Corte di Giustizia in *Painer*, l'apporto creativo può anche aversi limitatamente ad una singola e precipua fase del processo creativo dell'opera, ma se tale l'apporto è comunque in grado di imprimere il tocco dell'autore sull'opera, esso sarà meritevole di protezione.

Sotto un diverso profilo, con buona probabilità anche l'utilizzatore legittimo dell'IA avrà necessità di poter vantare delle prerogative economiche verso lo sfruttamento commerciale delle creazioni prodotte dal robot intelligente (che ha probabilmente acquistato proprio per tale precipua finalità). In quest'ultimo caso, un diritto che attribuisse le facoltà esclusive sui prodotti dell'IA unicamente all'ideatore della macchina intelligente parrebbe frustrare gli incentivi economici dell'utilizzatore dell'IA creativa<sup>65</sup>. Ed invero, in questa ipotesi, mentre gli incentivi ad innovare degli autori dell'IA saranno certamente compensati dai canoni di licenza corrisposti dall'utilizzatore (certamente calibrate in modo da riflettere il potenziale creativo dell'IA)<sup>66</sup>, sarebbero probabilmente frustrati quelli dell'utilizzatore dell'IA, che sarà interessato, viceversa, a poter trarre profitto dai prodotti dell'IA<sup>67</sup>: si noti, infatti, che l'uso principale della macchina intelligente creativa è quello di creare (e poi disseminare) beni equiparabili ad opere dell'ingegno.

---

<sup>64</sup> Sul punto K. HRISTOV, *Artificial Intelligence and the Copyright Dilemma*, cit., *supra* nota 27, 2017, 445.

<sup>65</sup> M. SENFLEBEN, L. BUIJTELAAR, *Robot Creativity: An Incentive-Based Neighbouring Rights Approach*, cit., *supra* nota 41, 2020, 13.

<sup>66</sup> Non sembra condivisibile la tesi di chi sostiene che i prodotti dell'IA siano realizzati a costo zero e dunque gli imprenditori non abbiano necessità di internalizzare gli investimenti nelle loro creazioni. Vedi G. SPINA ALÌ, *The Times They Are AI-Changin': Copyright and Computer Generated Works*, in *AIDA*, 2018, 373. Analogamente v. M. PERRY, T. MARGONI, *From music tracks to Google maps: Who owns computer-generated works?*, cit., *supra* nota 44, 2010, 628 secondo i quali proprio perché produrre arte tramite IA non costerebbe nulla, la sua appropriabilità da parte di terzi non autorizzati non dovrebbe portare ad un fallimento di mercato e non andrebbe considerata free riding. Si noti, per contro, come se la stessa messa a punto dell'IA in quanto prodotto richiede cospicui investimenti, spesso il recupero degli stessi potrebbe essere legato proprio dalla possibilità di appropriarsi dei frutti creati successivamente dall'IA.

<sup>67</sup> Sul punto v. P. SAMUELSON, *Allocating Ownership Rights in Computer-Generated Works*, cit., *supra* nota 45, 1986, 1207. Secondo l'autrice, poiché la generazione di output rappresenta lo scopo per cui i *generative programs* (ossia l'IA) sono creati, se l'inventore dell'IA decide di cederla a terzi, chiedendo un corrispettivo importante all'atto di cessione ovvero delle royalties molto alte per il suo utilizzo, è giusto che questi ceda parimenti (perlomeno alcun-) i diritti sui beni prodotti tramite l'impiego dell'IA, e questo al fine di creare incentivi per gli utilizzatori a sfruttare la tecnologia. Sul punto anche S. YANISKY-RAVID, *Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era*, cit., *supra* nota 27, 2017, 682.

## 7. Una proposta *de jure condendo* di regolamentazione della tutela dell'IA e dei suoi prodotti tramite il diritto d'autore e i diritti connessi

La disamina appena compiuta delle tesi che tentano di giustificare l'attribuzione all'essere umano di prerogative autoriali sui beni prodotti dalla macchina intelligente mostrano tutte evidenti profili critici che inducono a scartare una tale ipotesi. Eppure, che vi sia un *quid* creativo nel processo di allestimento della macchina, che si riflette poi nei suoi prodotti, sembra innegabile agli occhi di chi scrive<sup>68</sup>. Come certo pure sembra innegabile che se di creatività si voglia parlare, in capo all'autore (*recte: agli autori*) dell'IA, si tratti in questo caso di una creatività "affievolita", "attenuata" in qualche misura dall'intervento (imponderabile) della macchina intelligente. Ad ogni buon conto, poiché – come si diceva – la IA è un prodotto complesso, realizzato grazie all'apporto di una pluralità di contributi creativi, anche l'eventuale creatività che si riverbera a valle sui prodotti da questa creati andrebbe ricondotta congiuntamente a tutti quei soggetti che partecipano al processo creativo dell'IA, con le complessità già evidenziate in precedenza. Ecco che allora, riagganciandoci a quanto già proposto, là dove si introducesse per l'IA (in quanto prodotto autonomo) una protezione analoga a quella dell'opera cinematografica (che riconosce qualità di co-autore congiuntamente in capo a tutti quei soggetti che hanno massimamente contribuito alla realizzazione dell'opera, e allo stesso tempo assegna i diritti di sfruttamento commerciale dell'opera al suo produttore), sarebbe facile ipotizzare sempre in capo a quest'ultimo un diritto connesso sulle eventuali creazioni prodotte dalla macchina intelligente<sup>69</sup>.

Un diritto connesso sulle creazioni prodotte dall'IA, in capo al produttore dell'IA medesima, risolverebbe *in primis* l'annoso tema della nozione

---

<sup>68</sup> Dello stesso avviso A. GUADAMUZ, *Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works*, in *Artificial Intelligence and Intellectual Property*, a cura di Lee, Hilty, Liu, Oxford University Press, Oxford, 2021, 175.

<sup>69</sup> Si noti come la proposta differisca sensibilmente dal modello di protezione anglosassone dei «computer-generated works» definiti, nel diritto d'autore inglese, come quei prodotti "[...] generated by computer in circumstances such that there is no human author for the work" (art. 178 c.d.p.a.). La titolarità dei diritti su queste opere spetta, secondo l'art. 9 § 3 della normativa, alla persona "[...] by whom the arrangements necessary for the creation of the work are undertaken", dove tuttavia, volendo applicare l'insieme di norme alle creazioni dell'IA, non sarebbe chiaro comprendere se il soggetto autore sarebbe da intendersi come colui che ha predisposto il sistema di IA ovvero il suo utilizzatore finale (nel caso in cui i due soggetti non coincidano).

di creatività intesa quale “author’s own intellectual creation”<sup>70</sup> e del concetto di *authorship* come di provenienza dell’opera da un autore umano<sup>71</sup>. Come noto, invero, i diritti connessi prescindono dalla prova del gradiente di creatività dei prodotti su cui insistono (non essendo tale elemento previsto in questo caso come requisito di accesso alla tutela)<sup>72</sup> e sono, in diversi casi, collegati alla tutela dell’investimento<sup>73</sup>. L’attribuzione del diritto connesso, dunque, risolverebbe il problema della protezione degli investimenti<sup>74</sup>, e di conseguenza quello della tutela degli incentivi economici ad investire nella messa a punto di IA creative che vengono realizzate proprio in vista dei prodotti che riescono a concepire<sup>75</sup>.

---

<sup>70</sup> Proprio in ragione delle peculiarità appena descritte, secondo alcuni autori taluni beni intellettuali, come ad esempio i fonogrammi, sarebbero già di per sé tutelabili tramite la disciplina dei diritti connessi esistente (ad esempio per i fonogrammi) anche là dove prodotti dall’Ia, proprio perché la fattispecie costitutiva del diritto non risiede, in tal caso, nella creazione dell’opera, ma nella fissazione del bene intangibile. Cfr. P.B. HUGENHOLTZ *et al.*, *Trends and Developments in Artificial Intelligence Challenges*, cit., *supra* nota 54, 2020, 89 ss.

<sup>71</sup> A differenza del diritto d’autore classico, il diritto connesso trova la sua giustificazione unicamente nella tutela dell’investimento fatto dal titolare del diritto contro la misappropriation. Ha dunque natura esclusivamente economica. Così A. KUR, T. DREIER, *European Intellectual Property Law – Text, Cases & Materials*, Edward Elgar Publishing, Cheltenham, 2013, 242.

<sup>72</sup> Cfr. BERTANI, *Diritto d’autore europeo*, cit., *supra* nota 7, 2011, 288 ss., ove si evidenzia che i diritti connessi vengono in gioco per fornire una protezione a prestazioni di artisti e di imprenditori culturali “... che per essere prive tipicamente di carattere creativo non potrebbero avere accesso al diritto d’autore”. Con precipuo riferimento al tema della fattispecie costitutiva dei diritti connessi, l’Autore ne sottolinea il carattere oggettivo, ritenendosi integrata ogniqualvolta sia stata espletata la prestazione oggetto della fattispecie (che in alcuni casi prevede l’organizzazione ed il coordinamento di diversi fattori produttivi – es. nel caso del produttore fonografico o audiovisivo – mentre in altri ha ad oggetto una prestazione complementare a quella creativa dell’autore – es. l’esecuzione dell’opera musicale).

<sup>73</sup> Come magistralmente spiegato da AUTERI, i diritti connessi regolano, a ben vedere, una serie assai eterogenea di fattispecie accomunate fra loro solo dal fatto di essere in qualche misura ed in diverso modo “connessi” al diritto d’autore. Ed invero, in alcuni casi tali fattispecie proteggono creazioni simili a quelle protette dal diritto d’autore (come nel caso delle interpretazioni ed esecuzioni di opere), in altri la protezione si appunta sui materiali/supporti necessari per la fruizione dell’opera o per lo stesso venire in essere dell’opera (si pensi, ad esempio, alla tutela del fonogramma, del videogramma, delle emissioni radiotelevisive). In questo secondo caso, i diritti connessi tipicamente proteggono i risultati di un’attività organizzativa svolta massimamente in forma di impresa. Così AUTERI, in *Diritto Industriale, proprietà intellettuale e concorrenza*, cit., *supra* nota 7, 2020, 745. Analogamente sul punto J.-A. LEE, *Computer-generated Works under the CDPA 1988*, in *Artificial Intelligence and Intellectual Property*, a cura di Lee, Hilty e Liu, cit., *supra* nota 68, 2021, 183 ss.

<sup>74</sup> È bene notare come non sia prevista alcuna soglia minima di investimenti per accedere alla protezione garantita dai diritti connessi, v. A. RAMALHO, *Intellectual Property Protection for AI-generated Creations. Europe, The United States, Australia and Japan*, cit., *supra* nota 35, 2021, 33.

<sup>75</sup> Sul punto v. S. LAVAGNINI, *Intelligenza artificiale e proprietà intellettuale: proteggibilità del-*

Il diritto connesso sulle creazioni dell'IA, che potrebbe a sua volta decorrere dalla fissazione di tali creazioni su supporto tangibile (o non) e avere una durata più ridotta di quella tributata alle opere dell'ingegno classiche, potrebbe chiaramente concernere, come nel caso del produttore cinematografico, solo alcune fattispecie esclusive (ossia principalmente il diritto di riproduzione, distribuzione, comunicazione al pubblico, making available right).

Da ultimo, una tale soluzione potrebbe certamente agevolare le istanze degli utenti che lecitamente acquisiscono la disponibilità del sistema di IA e sono interessati ad appropriarsi dei prodotti da questa realizzati. Il contratto di licenza/cessione del sistema intelligente potrebbe, infatti, prevedere, fra le facoltà di utilizzo cedute, quella di sfruttamento delle creazioni prodotte dalla macchina.

---

*le opere e titolarità dei diritti*, in *Il Diritto d'Autore*, 2018/4, 466. Secondo l'Autrice la mancata tutela delle opere generate dall'IA potrebbe disincentivare gli investimenti in R&S sui sistemi di intelligenza artificiale, questo comporterebbe gravi conseguenze soprattutto nel caso in cui le stesse trovassero tutela in altri ordinamenti. Cfr. Più in generale, M. LIBERTINI, *Tutela e promozione delle creazioni intellettuali e limiti funzionali della proprietà intellettuale*, in *AIDA*, 2014, 336, il quale ribadisce il ruolo delle privative industriali/intellettuali quali strumenti di politica economica. Conseguentemente, l'Autore suggerisce di impostare l'analisi tesa a sondare le prospettive di nuova formulazione dell'esclusiva sulla scorta di una valutazione imperniata sull'effettiva funzionalità della tutela rispetto allo scopo dell'incremento del benessere economico collettivo e del sostegno all'innovazione.

Maria Letizia Bixio

## Applicazioni della *blockchain* nei processi di tracciabilità e certificazione, valutazioni in itinere

SOMMARIO: 1. Introduzione. – 2. *Blockchain* nel sistema della tracciabilità. – 2.1. Tracciabilità quale leva pro-competitiva: aspetti positivi nell'impiego della *blockchain* per i consumatori e per le imprese. – 2.2. Test per la verifica dei limiti nell'applicazione della tecnologia. – 3. Per un'ipotesi evolutiva della funzione: dal marchio di certificazione alle "certificazioni" *blockchain-based*. – 4. Conclusioni.

### 1. Introduzione

La competitività delle imprese e la loro attitudine ad uno sviluppo sostenibile non possono prescindere dal ricorso a processi e soluzioni innovative, né dalla funzionalizzazione di talune competenze<sup>1</sup>. Non stupisce che transizione digitale e transizione verde siano coesenziali all'inquadramento del tema e alla formulazione di possibili proposte. La *twin transition* è infatti il cuore della Agenda digitale europea e come tale deve ispirare ed indirizzare le scelte nazionali<sup>2</sup>. Non vi è dubbio che l'innovazione

---

<sup>1</sup> Il digitale ha come naturale predisposizione quella di facilitare la raccolta di una maggiore mole di dati, riducendone al tempo stesso i tempi e i costi. Si riducono inoltre le possibilità di errore e manomissione del dato, criticità tipiche del mondo analogico. Inoltre, tra i benefici legati al miglioramento del processo stesso di tracciabilità e rintracciabilità vi sono la maggiore velocità nel poter identificare i prodotti e la conseguente riduzione dei costi di gestione di eventuali blocchi o richiami. Per un'analisi approfondita dei cambiamenti sistemici derivanti dall'innovazione tecnologica, a livello regolatorio, ma non solo, si veda M. GAL, *Competition and Innovation in the digital environment*, in AA.VV. (a cura di G. Colangelo, V. Falce), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Bologna, 2017, 11 ss.

<sup>2</sup> Richiesta dal Piano Nazionale di Ripresa e Resilienza la *twin transition* è la doppia transizione cui le imprese devono rispondere negli obiettivi fissati dall'Europa entro il 2050. Sia la transizione verde che quella digitale, infatti, sono priorità politiche della Commissione europea

tecnologica stia già incidendo positivamente su tutte le dinamiche legate al tema della tracciabilità<sup>3</sup>, semplificando prassi in passato ingessate da vincoli normativi e potenziando l'operatività attraverso l'automazione.

È questo il motivo per cui si assiste ad un crescente interesse nei confronti delle molteplici, e talvolta ancora inesplorate, declinazioni dell'utilizzo della *blockchain*, che, per esempio, nel settore industrialistico potrebbe rivoluzionare l'ambito della tracciabilità e delle certificazioni attraverso il suo impiego.

Grazie alla garanzia di immutabilità delle informazioni promessa dalle piattaforme *blockchain*, così come al potenziale di assoluta trasparenza, che verrebbe garantita lungo la filiera, gli *stakeholder* si mostrano fiduciosi nell'incremento dell'efficacia e dell'efficienza dei processi di recupero dei dati in caso di situazioni critiche, come ad esempio la "*food safety*"<sup>4</sup>.

---

nel lungo termine. Sebbene queste due transizioni simultanee possano rafforzarsi a vicenda in molte aree, non sono automaticamente allineate. Ad esempio, l'incremento dell'impiego delle tecnologie digitali può avere un forte impatto ambientale che andrebbe contro gli obiettivi della transizione verde. Questo è il motivo per cui un approccio integrativo alla gestione delle transizioni gemelle è importante per garantire la loro attuazione di successo. Più diffusamente si veda il report S. DI MUENCH, E. STOERMER, K. JENSEN, T. ASIKAINEN, M. SALVI, F. SCAPOLO, *Towards a green and digital future*, EUR 31075 EN, Publications Office of the European Union, Luxembourg, 2022. Di contro, è altresì vero che i requisiti di due diligence normativa, l'aumento delle aspettative di investitori e consumatori e i progressi tecnologici hanno incrementato notevolmente il grado di attenzione per i temi della sostenibilità. Determinante per la sostenibilità o meno di un prodotto è infatti il flusso di informazioni, quindi materiali che lo compongono. In tal senso si vedrà come il sistema *blockchain* può ad esempio velocizzare i controlli sulla produzione, finalizzati all'ottenimento di marchi collettivi e di certificazione.

<sup>3</sup>Il termine tracciabilità riferisce idealmente al percorso di un prodotto da prima della fase di produzione dello stesso sino alla sua messa in vendita (ad esempio per un bene alimentare si parte dalle materie prime utilizzate, opportunamente identificate e mappate, sino alle fasi della lavorazione, che conducono alla distribuzione del prodotto finito sul mercato). Il concetto di tracciabilità non va confuso con quello di rintracciabilità, che indica l'esatto processo inverso, ovvero l'iter che partendo dal prodotto finito risale a tutte le fasi di distribuzione e lavorazione fino all'origine delle materie prime. La rintracciabilità, messa a sistema, abilita un processo automatizzato e integrato che permette di ricostruire e intercettare immediatamente l'origine di eventuali anomalie che possono essere insorte nella *supply chain*, comportando elementi di alterazione, perdita o contraffazione di uno o più prodotti.

<sup>4</sup>Quando il concetto di tracciabilità viene evocato con riguardo al comparto alimentare si intende richiamare la capacità di tenere traccia di ogni alimento utilizzato per il consumo, e di tutti i processi che essi hanno subito, attraverso tutti gli stadi della filiera. Da notare che detto tracciamento risponde al regolamento n. 178/2002 del 28 gennaio 2002 che stabilisce i principi e i requisiti generali della legislazione alimentare e istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare. Inoltre, dalla disponibilità di dati viene generata maggiore efficienza dei processi di *supply chain*, con effetti sul miglioramento nella gestione delle scorte, sulla riduzione degli sprechi e sul consolidamento delle relazioni di filiera.

## 2. Blockchain nel sistema della tracciabilità

Con il termine *blockchain* si intende un particolare tipo di tecnologia basata su registri distribuiti<sup>5</sup>, in cui i dati delle transazioni sono raccolti in c.d. blocchi collegati tra loro ed inseriti all'interno di un registro secondo una sequenza temporale. In questo modo le informazioni archiviate, una volta immesse nel registro e validate, sono (dovrebbero essere) inalterabili e vengono riportate a tutti i partecipanti alla piattaforma *blockchain*<sup>6</sup>.

Di fatto ci si trova dinanzi ad una sorta di registro digitale che include numerose voci raggruppate in blocchi, concatenati tra loro in ordine cronologico, la cui integrità è (dovrebbe essere) garantita dall'uso della crittografia. La *blockchain* non è tipicamente considerata un mezzo di comunicazione e nemmeno un sistema di *business application* a sé stante, motivo per cui spesso si usa l'espressione "applicazioni basate sulla *blockchain*".

Nell'ambito dell'ordinamento giuridico nazionale, la definizione di "tecnologie basate su registri distribuiti" è stata inclusa nell'art. 8 ter del d.l. n. 135/2018<sup>7</sup>, dove, si definiscono "*Distributed ledger technology*", "*le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati, sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*"<sup>8</sup>, la norma inoltre, al fine di chiarire come tramite la registra-

---

<sup>5</sup>Per un primo inquadramento giuridico e definitorio si rimanda a M. GIULIANO, *La "blockchain" e gli "smart contracts" nell'innovazione del diritto nel terzo millennio*, in *Il Diritto dell'informazione e dell'informatica*, (6), 989-1039, 2018 e G. REMOTTI, *Blockchain smart contract. Un primo inquadramento*, in ODCC, 2020, 19.

<sup>6</sup>La *blockchain* è stata introdotta per la prima volta nel 2008 quale prima vera soluzione informatica al problema del consenso distribuito per fungere da registro condiviso delle transazioni della nascente cripto-valuta Bitcoin, un sistema di pagamento basato su un registro distribuito che non richiede la presenza di una banca per funzionare, e nel quale le registrazioni dei trasferimenti di (cripto)valuta vengono archiviate in una catena di blocchi (c.d. blockchain). Attraverso il meccanismo informatico noto come "proof of work" si consente ai nodi di una rete (che non si conoscono tra loro) di raggiungere ugualmente il consenso nella validazione delle transazioni.

<sup>7</sup>D.l. 14 dicembre 2018, n. 135, Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione. (18G00163) d.l. convertito con modificazioni dalla legge 11 febbraio 2019, n. 12 (in G.U. 12 febbraio 2019, n. 36). Tra i primi commenti si segnala C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto mercato tecnologia*, 201; M. MANENTE, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note*, Studio I-2019, Consiglio Nazionale del Notariato, disponibile al sito: <https://notariato.it/wp-content/uploads/S-1-2019-DI.pdf>.

<sup>8</sup>Al comma terzo del medesimo articolo viene poi previsto che la memorizzazione di un docu-

zione della documentazione attraverso la tecnologia *blockchain* si producano gli effetti di una registrazione legalmente valida e riconosciuta<sup>9</sup>, al terzo comma puntualizza che: “*La memorizzazione di un documento informatico attraverso l’uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all’articolo 41 del regolamento europeo in materia di identificazione elettronica*”.

Pur volendo ridurre al minimo il dettaglio di questioni squisitamente tecniche, giova in questa sede evidenziare come per sondare con successo le possibili sinergie tra l’impiego di detta tecnologia e una serie di processi legati alla tracciabilità delle filiere produttive ovvero alla costituzione o alla circolazione di titoli di proprietà intellettuale, non si può prescindere da un esame trasversale di natura tecnico-legale.

L’analisi letterale del dato normativo rimanda l’approfondimento a talune peculiarità tecniche di detti registri, che al contempo possono rappresentare punti di caduta rispetto allo schema della certezza del diritto.

Un primo elemento da attenzionare sta nel fatto che le transazioni registrate nel c.d. registro distribuito sono anzitutto dislocabili in più luoghi e presso soggetti differenti, e, nel contempo, non è prevista un’autorità centrale atta a mantenere il controllo sul registro e sulla sua integrità.

Se, quindi, dal punto di vista informatico, il vantaggio dei registri sta nell’eliminazione del problema del “*single point of failure*” (letteralmente “singolo punto di vulnerabilità”), e dunque l’ampia “distribuzione” diviene sinonimo di sicurezza informatica<sup>10-11</sup>, dal punto di vista giuridico l’as-

---

mento informatico attraverso l’uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all’art. 41, regolamento UE n. 910/2014 in materia di identificazione elettronica (Regolamento EIDAS). Infine, il quarto comma dispone che dovrà essere l’Agenzia per l’Italia Digitale ad individuare gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.

<sup>9</sup>In seguito a questi aggiornamenti normativi si è assistito al proliferare di numerose piattaforme tecnologiche dedicate all’archiviazione e gestione di documentazione relativa ad asset immateriali, tra queste ricordiamo forse la più autorevole che è “WIPO PROOF” di WIPO (World Intellectual Property Organization). L’archiviazione di un documento tramite queste piattaforme genera un certificato con validità legale comprovante la registrazione e recante data e ora del caricamento. In tal modo viene resa evidente l’esistenza di quel file in quel determinato momento.

<sup>10</sup>Più diffusamente si veda M. MANENTE, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note*, Studio I-2019, Consiglio Nazionale del Notariato, cit., nello spiegare come in caso di registro centralizzato un attacco perpetrato all’autorità centrale consentirebbe all’hacker di prendere il controllo del registro e di alterarlo, in un registro distribuito l’attacco sarebbe notevolmente più difficile, poiché richiederebbe il simultaneo attacco di tutti (o almeno della maggioranza) delle copie del registro esistenti.

<sup>11</sup>A riguardo non stupisce che ad oggi si siano sviluppati prevalentemente sistemi di registrazione basati su registri centralizzati.

senza di un controllo centralizzato in qualità di “garante” diviene la fonte delle principali perplessità sugli effettivi benefici derivanti dall’impiego della tecnologia in contesti dove il fine ultimo è quello di “certificare” o, più impropriamente, “rassicurare” il consumatore-utente.

Inoltre, altro aspetto critico attiene al meccanismo di formazione del consenso alla registrazione.

In altre parole, mentre in un registro centralizzato sarebbe compito dell’autorità che lo amministra validare le singole registrazioni, nei registri distribuiti, dovrà individuarsi un processo che approvi a livello collettivo le singole registrazioni<sup>12</sup>. Si tratta, invero, di un problema di difficile soluzione, che fino ad oggi ha reso poco conveniente l’adozione di registri di tipo distribuito, preferendo il più sicuro sistema del registro centralizzato, garantito da una autorità centrale.

I registri distribuiti coesistono, quindi, con il difficile scoglio della creazione di un meccanismo di consenso distribuito, che consenta di evitare che singole registrazioni si accavallino oppure che si disponga più volte delle medesime risorse.

A ciò si aggiunge il correlato problema della (mancata) remunerazione del sistema di consenso, laddove, la collettività investita del compito di validare le transazioni inserite nel registro, necessita di un incentivo economico, o comunque di un meccanismo compensativo tale da non far cessare l’interesse alla corretta manutenzione dei registri.

Ad oggi le criticità illustrate non sono oggetto di regolamentazione, forse proprio per evitare che la costante evoluzione delle tecnologie e delle loro applicazioni, non rimanga imbrigliata in schemi eccessivamente rigidi. Tuttavia, in un prossimo futuro pare auspicabile che la normativa possa meglio chiarire i profili soggettivi e oggettivi dei partecipanti ai meccanismi di consenso, andando a meglio definire le “regole d’ingaggio”.

Alla luce di queste prime osservazioni, si sarà compreso come l’impiego della tecnologia *blockchain* nei sistemi di tracciabilità rappresenta una

---

<sup>12</sup> All’interno della *blockchain*, i consensi, in estrema sintesi, possono essere ottenuti attraverso il sistema del Proof-of-Work (PoW) e del Proof-of-Stake (PoS). Nella prima ipotesi, il consenso si ottiene attraverso il c.d. “mining” che consiste nell’analisi di specifiche funzioni matematiche (funzioni di hash). Nel caso in cui si utilizzi il sistema del Proof-of-Stake, invece, il consenso è ottenuto attraverso il c.d. “staking”, con il quale i partecipanti alla rete che vogliono essere coinvolti nella verifica della validità delle transazioni e nella creazione di blocchi nella rete devono detenere una certa quota nella rete, per esempio mettendo una certa quantità di moneta della rete in un portafoglio collegato alla sua *blockchain*. Per una disamina si segnala: F. GALANTI, *Introduzione ai sistemi di consenso: Proof-of-Work e Proof-of-Stake*, disponibile al sito: <https://medium.blockchainedu.net/introduzione-ai-sistemi-di-consenso-proof-of-work-proof-of-stake-e6564ddad6aa>.

componente dall'elevato potenziale innovativo, inserita in un sistema ben più ampio ed in costante evoluzione, la cui tenuta, andrà verificata di settore in settore.

## 2.1. Tracciabilità quale leva pro-competitiva: aspetti positivi nell'impiego della *blockchain* per i consumatori e per le imprese

Una solida tracciabilità di filiera non è solo un valore aggiunto per competere sul mercato (comunicando qualità e origine), elementi storicamente correlati alla *ratio* stessa della funzione del marchio, ma è anche la chiave per una più efficiente gestione dei rapporti organizzativi alla base dell'attività d'impresa<sup>13</sup>. Molteplici sono i riflessi pro-competitivi per le aziende. Ad esempio a livello di organizzazione interna l'impresa ottiene la tracciabilità di ogni singola unità di prodotto, il pieno controllo sulla gestione delle risorse (materie prime, trasporto) e la validità legale di una certificazione utile per la prevenzione di comportamenti illeciti da parte di terzi. A livello esterno, invece, incrementa valori strategici quali la trasparenza lungo la filiera, l'efficacia e l'efficienza dei processi di recupero dei dati in caso di situazioni critiche, l'analisi delle transazioni passate per valutare l'affidabilità dei fornitori. Non da ultimo, assicura la tutela del consumatore, sempre più sensibilizzato alla conoscenza delle informazioni riguardanti un determinato prodotto, le quali, se raccolte in maniera puntuale e dettagliata, possono rappresentare un importante valore aggiunto da poter spendere sul mercato<sup>14</sup>. La tracciabilità, offre dunque alle aziende

---

<sup>13</sup> Cfr. anche A. CHAKRABARTI, A. CHAUDHURI, *Blockchain and its Scope in Retail*, in ???, vol. 4, July 2017, 3053.

<sup>14</sup> Il Ministero dello Sviluppo Economico, a seguito di uno studio del fenomeno *blockchain* applicato ai fini di tracciabilità di prodotti made in Italy, ha evidenziato che la conoscenza sulle nuove tecnologie da parte delle aziende è ancora limitata ed è, quindi, necessario instaurare un adeguato percorso di accompagnamento per facilitare la condivisione delle *best practices*. Ha altresì sottolineato l'assenza di standard contrattuali e la necessità di utilizzo di linguaggi comuni (e valorizzando quelli già in uso nella filiera come *eBIZ* – il linguaggio standardizzato per gli scambi di dati e documenti all'interno della filiera tessile/abbigliamento/calzature) per innescare un approccio alla digitalizzazione che riesca a coinvolgere gli attori pubblici interessati. Nel progetto la *blockchain* è emersa come una tecnologia adatta per il sostegno e la valorizzazione anche del Made in Italy, ma a due condizioni: 1) che venga premiata la trasparenza, ovvero la disponibilità a fornire informazioni affidabili e complete, con meccanismi oggettivi; 2) che sia valorizzato un sistema accessibile a tutti gli attori interessati, ove autorizzati dal modello di governance della rete che potrà essere progettato; cfr. <https://www.mise.gov.it/images/stories/documenti/IBM-MISE-2019-BC.pdf>.

l'opportunità di verificare in modo credibile tutte le loro affermazioni, ad esempio circa la sostenibilità dei prodotti, innescando meccanismi di valorizzazione della trasparenza atti a rendere le imprese pro-competitive<sup>15</sup>.

In concreto, nel processo di tracciabilità viene ricompresa l'importante fase della serializzazione dei prodotti, la quale prevede l'assegnazione di un codice per qualsiasi articolo o imballo. Gli *standard* che guidano la fase di serializzazione sono, nella maggior parte dei casi, gli *standard* GS1<sup>16</sup>, il più comune è il codice a barre.

Con tale procedura, viene conferita al singolo prodotto un'identità precisa che permette di geo-localizzarlo e/o tracciarlo a partire dallo stadio di materia prima, sino alla completa integrazione con le successive fasi di lavorazione, stoccaggio, movimentazione e distribuzione del prodotto finito. Le soluzioni tecniche per la tracciabilità digitale sono molteplici<sup>17</sup> e vedono un combinato disposto di impiego di piattaforme *software*, per la registrazione dei dati e la eventuale integrazione, e di strumenti *hardware* per la loro decodificazione, come i lettori per i codici a barre, i visori, i sensori *IoT* ovvero gli smart tag.

I sistemi di tracciabilità rispondono ad un mercato della domanda a due versanti, infatti, se da un lato vi è l'azienda interessata a geolocalizzare i propri prodotti, a monitorare dove si trovano e a verificarne gli acquisti,

---

<sup>15</sup> Riflessioni che originano nel più ampio dibattito sulla funzione del marchio, e ancor più dei segni distintivi di uso collettivo, cfr. M. LIBERTINI, *Marchi collettivi e marchi di certificazione, funzioni e problemi della disciplina dei segni distintivi di uso collettivo*, in *Riv. dir. ind.*, 2019, 466-470. Per un approfondimento in tema di trasparenza e sostenibilità con riferimento alla raccolta e gestione dei dati si rimanda a E. DEL BUFALO, *Trasparenza informativa, sostenibilità ed integrazione nelle supply chain globali*, in AA.VV., *Fairness e innovazione nel mercato unico digitale*, a cura di V. Falce, Torino, 2020, 121.

<sup>16</sup> GS1 è un'organizzazione non profit che sviluppa e mantiene standard globali per la comunicazione tra imprese. Il più noto fra questi standard è il codice a barre, un simbolo grafico stampato sui prodotti che può essere scannerizzato elettronicamente. Gli standard GS1 sono il linguaggio comune per identificare, catturare e condividere le informazioni lungo la supply chain e assicurano che le informazioni importanti siano accessibili, corrette e facilmente comprensibili.

<sup>17</sup> Tra i sistemi di tracciabilità più diffusi vi sono quelli che sfruttano il QRCode e la tecnologia Rfid. In particolare, grazie a una semplice scansione dallo smartphone del QR Code si potrà visionare il certificato di tracciabilità; la tecnologia Rfid è invece un sistema di identificazione a radiofrequenza con il quale si assicura che il prodotto non sia stato oggetto di contraffazione, visto che solo la merce uscita dall'azienda in questione è dotata del c.d. tag Rfid abbinato, costituito da una sorta di codice fiscale univoco e irripetibile.

Cfr. TAPAN B., *How Blockchain Solves the Supply Chain Problems Using RFID Techniques*, 2022, disponibile su SSRN: <https://ssrn.com/abstract=4287240> or <http://dx.doi.org/10.2139/ssrn.4287240>.

dall'altro lato vi sono i consumatori interessati ad avere garanzie di qualità ed a conoscere gli standard di realizzazione.

La tracciabilità dei prodotti ha visto nell'impiego della tecnologia *blockchain* nuovi fronti di opportunità, per le aziende e per i consumatori, derivanti dalla puntuale raccolta e memorizzazione delle informazioni su tutte le componenti di un prodotto, così come su tutte le pratiche di approvvigionamento dei fornitori e di tutti i vari operatori esterni coinvolti nei processi di lavorazione.

Uno dei settori in cui la *blockchain* riveste ormai un'importanza fondamentale è quello agroalimentare. Il suo utilizzo e, soprattutto, la tracciabilità che ne deriva risulta ormai imprescindibile in tale settore perché consente di tenere traccia degli spostamenti degli alimenti nei diversi stadi della filiera che partono dal produttore fino al consumatore, inoltre, consente di migliorare la gestione dei processi di richiamo prodotti e contraffazione.

L'impiego della tecnologia blockchain richiede necessariamente un'integrazione con le tecnologie *IoT* per evitare errori. Infatti, se è vero che le soluzioni *IoT* collegano il mondo fisico con quello digitale, acquisendo dati come la temperatura e l'umidità durante il trasporto o lo stoccaggio del prodotto, dall'altro lato la *blockchain* fornisce una piattaforma sicura e (quasi) immutabile in cui questi dati possono essere archiviati e resi accessibili a ogni attore coinvolto nella catena di approvvigionamento<sup>18</sup>.

Per tutelare l'integrità dei prodotti alimentari è fondamentale scegliere una struttura informatica sicura per evitare furti di dati e alterazioni da terze parti, motivo per cui si guarda sempre più alle piattaforme *digital ledger* accessibili da chiunque e in grado di garantire attendibilità e affidabilità dei dati.

---

<sup>18</sup> Esempi concreti di industrie del settore alimentare che hanno implementato nei loro sistemi la tecnologia basata sulla *blockchain* sono, ad esempio, Barilla, Carrefour, Nestlé. Il produttore di pasta e food italiano, Barilla, in collaborazione con IBM ha affrontato il tema della trasparenza e della tracciabilità nel suo ciclo di produzione del pesto: dalla coltivazione, al trattamento, alla raccolta, fino al trasporto, allo stoccaggio, al controllo di qualità e infine alla distribuzione, tutti i dettagli sono tracciati e resi disponibili su un sistema di blockchain che il cliente può verificare scansionando il codice QR del pesto. Dalla collaborazione di Nestlé e OpenSc (società co-fondata da WWF e BCG *Digital Ventures*) è scaturita una piattaforma *blockchain* in grado di tracciare il latte delle fattorie e dei produttori dalla Nuova Zelanda fino alle fabbriche e ai magazzini Nestlé in Medio Oriente, testimonianza dell'impegno dell'azienda per favorire la trasparenza. Di fatto, il colosso svizzero vuole che i propri consumatori prendano decisioni informate e, in quest'ottica, utilizza la tecnologia *blockchain* per condividere informazioni affidabili con gli stessi. Inoltre, dal 2017, Nestlé tramite la piattaforma IBM *Food Trust* ha introdotto la possibilità di fornire tutte le informazioni relative ai prodotti tracciati.

La tracciabilità, come si diceva, non è l'unico vantaggio apportato dalla tecnologia *blockchain*, vi sono anche vantaggi economici, tra cui la possibilità di impiego della *blockchain* come leva antifrode, economica e sostenibile. Considerando che un prodotto alimentare su dieci risulta adulterato o etichettato in modo errato, grazie all'impiego della *blockchain* si possono facilmente individuare i prodotti difettosi e isolarli, evitando costosi richiami generalizzati di prodotti.

In tal senso, al netto dell'auspicabile miglioramento dell'assetto regolamentare, e della verifica di una serie di garanzie tecniche, allo stato non verificabili, le tecnologie basate su registri distribuiti, pare possano comunque garantire un elevato grado di supporto nell'identificazione e tracciamento di prodotti, configurandosi come strumento potenzialmente affidabile, quantomeno rispetto alla gestione analogica e centralizzata di dati, e ben spendibile per la promozione sul mercato dell'attività dell'impresa.

Per questa ragione l'utilizzo di soluzioni *blockchain-based* finalizzate alla tracciabilità di filiera, ha mostrato quale primario obiettivo quello di garantire specifiche qualità dei prodotti e prevenire le frodi soprattutto nella filiera alimentare, nella moda e nella grande distribuzione<sup>19</sup>. Le soluzioni *blockchain* sono state prescelte anche stante la capacità di gestire, a basso costo, un'enorme quantità di dati, che poi rappresenta la chiave per un'efficace e veritiera tracciabilità.

Sul punto giova però far notare come i casi studio esaminati, afferenti al mondo dell'agroalimentare, mostrano l'impiego della tecnologia da parte di ciascun gruppo aziendale al fine di efficientare la tracciabilità di filiera (ricostruzione del percorso, tracciabilità e rintracciabilità<sup>20</sup>), tuttavia, allo stato pare i tali sistemi scelti mantengano un controllo accentrato e un potere di verifica solamente in capo all'azienda.

Se dunque sono comprensibili le ragioni che hanno spinto gli *stakeholders* a mostrare grande interesse nell'utilizzo di detta tecnologia all'interno delle attività d'impresa, ponendo fiducia nella garanzia di immutabilità delle informazioni promessa, anche *ex lege*, dalle soluzioni *blockchain-based*, va ricordato che la garanzia di immutabilità resta discutibile<sup>21</sup>, in quanto i

---

<sup>19</sup> Non a caso le filiere che maggiormente offrono esempi di utilizzo della tecnologia *blockchain* sono quelle che sono state spesso caratterizzate da richiami di prodotto a causa di contaminazioni e rischi per la salute.

<sup>20</sup> Vedi *supra*, nota 3.

<sup>21</sup> Anche le note *blockchain* pubbliche quali Bitcoin ed Ethereum, possono essere alterate con il consenso della maggioranza dei nodi e, perciò, esposte ai c.d. "attacchi del 51%".

sistemi ad oggi teorizzati rendono difficile, ma non impossibile, un'alterazione del registro distribuito.

## 2.2. Test per la verifica dei limiti nell'applicazione della tecnologia

Attenzione però a non travisare il valore della *blockchain*. La sua tecnologia applicata alla tracciabilità in una filiera produttiva, infatti, dovrebbe garantire che i dati condivisi e gestiti al suo interno non possano essere modificati, ma certamente non garantisce la veridicità del dato iniziale<sup>22</sup>.

Con riferimento a quanto detto, pare evidente che la *blockchain* non può rappresentare uno strumento di “certificazione” di un determinato prodotto, bensì un valido metodo di memorizzazione e gestione di dati e informazioni dettagliate. Difatti, qualora venisse registrata un'informazione sbagliata, quest'ultima rimarrebbe tale anche all'interno del registro *blockchain* utilizzato.

La *blockchain* sembra spesso poter divenire una soluzione alla ricerca di un problema e per questo è bene prestare attenzione e tenere a mente quali sono i criteri da seguire per decidere se l'opzione *blockchain* possa essere davvero utile:

1. Si vuole creare un database condiviso con altri attori e organizzazioni, e mettere in comune le informazioni che si stanno raccogliendo nel database?
2. Si richiede che gli attori del sistema possano scrivere in parallelo sul database?
3. Si ritiene necessario registrare in maniera immutabile tutta la storia delle modifiche impedendo a chiunque (incluso se stessi) di aggiustare o cancellare i valori passati?
4. Si vuole evitare a tutti i costi che un intermediario fidato operi sul database eseguendo comandi per nostro conto?
5. Le transazioni eseguite dai vari attori interagiscono tra loro, creando interdipendenze tra i dati?

Se almeno una delle cinque domande ha ricevuto risposta negativa allora sicuramente si può risolvere il problema con una tecnologia più sempli-

---

<sup>22</sup> È solo grazie all'Identificazione univoca automatica associata all'uso di sensori e tag RFID/NFC che la *blockchain* può abilitare applicazioni ancora più estese, fondate su una gestione delle informazioni certa e garantita all'insegna della trasparenza end-to-end.

ce e con migliori performance rispetto alla *blockchain*<sup>23</sup>. Se invece tutte e cinque le domande hanno ricevuto risposta positiva, la *blockchain* potrebbe essere la soluzione da prediligere.

Se un settore giunge alla conclusione che il ricorso a un registro distribuito assicura un livello di affidabilità e verifica non ottenibile con i meccanismi tradizionali di condivisione dei dati, allora sarà necessario vagliare altri due fronti che non si approfondiranno in questa sede, ovvero l'interoperabilità delle soluzioni di tracciabilità basate sulla *blockchain* e i costi.

### 3. Per un'ipotesi evolutiva della funzione: dal marchio di certificazione alle "certificazioni" *blockchain-based*

Guardando al sistema dei marchi in generale e nello specifico a quello dei marchi di certificazione<sup>24</sup>, la tecnologia *blockchain* potrebbe in un futuro prossimo svolgere un ruolo di rafforzamento dell'effettività delle funzioni cui questi segni risultano preposti<sup>25</sup>.

Se *blockchain* è definibile quale condivisione di dati ed informazioni distribuite a catena in un ordine cronologico, auspicabilmente immutabile, questo sistema potrebbe contribuire al rafforzamento di talune procedure di certificazione che determinano l'origine ed il procedimento di formazione di prodotti o servizi.

Il processo di archiviazione generato da una tecnologia *blockchain* contribuirebbe quindi a favorire l'ingresso anche delle PMI in un circolo pro-concorrenziale virtuoso che, come è si è già detto, influirebbe in maniera preponderante anche sul progresso tecnologico. Difatti, da un lato, il si-

---

<sup>23</sup> Il test prende spunto dall'articolo di GREENSPAN G., *Do you really need a blockchain for that?*, 2019, disponibile al sito <https://www.coincenter.org/education/crypto-regulation-faq/do-you-really-need-a-blockchain-for-that/>.

<sup>24</sup> Con riguardo alle funzioni del marchio di certificazione e collettivo e al loro rapporto con il marchio individuale, all'indomani della riforma del 2019, si rimanda a C. GALLI, *Marchi collettivi, marchi di certificazione, marchi individuali ad uso plurimo e denominazioni geografiche dopo le novità normative del 2019*, in *Il Diritto industriale*, n. 1, Milano, 2020, 97-98. Cfr. anche G. IUFRIDA, *I segni distintivi*, in AA.VV. (a cura di G. Oliveri, A. Genovese), *Trattato Omnia "Proprietà Intellettuale"*, Utet Giuridica, Milano, 2021, 49.

<sup>25</sup> L'analisi la si potrebbe contestualizzare alla luce delle riflessioni generali in tema di promozione delle creazioni e limiti dell'esclusiva, valutando se l'impiego della *blockchain* possa da un lato rafforzare l'esercizio dell'esclusiva, ma al contempo renderla più "democratica" laddove vagliata da un sistema di consenso su larga scala. Sul punto si suggerisce di ripartire dall'analisi di M. LIBERTINI, *Tutela e promozione delle creazioni intellettuali e limiti funzionali della proprietà intellettuale*, in *AIDA*, 2014, 321 ss.

stema *blockchain* consente di tracciare in maniera immutabile i procedimenti di realizzazione di un prodotto o servizio, contribuendo a creare certezza e fiducia nei consumatori; dall'altro, avrebbe un naturale valore comunicativo, in quanto veicolerebbe un messaggio positivo tra i consumatori e le imprese: un qualcosa in più che sortirebbe l'effetto di orientare i primi verso scelte di mercato sempre più rispondenti a nuovi bisogni e, di conseguenza, le seconde ad investire sulle caratteristiche innovative dei prodotti e servizi, comprese quelle attualmente più in voga dell'etica e della sostenibilità ambientale<sup>26</sup>.

Con la direttiva UE n. 2436/2015, recepita nel nostro ordinamento con d.lgs. 20 febbraio 2019, n. 15, in vigore dal 23 marzo 2019, sono state introdotte rilevanti modifiche in tema di segni distintivi: in particolare è stata modificata la previgente disciplina del marchio collettivo, distinguendolo in marchio collettivo e marchio di certificazione<sup>27</sup>. Il primo è uno segno distintivo che nasce per poter essere utilizzato da una pluralità di soggetti indipendenti, il cui obiettivo è quello di ricollegare i prodotti che ne sono contraddistinti non all'imprenditore singolo, ma al gruppo, che si fa "garante" delle particolari caratteristiche qualitative indicate in un apposito Regolamento (il disciplinare di produzione); il secondo, invece ha lo scopo di attestare l'esistenza di determinate caratteristiche dei prodotti in quanto tali e dei procedimenti di fabbricazione, secondo un regolamento specifico (il regolamento d'uso), che deve essere depositato insieme alla domanda di marchio; in questo caso è un soggetto privato a fungere da garante dei requisiti verificati<sup>28</sup>.

---

<sup>26</sup> Tra le altre, dunque, la tecnologia *blockchain* potrebbe essere idonea a dimostrare la conformità di determinati prodotti rispetto a politiche di sostenibilità ed ambientali e, in definitiva, utile all'acquisizione e registrazione di dati informativi sull'origine, qualità, sostenibilità etica di un prodotto offerto al pubblico dei consumatori. Ora, con quello che potrebbe sembrare un eccesso di zelo, si potrebbe sostenere che in futuro il sistema della *blockchain* e la proprietà industriale – i.e. in particolare, i marchi di collettivi e di certificazione – potrebbero agire all'unisono a favore dell'ottimizzazione di pratiche di sostenibilità ambientale con importanti ricadute anche a livello di mercato. Per meglio contestualizzare il perimetro di interferenza tra funzione dei marchi e relativo impatto nel mercato, si rimanda a C. GALLI, *Protezione del marchio e interessi del mercato*, in AA.VV., *Studi in onore di Adriano Vanzetti*, Milano, 2004, 661 ss.

<sup>27</sup> Per un esame più dettagliato dell'impatto della riforma si veda C. GALLI, *Marchi collettivi, marchi di certificazione, marchi individuali ad uso plurimo e denominazioni geografiche dopo le novità normative del 2019*, in *Il Diritto industriale*, n. 1, cit.

<sup>28</sup> Il Regolamento sul marchio UE definisce i marchi di certificazione UE come marchi "idonei a distinguere i prodotti o i servizi certificati dal titolare del marchio in relazione al materiale, al procedimento di fabbricazione dei prodotti o alla prestazione del servizio, alla qualità, alla precisione o ad altre caratteristiche, a eccezione della provenienza geografica, da prodotti e servizi non certificati" (art. 83, par. 1, RMUE). Questa definizione coincide solo in parte con quella adotta-

Cuore della disciplina è l'obbligo di neutralità cui il soggetto certificato dovrà conformarsi. Infatti, sebbene qualsiasi persona fisica o giuridica, tra cui istituzioni, autorità e organismi di diritto pubblico, possono presentare domanda di marchio di garanzia o di certificazione, la condizione da rispettarsi è che detta persona non svolga un'attività che comporti la fornitura di prodotti o servizi del tipo certificato. Il titolare di un marchio di certificazione non può dunque gestire un'attività che comporti la fornitura di prodotti e servizi del tipo certificato. Il rationale della norma sta nel tentativo di scongiurare il conflitto d'interesse che si ingenererebbe nella sovrapposizione soggettiva della figura di vigilante con quella di vigilato. Tale ipotesi per altro potrebbe altresì sfociare in pratiche di concorrenza sleale tra produttori consistenti in barriere di ingresso o cartelli.

La proposta evolutiva che si vuole qui ipotizzare comporterebbe una sostanziale delega alla *blockchain* delle verifiche svolte dal titolare del marchio di certificazione. In pratica con una soluzione *permissionless* è immaginabile la predisposizione di uno *smart contract* atto a regolare la concessione delle licenze di utilizzo del segno per i produttori che ne facciano richiesta<sup>29</sup>. Un contratto che quindi prevedrebbe *ex ante* i requisiti per l'ottenimento segno di garanzia e certificazione<sup>30</sup>, e grazie all'automazione e alla trasparenza della verifica eviterebbe qualsivoglia distorsione del mercato riconducibile all'arbitrio umano. Come si è detto l'architettura della *blockchain* decentralizzata si auto-legittima prescindendo dall'intervento di una autorità<sup>31</sup>, ma trattasi di ipotesi proposta in astratto, e al netto delle perplessità già espresse circa l'inalterabilità della *blockchain*.

---

ta dall'art. 11 *bis* del Codice della Proprietà Industriale italiano. Infatti, a differenza del marchio comunitario, il marchio di certificazione italiano può essere utilizzato anche per indicare l'origine geografica di un prodotto o servizio, seppur non disgiunta dalla certificazione di altre caratteristiche. Cfr. anche M. LIBERTINI, *Marchi collettivi e marchi di certificazione, funzioni e problemi della disciplina dei segni distintivi di uso collettivo*, in *Riv. dir. ind.*, 2019, 466.

<sup>29</sup> Più diffusamente si vedano le riflessioni di G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. e proc. civ.*, (2), 2018, 441-460.

<sup>30</sup> I marchi di garanzia o di certificazione svolgono la funzione di certificare la sussistenza di determinate caratteristiche dei prodotti e dei servizi (ad esempio, la qualità), ossia – similmente ai marchi collettivi – asseverano la conformità di questi ad uno specifico regolamento (c.d. regolamento d'uso), che deve essere depositato insieme alla domanda di registrazione del marchio. Tali elementi sarebbero tutti traducibili in requisiti *ex ante* da inserire nello *smart contract*. Cfr. M. LIBERTINI, *op. cit.*, 483.

<sup>31</sup> In tal senso si rimanda a G. REMOTTI, *op. cit.*, 44-45. Secondo cui con riguardo ai marchi collettivi la *blockchain* potrebbe contribuire ad una migliore gestione del segno sia nei confronti dei consumatori, sia nei rapporti tra i soggetti autorizzati all'utilizzo del segno, ma in questo caso sarebbe da favorire un'architettura più accentrata. "Questo sistema, seppur in linea, assicurerebbe non pochi vantaggi. Così nei rapporti intercorrenti tra i diversi produttori autorizzati

In tal senso la sola soluzione *blockchain based* veramente utile per rafforzare gli attuali strumenti di tracciabilità e di certificazione dovrebbe essere proposta da un soggetto riconosciuto e riconoscibile come affidabile.

Ove, infatti, fossero le autorità preposte alla concessione dei marchi d'impresa a "programmare" lo *smart contract*, ovvero ad implementare vie di interoperabilità della tecnologia *blockchain ad adiuvandum* degli attuali processi informatici inerenti lo status delle tutele dei segni distintivi, realisticamente si potrebbero superare diverse delle ritrosie che paiono oggi limitare le proposte più ambiziose in materia e si addiverrebbe ad una nuova funzione certificativa utile in molteplici fasi della vita di un marchio d'impresa.

Interrogativo finale è dunque "digitalmente certificati" sì, ma come e da chi<sup>32</sup>? Chi si assume la responsabilità della certificazione e su chi dovrebbe poi incombere la responsabilità della manutenzione dei registri?

In dottrina si indagano, infatti, i benefici degli strumenti di *governance* totalmente decentrati, utilizzando protocolli di consenso basati su *smart contract*. Ma il modello sembra ancora di difficile integrazione con i sistemi vigenti.

Sul punto vale la pena ricordare che la stessa regolazione finanziaria ha rigettato i "DAO", perché carenti sotto il profilo della soggettività, ancor prima che della imputabilità<sup>33</sup>.

La scarna normativa in materia di blockchain esaminata in esordio pare ancora incompatibile con quei registri distribuiti che tuttavia non prevedano anche una formazione altrettanto distribuita del consenso<sup>34</sup>. Non da ul-

ad utilizzare il marchio collettivo, si potrebbe realizzare un controllo più efficiente ed economico del rispetto del disciplinare; si avrebbe altresì una riduzione dei costi di monitoraggio e di sorveglianza circa il rispetto delle prescrizioni contenute nel disciplinare determinando per conseguenza una possibile riduzione del prezzo finale del prodotto così marcato, il tutto a vantaggio anche del consumatore finale". Cfr. anche M. RICOLFI, *Trattato dei marchi*, Torino, 2015.

<sup>32</sup> Sul punto si potrebbero riproporre le considerazioni di E. BELLISARIO, *La responsabilità degli organismi di certificazione della qualità*, in *Danno e resp.*, 2011, 1079, ovvero tornare sul macro tema dell'affidamento del pubblico rispetto all'informazione merceologica convogliata dal marchio, e sul punto si rimanda integralmente a G. GHIDINI, *Profili evolutivi del diritto industriale*, Milano, 2015, 341 ss.

<sup>33</sup> Decentralized autonomous organization, in sigla DAO (*Organizzazione autonoma decentralizzata*), talvolta anche decentralized autonomous corporation (DAC) è una organizzazione la cui attività ed il cui potere esecutivo sono ottenuti e gestiti attraverso regole codificate, attraverso *smart contract*.

<sup>34</sup> Cfr. M. MANENTE, *op. cit.*, conclude evidenziando come "se lo *smart contract* deve essere fonte di obbligazione e di vincolo per le parti, esso non può certo essere collocato all'interno di un registro su cui "qualcuno", non dotato (ex lege) dei requisiti di garanzia e terzietà di norma riconosciuti allo Stato, abbia facoltà e poteri di intervento o modifica; il potenziale danno per il cittadino sarebbe evidente. Insomma, la garanzia del cittadino o proviene dallo "Stato", attra-

timo resta aperto il tema della possibile pluralità e coesistenza di *blockchain*, e dell'assenza di strumenti per capire quale sia quella "certificata". Di qui la necessità di individuare soluzioni tecnologiche che possano fare al caso delle esigenze di certezza che il sistema richiede.

## 4. Conclusioni

Con l'intento di vagliare sommariamente le più recenti interazioni tra tecnologia *blockchain* e determinati settori del comparto industrialistico dei marchi d'impresa e della grande distribuzione, sono state messe a fuoco opportunità e problematiche sottese agli sviluppi dell'applicabilità della tecnologia ai sistemi di tracciabilità e ai marchi di certificazione.

Come prima conclusione senz'altro si ritiene necessario, affinché la tecnologia *blockchain* possa integrarsi e contribuire proattivamente alla gestione dei diritti IP *tout court*<sup>35</sup>, che divenga affidabile e scalabile, che vi sia dunque un insieme di standard concordati e supportati anche a livello internazionale. Utile in tal senso potrebbe essere la redazione di linee guida con indicazione di standard contrattuali e utilizzo di linguaggi comuni per lo scambio di dati e documenti all'interno delle filiere.

Inoltre, è fondamentale che le autorità di regolamentazione e le amministrazioni competenti in materia di marchi, collaborino per contribuire all'implementazione di questa tecnologia a sostegno e semplificazione degli attuali procedimenti di tutela (es. depositi, prove d'uso, disciplinari, ecc.), assicurandone l'affidabilità della certificazione; per far questo, ad oggi, parrebbe praticabile solo l'impiego del modello più accentratore così detto *permissioned ledger*.

---

verso il ricorso ad una autorità statale (Agenzie delle Entrate, Anagrafe, ecc.) come avviene negli attuali registri centralizzati, oppure dovrà provenire dalla "collettività" attraverso la realizzazione nel registro distribuito di una sorta di esercizio diretto del potere democratico. Se tale è la ricostruzione, tuttavia, emerge in tutta evidenza un'ulteriore lacuna del dettato normativo: poiché abbiamo sopra chiarito che la garanzia di inalterabilità ed immutabilità di un registro distribuito dipende direttamente dalla sua maggiore o minore diffusione, quanto deve essere distribuito un registro affinché sia considerato affidabile?"

<sup>35</sup>Per proseguire l'indagine con interrogativi critici, si rimanda a M. TOLUWABORI, *How Blockchain Technology Is Reshaping International Trade in Goods: Its Disruptive Effect and How International Law Is Responding*, 2018, accessibile su; SSRN: <https://ssrn.com/abstract=3626401> or <http://dx.doi.org/10.2139/ssrn.3626401>: "There is a lack of governance structure in the block-chain terrain. Due to this, many companies are less willing to take the risk to adopt a technology that has no adequate governance structure". From the legal perspective, there are questions such as "Is a smart contract legally binding? Can it give rise to a legally binding contractual relation under the law?"



Marco Macchia

## **Il Digital Finance Package e l'elogio della regolazione**

SOMMARIO: 1. La digitalizzazione nel settore finanziario. – 2. L'impiego dei big data nel settore finanziario. – 3. Le regole di funzionamento delle cripto-attività a tutela degli utenti. – 4. La concorrenza tra diversi strumenti finanziari digitali. – 5. La centralità della dimensione pubblicitaria.

### **1. La digitalizzazione nel settore finanziario**

Nei tempi attuali di big data, piattaforme, social network, il mondo del digitale sembra rappresentare la nuova frontiera della politica industriale. Grazie al trattamento di grandi masse di dati, connotati da velocità, varietà e volume, gli algoritmi possono rivelarci correlazioni e causazioni. Possono rivelare relazioni tra scelte, comportamenti, gusti e azioni al punto da costruire modelli predittivi di domanda e offerta di prodotti e servizi. Al crescere della dimensione del mercato del digitale si riduce lo spazio per il mercato dei beni forniti in modo tradizionale. Ne deriva che oggi quasi tutto è veicolato tramite il mercato digitale, polarizzando la domanda e distorcendo i consumi abituali<sup>1</sup>.

Ciò solleva la questione delle regole. Le regole disegnate per governare il vecchio mercato non paiono più adeguate a mitigare i rischi derivanti dall'uso di algoritmi predittivi o di apprendimento automatico. E le regole private, decise dalle grandi piattaforme, frutto di autoregolamentazione, in risposta al proprio modello di business e ai propri codici di condotta, non

---

<sup>1</sup>Basti vedere il rapporto dell'Osservatorio sull'intelligenza artificiale del Centro Comune di Ricerca della Commissione europea e OCSE, *National strategies on Artificial Intelligence: A European perspective*, 2021. Sul tema, C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. eur.*, 2019, 101 ss.

soddisfano la neutralità dell'offerta e della domanda, perché sono selettive ossia spingono o rendono più facile la fruizione di alcuni contenuti rispetto ad altri. Per queste ragioni la Commissione Von der Leyen ha avviato una grande stagione riformatrice nel tentativo di regolare per la prima volta qualcosa che finora non era mai stato regolato, quella prateria del nuovo mondo finora accompagnata non dall'assenza di regole, ma da regole selettive espressione dell'autonomia dei privati<sup>2</sup>.

Del resto, quando l'innovazione tecnologica è applicata alla finanza la dimensione delle fattispecie e della sua regolazione non può che assumere una dimensione sovrastatale, risultando sganciata da sedi fisiche e richiedendo una risposta forte europea. «Approcci nazionali divergenti non permettono, infatti, il consolidamento di un *level playing field* e ledono gli interessi di imprese, intermediari e investitori, ostacolando la creazione di un vero mercato unico e agevolando paesi terzi che si siano dimostrati attivi nel settore»<sup>3</sup>.

Il pacchetto per la finanza digitale (*Digital Finance Package*), adottato dalla Commissione nel 2020, sembra rispondere a questo scopo: *a Europe fit for the digital age*. L'idea è quella di spostare l'attenzione sulla dinamica della competitività a livello europeo, cercando di conciliare la regolazione degli algoritmi con lo sviluppo della finanza digitale in un'ottica di tutela dei consumatori e dei cittadini europei nella nuova economia dei dati<sup>4</sup> e di protezione della stabilità del sistema finanziario. I pilastri del *Digital Finance Package* sono noti. Ne fanno parte due strategie, una per la finanza digitale *Digital Finance Strategy* disegnata per sostenere la finanza data-driven, una per i pagamenti al dettaglio (*Retail Payments Strategy for the EU*). Nonché due proposte di regolamento, una dedicata ad un quadro normativo sulle crypto-attività e sulle infrastrutture di mercato basate sulla tecnologia di registro distribuito (Regolamento MiCA), e una proposta di regolamento per un quadro normativo sulla resilienza operativa digitale nel sistema finanziario (DORA)<sup>5</sup>.

---

<sup>2</sup> U. VON DER LEYEN, *Un'Unione più ambiziosa. Il mio programma per l'Europa. Orientamenti politici per la prossima Commissione europea 2019-2024*, 16 luglio 2019; nonché Comunicazione della Commissione europea su "L'intelligenza artificiale per l'Europa", COM(2018)237 final, 25 aprile 2018.

<sup>3</sup> V. FALCE, A. SCIARRONE ALIBRANDI, F. ANNUNZIATA, M. RABITTI, M. SIRI, *Intelligenza artificiale e FinTech*, in *Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione*, a cura di F. Donati, A. Pajno, A. Perrucci, vol. III, Bologna, 2022.

<sup>4</sup> La Commissione europea ha, infatti, proposto un riesame della direttiva relativa ai crediti al consumo, garantendo una coerenza sistematica tanto con il pacchetto relativo alla direttiva sui servizi digitali quanto con la proposta di regolamento in relazione all'armonizzazione dell'uso dell'intelligenza artificiale e il *Digital Finance Package* nel suo complesso.

<sup>5</sup> L'Expert Group on Regulatory Obstacles to Financial Innovation ("ROFIEG"), istituito

Già da questo sommario quadro è evidente come l'impegno del legislatore europeo si concentri sugli effetti prodotti dallo sviluppo della digitalizzazione in ambito monetario, in risposta al timore che si sviluppino in modo incontrollato valute digitali "private", sebbene le stesse non siano sostituti della moneta legale. Il fenomeno riguarda sia i token di criptovaluta basati su blockchain decentralizzate (come bitcoin, ethereum, ecc.), i quali hanno registrato una crescita particolarmente intensa e progressiva, assicurando la possibilità di effettuare investimenti nella garanzia dell'anonimato delle transazioni, sia le *stable coin*, come ad esempio DIEM (ex progetto Libra)<sup>6</sup>, che sono oggetto di più recente definizione e sono volte a introdurre vere e proprie *valute alternative* a quelle legali per lo sviluppo di sistemi di pagamento "privati" non assoggettati a controlli<sup>7</sup>. Pur presen-

---

dalla Commissione europea nel 2018 per accertare l'idoneità del quadro giuridico e normativo dell'Unione europea al fine di permettere lo sviluppo del FinTech raccomandava l'adozione di una serie di misure incentrate su quattro macro-aree: a) la gestione dei rischi legati all'utilizzo di tecnologie innovative come l'intelligenza artificiale e la tecnologia di contabilità distribuita ("distributed ledger technology – DLT"), rischi da affrontare in una prospettiva fortemente trasversale e non limitata al settore finanziario; b) la riduzione della frammentazione nel mercato unico digitale e la conseguente armonizzazione della normativa a livello UE, al fine di garantire parità di condizioni ai diversi operatori del settore finanziario nell'utilizzo delle nuove tecnologie; c) l'adeguamento del quadro normativo dell'UE per facilitare l'innovazione digitale attraverso il contemperamento tra le opportunità offerte dal FinTech e la protezione dei dati; d) la valutazione del potenziale impatto della Fintech sui consumatori, sia dal punto di vista dell'inclusione finanziaria che dell'uso etico dei dati.

Come messo in luce da V. FALCE, A. SCIARRONE ALIBRANDI, F. ANNUNZIATA, M. RABITTI, M. SIRI, *Intelligenza artificiale e FinTech*, in *Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione*, cit., emerge sia la proposta di regolamento MiCA per un quadro normativo dell'UE sui cripto-asset (intesi come "una rappresentazione digitale di valori o diritti che possono essere archiviati e scambiati elettronicamente"), che la proposta di regolamento sulle infrastrutture DLT volta a introdurre un c.d. approccio "sandbox" per le infrastrutture di mercato basate su tecnologia a registro distribuito, consentendo deroghe temporanee alle norme esistenti per favorire l'acquisizione di esperienza dei regolatori.

<sup>6</sup>Nel giugno del 2019 Facebook ha pianificato l'emissione di un sistema di pagamenti globale basato sulla *stable coin* Libra (ora Diem), una criptovaluta privata basata su tecnologia DLT con valore replicante l'andamento del dollaro, tale da presentare alcune caratteristiche delle *fiat crypto-currency*.

<sup>7</sup>Nell'ultimo decennio il mercato dei cripto-asset è stato attraversato da una crescita esponenziale. Basti pensare che dall'emissione del primo Bitcoin nel gennaio 2009, sono state decine di migliaia le emissioni di nuovi asset digitali che hanno modificato i mercati finanziari globali. Allo stato sono quasi 19.000 i cripto-asset in circolazione, di cui la quasi totalità funzionanti con tecnologia Distributed Ledger Technologies con una capitalizzazione di mercato di circa 1.800 miliardi di dollari. Contestualmente, tuttavia, quasi 2.300 progetti di cripto-asset sono falliti in questi anni. Le motivazioni alla base del fallimento di un progetto sono molteplici: alcuni vengono abbandonati dallo sponsor principale, altri subiscono attacchi hacker, ma la maggior parte di essi, quasi un progetto su tre, viene creato per realizzare una frode, con il coinvolgimento

tandosi come un'alternativa al sistema finanziario, le criptovalute nascondono numerosi rischi e pericoli<sup>8</sup>.

Insomma, il settore pubblico tende significativamente ad avvicinarsi al mondo delle criptovalute con obiettivi di regolazione, e al contempo molte banche centrali stanno sviluppando la propria *Central Bank Digital Currency* (CBDC). Anche l'Europa non fa eccezione, perché l'innovazione tecnologica e lo sviluppo delle tecnologie digitali stanno ridisegnando la domanda e l'offerta di nuove forme di pagamento affinché siano efficaci, inclusivi e sicuri. Le misure sulla finanza digitale sembrano proprio fornire un supporto in tal senso per una possibile valuta digitale della BCE.

## 2. L'impiego dei big data nel settore finanziario

La governance dei dati pone una serie di sfide inedite per i regolatori, tra le quali un posto speciale è riservato agli strumenti di protezione dei consumatori e degli investitori. Il punto principale è che questa sfida deve essere affrontata considerando un accorciamento progressivo dei cicli

---

frequentemente dei piccoli investitori. In argomento, V. FERRARI, *The regulation of crypto-assets in the EU – investment and payment token under radar*, in *Maastricht Journal of European and Comparative Law*, 2020, 325 ss.; C.M. STIEFMUELLER, *One born every minute: Striking the balance between promoting innovation and protecting citizens. An analysis of the EU Digital Finance Package*, James Pieper, 2021, 44; D.A. ZETZSCHE, F. ANNUNZIATA, D.W. ARNER, R.P. BUCKLEY, *The markets in crypto-assets regulation (Mica) and the EU digital finance strategy*, European Banking Institute, 2020, 2.

Deve aggiungersi che finora l'approccio alla regolamentazione in materia delle autorità europee è stato caratterizzato dalla scelta di formulare una disciplina *ad hoc* solo per alcune specifiche tipologie di cripto-asset, optando per integrare altre tipologie di asset digitali nelle discipline vigenti e una non regolamentazione in tema soprattutto di cripto-valute, categoria nella quale rientra anche il fenomeno più controverso del fintech, il Bitcoin.

<sup>8</sup>È importante comprenderne il meccanismo di funzionamento. «Come l'oro, un bitcoin va "estratto", o guadagnato; lo si estrae registrando per primi un "blocco" di transazioni. Un "miner" (un proprietario di computer con forte potenza di calcolo) propone un blocco di transazioni da registrare e aggiungere alla catena, o blockchain. Quel blocco serve come input in una funzione che genera un numero ("hash") tra miliardi di possibili combinazioni. Si pensi a un dado con miliardi di facce: ogni lancio del dado genera un hash. Il primo miner che ottiene un hash inferiore ad una soglia (basata sul numero di miner che interagiscono nella rete) registra il blocco e ottiene il premio (attualmente 6,25 bitcoin).

Quindi ogni volta che un miner propone un nuovo blocco si scatena una gara tra computer per essere il primo a generare un hash sotto la soglia minima. Le possibili combinazioni sono così tante che in media ci vogliono decine di trilioni di tentativi da tutti i computer partecipanti prima che qualcuno registri un blocco. E più sono i miner più la difficoltà aumenta e con questa i tempi di calcolo», così in T. BOERI, R. PEROTTI, *Bitcoin & Co. le antimonetie liberano solo i criminali*, in *La Repubblica*, 15 febbraio 2023.

temporali e dei tempi decisionali che caratterizzano il contesto odierno. Se prima si avevano a disposizione diversi anni per adattare processi e persone alle nuove tecnologie e alle relative applicazioni, ora è molto ridotto il margine per agire, formare il personale e aggiornare le competenze di chi deve guidare il cambiamento. Si tratta di una “trasformazione compressa”.

L'insieme di dati che riguardano gruppi di utenti sono considerati alla stregua di una risorsa essenziale necessaria per l'accesso al mercato, data la dominanza dei mercati intermediati dalle grandi piattaforme digitali. Per non limitare la libertà d'impresa, la Proposta di Regolamento sull'intelligenza artificiale<sup>9</sup> considera il *credit scoring*, ossia l'impiego degli algoritmi sul mercato del credito, un sistema ad alto rischio dato l'impatto dello stesso sui diritti fondamentali. La conseguenza di tale qualifica sta principalmente nel divieto di usare un sistema interamente automatizzato che sia privo di meccanismi di sorveglianza umana. In particolare, la normativa richiede requisiti di qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza, i quali sono strettamente necessari per attenuare i rischi per i diritti fondamentali e la sicurezza posti dall'intelligenza artificiale<sup>10</sup>. Dunque, sorveglianza, tracciabilità e qualità dei dati devono accompagnare tutti gli algoritmi predittivi a fini decisionali ad alto rischio, tra cui quelli che contengono informazioni relative al credito<sup>11</sup>.

L'approccio è sempre quello fondato sul rischio. Nel rispetto dei diritti e delle libertà individuali, la legislazione europea valorizza l'*accountability* dei soggetti che effettuano trattamenti di dati personali attribuendo altresì nuova linfa a basi giuridiche diverse, come il legittimo interesse, fondate su una “responsabilizzazione” del titolare del trattamento, nell'apertura verso gli sviluppi della tecnologia. La gestione dei dati deve, in questo quadro,

---

<sup>9</sup> Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM(2021)206 final. Sul tema, C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, n. 3.

<sup>10</sup> In argomento, V. FALCE, *Financial Innovation tra disintermediazione e mercato*, Torino, 2021; V. FALCE, A. GENOVESE, *La portabilità dei dati in ambito finanziario*, in *Quaderno Fin-Tech, Consob*, 2021; V. FALCE, J. CANNATAKI, O. POLLICINO, *Legal Challenges of Big data*, Cheltenham, UK, 2020.

<sup>11</sup> Sull'art. 14 della Proposta di regolamento sull'uso dell'AI contenente il divieto all'impiego di sistemi IA ad alto rischio in via interamente automatizzata e privi di supervisione umana, K. LAGENBUCHER, *Responsible AI-based Credit Scoring – A Legal Framework*, in *European Business Law Review*, 2020, 4, 527 ss.

avvenire in armonia con la Carta dei diritti fondamentali dell'Unione europea e il diritto derivato in materia di protezione dei dati, di tutela dei consumatori, di non discriminazione e di parità di genere. Occorre garantire, in altre parole, che le informazioni relative ai crediti siano presentate in maniera chiara e adeguata rispetto ai dispositivi digitali cui si fa ricorso, con l'obiettivo di proteggere la formazione del consenso informato da parte dei consumatori, fatta eccezione per quei sistemi di IA messi in servizio per uso proprio da fornitori di piccole dimensioni.

Oltre a creare un ponte ideale con la regolamentazione generale dell'intelligenza artificiale, il *Digital Finance Package* è diretto a rivisitare in chiave migliorativa le norme per la valutazione del merito creditizio, e quindi la capacità di un consumatore di rimborsare il credito ottenuto, nell'ottica di arginare l'annoso problema dell'indebitamento eccessivo, promuovendo l'educazione finanziaria e garantendo che sia messa a disposizione dei consumatori una preliminare e prodromica consulenza in materia di debito. Sempre sul fronte dei sistemi per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, il *Digital Finance Package* amplia il set di dati da utilizzare nella valutazione del merito creditizio, con esclusione dei dati personali sensibili – come quelli sanitari – in un'ottica di bilanciamento con i principi fondamentali a tutela della persona e con le normative di settore in merito. E con riferimento allo specifico tema della tutela dei dati del cliente-investitore, nel contesto del riesame della PSD2, la Commissione valuta l'impatto dell'autenticazione forte del cliente sul livello di frode nei pagamenti nell'Unione ed esamina se si debbano prendere in considerazione misure supplementari per affrontare nuovi tipi di frode, in particolare per quanto riguarda i pagamenti istantanei, nonché i limiti legali esistenti per i pagamenti *contactless*, al fine di trovare un equilibrio tra la loro praticità e i rischi di frode, nel più generale obiettivo di tutela del consumatore.

Ne discende che la soluzione regolatoria offerta sembra muoversi sulla linea del compromesso tra i vantaggi competitivi dell'ecosistema digitale e la tutela dei consumatori ad essere correttamente informati, valutati su dati qualitativamente validi e a far valere la "responsabilizzazione" dei titolari dei trattamenti. Un modo per salvaguardare l'innovazione senza perdere di vista i principi fondamentali a tutela della persona umana.

Lo scopo è quello di istituire uno spazio comune di dati finanziari, che garantirebbe una migliore condivisione degli stessi tra i paesi dell'Unione. La finalità di una condivisione su larga scala di dati finanziari tra i paesi europei assicurerebbe una minor frammentazione del mercato unico di capitali europei, risultando in una maggior efficienza per le imprese e i citta-

dini. Inoltre, uno spazio di dati condivisi permetterebbe alle Autorità di vigilanza europee di avere a disposizione tutte le informazioni finanziarie oggetto di vigilanza, aumentando l'efficienza della regolamentazione attraverso il perfezionamento e l'implementazione dei nuovi strumenti *Regtech* e *Suptech*, anch'essi alla base della strategia per la finanza digitale della Commissione europea. Il raggiungimento di questo obiettivo da parte della Commissione garantirebbe la formalizzazione di un sistema finanziario "aperto", con la possibilità per i consumatori di ricevere consulenze personalizzate in linea con le proprie esigenze, e per le imprese di avere maggior efficienza in termini di scambi tra aziende di paesi diversi.

### **3. Le regole di funzionamento delle crypto-attività a tutela degli utenti**

Come premesso, il *Digital Finance Package* comprende sia la definizione degli orizzonti strategici per la finanza digitale e per i pagamenti al dettaglio, sia una proposta di regolamentazione a livello europeo delle crypto-attività e della tecnologia DLT, con i due regolamenti "Markets in Crypto-Assets" e "Digital Ledger Technology". La filosofia è quella di fornire un quadro giuridico solido al fine di potenziare lo sviluppo di questi mercati, definendo chiaramente il trattamento normativo delle crypto-attività.

Una tale infrastruttura normativa sembra rispondere ad una pluralità di esigenze. Da un lato, promuove l'innovazione nell'idea che, per stimolare lo sviluppo delle crypto-attività e un più ampio ricorso alla DLT, serva istituire un quadro sicuro e proporzionato a sostegno dell'innovazione e della concorrenza leale. Ciò agevola anche investimenti nella struttura tecnologica per far funzionare la finanza digitale, che può essere notevolmente costosa. Un investimento in un sistema di pagamento per essere redditizio ha bisogno di contare su di una prevedibile "massa critica". Se la redditività dell'investimento risulta problematica si preferisce restare alle compensazioni bilaterali o limitarsi ad aderire a procedimenti di compensazione all'ingrosso.

I moderni strumenti telematici permettono di compensare debiti con crediti e, organizzati in maniera multilaterale, permettono altresì di fare sistema: una struttura organizzata di compensazione permette di compensare debiti e crediti di una pluralità di aderenti al sistema. Portata alle estreme conseguenze una serie integrata di sistemi di pagamento potrebbe condurre verso una "economia senza moneta", nella quale scompaiono sia la moneta legale che la moneta scritturale e la moneta viene ridotta ad unità di misura di compensazioni fra debiti e crediti.

Da un altro lato, serve ad arginare il fenomeno della pluralità di interventi normativi nazionali – da armonizzare successivamente – relativi al *fintech* dei singoli Stati, in particolare Malta, Francia, Germania e Lichtenstein, che avrebbero potuto creare i presupposti per pericolosi arbitraggi regolamentari<sup>12</sup>. Da un altro lato ancora, le regole di funzionamento permettono di bilanciare lo sviluppo tecnologico con l'esigenza di ricondurre lo stesso nei confini della regolazione, al fine di assicurare il rispetto di alcune garanzie inderogabili, dal momento che sviluppo e tutela non devono essere poste in contrapposizione, ma in sovrapposizione.

È fondamentale ricordare come questi strumenti di finanza digitale non possano essere lasciati all'autonomia dei privati, bensì necessitano di essere sottoposti, in tutto o in parte, ad una disciplina pubblicistica che tuteli gli investitori e gli utenti. La medioevale *lex mercatoria* o il fenomeno della *soft regulation*, cioè l'autoregolamentazione privata sollecitata da norme legislative o da atti di autorità non aventi un diretto potere normativo (ad es., autorità internazionali, come nel nostro caso la Banca dei regolamenti internazionali o le raccomandazioni dell'Unione) non paiono strumenti sufficienti per proteggere la generalità degli interessi.

Riflettendo sulle linee generali la necessità della disciplina pubblicistica deve essere individuata con riferimento al contesto di servizio (pubblico) volto a soddisfare un'esigenza fondamentale della collettività, nel caso di specie la tutela del risparmio. Date queste premesse, la presenza di un'attività di prestazione di rilievo pubblicistico giustifica la presenza di regole pubbliche a tutela della generalità degli utenti e degli interessi coinvolti.

Sebbene le cripto-attività non siano sostituti della moneta legale, i meccanismi di compensazione a cui possono dare luogo permettono di usarle come mezzo di scambio per l'acquisto di beni e servizi o con finalità di investimento. Laddove venga valorizzata questa valenza alternativa dello strumento finanziario digitale, la disciplina pubblicistica richiede che vi sia certezza nella solvibilità e nella circolazione. Garanzia che l'autonomia privata non può offrire.

Per questa ragione i tratti essenziali dell'infrastruttura di funzionamento dovranno: a) definire le specifiche tecnico-operative relative alle modalità di utilizzo del servizio; b) assicurare controlli e presidi di sicurezza dei sistemi informativi e dei dati trattati adeguati ai meccanismi di trattamento e trasmissione delle informazioni, avendo riguardo alla autenticità, integrità,

---

<sup>12</sup>F. MATTASSOGLIO, *Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario (ignorando bitcoin)*, in *Riv. dir. banc.*, aprile/giugno, 2021, 414 ss.

tracciabilità e riservatezza dell'informazione; c) garantire un livello di continuità operativa tale da consentire il regolare funzionamento del sistema interessato; d) indicare, nei contratti, livelli di servizio coerenti con tali caratteristiche. Per realizzare tutto ciò occorre un potere sovrano così come accade per la moneta legale.

Muovendo da ciò diviene chiaro come il valore aggiunto della proposta di regolamento MiCA (Markets in Crypto-asset Regulation) sta nella definizione dei contorni di mercati per le cripto-attività non assimilabili a strumenti finanziari, nei depositi (strutturati), e nella "tokenizzazione" delle attività finanziarie tradizionali in funzione di un più ampio ricorso alla tecnologia DLT nei servizi finanziari<sup>13</sup>. Oggetto della proposta sono le cripto-attività, nonché i token di moneta elettronica (art. 2) in funzione della tutela dei consumatori (art. 1, lett. d), per prevenire gli abusi di mercato e assicurare la trasparenza e la stabilità del mercato stesso. Pur essendo ancorati a distinzioni nominalistiche, si intende introdurre un quadro normativo per tutte le cripto-attività non assoggettabili alle discipline già vigenti, nonché sviluppare una precisa tassonomia per tutte le tipologie di cripto-asset oggi in circolazione.

In tale provvedimento le norme di protezione giocano un ruolo chiave mediante obblighi di informazione per gli utenti, che passano mediante la pubblicazione di "white-paper" – da cui gli emittenti più piccoli e gli utility token sono esenti – volti a informare e proteggere gli investitori. Il white paper deve includere informazioni sul progetto, sull'offerente, sui rischi, ma anche sull'impatto ambientale della tecnologia DLT utilizzata. Deve essere notificato all'autorità competente almeno venti giorni prima della sua pubblicazione. Deve essere aggiornato in caso di significativi cambiamenti e impone obblighi per l'intermediario di agire onestamente e con diligenza professionale.

Le imprese tecnologiche accedono sempre di più al settore dei servizi finanziari, ricoprendo la maggior parte delle volte il ruolo dell'interme-

---

<sup>13</sup> Come ben chiarito da V. FALCE, *Consulenza decentrata tra algo-governance ed elemento fiduciario*, in *Astrid Rassegna*, n. 17/2022, la «proposta mira a introdurre una disciplina bespoke del mercato dei cryptoasset diversi dagli strumenti finanziari. Gli aspetti fondamentali sono: i) una definizione comune di crypto-asset, con un approccio, per così dire, "catch-all", anche in funzione antielusiva; ii) la "passaportazione" delle offerte previa notifica di un white paper, nonché un regime di autorizzazione dei service provider (MiFID-like); iii) regole per l'integrità del mercato (MAR-like); iv) una disciplina più stringente degli stablecoins, ossia, in gergo europeo, degli asset reference token (ART), e degli e-money token, con una vigilanza dell'EBA su quelli significativi e un coinvolgimento forte della BCE; v) una disciplina unica delle esenzioni, ossia di ciò che non rientra nella proposta MiCAR».

diario, e quindi agendo come una vera e propria piattaforma di vendita di servizi finanziari, per operazioni come finanziamenti, prestiti o assicurazioni. Oltre alla tutela per gli investitori, emerge altresì la necessità di tutelare la stabilità del mercato: in media il grado di rischio delle cripto-attività non disciplinate dalla legislazione vigente è simile a quello degli strumenti finanziari già legiferati dalle norme dell'Unione europea<sup>14</sup>. D'altronde, mentre alcuni asset digitali sono a rischio contenuto (pur se la volatilità dei cripto-asset più scambiati sui mercati è sicuramente un tema da considerare), i cripto-asset di nuova generazione (gli stablecoin *in primis*) hanno le capacità per diventare potenzialmente sistemiche<sup>15</sup>.

#### 4. La concorrenza tra diversi strumenti finanziari digitali

In linea generale, le strategie per le nuove frontiere dei pagamenti al dettaglio e della finanza digitale condividono l'obiettivo – oltre che di creare un quadro regolamentare *innovation and digital friendly* – di consentire e sostenere l'ulteriore sfruttamento del potenziale della finanza digitale in termini di innovazione e concorrenza, attenuando allo stesso tempo i rischi.

Entro il 2024 l'Unione europea dovrà sviluppare un quadro esaustivo della tecnologia di registro distribuito e delle cripto-attività nel settore finan-

---

<sup>14</sup> Sul punto, la Commissione europea ha deciso di agire su più fronti per gestire i rischi derivanti dalle nuove tecnologie applicate alla finanza, adottando il principio “stessa attività, stesso rischio, stesse norme”. Più nel particolare, entro il 2024 si dovranno verificare i perimetri della vigilanza prudenziale e la loro conformità con i rischi derivanti dalla fornitura di servizi finanziari da parte di imprese tecnologiche e dei sempre più presenti conglomerati tecnofinanziari. In merito a tale profilo, la Commissione dovrà riesaminare la direttiva FICOD sui conglomerati finanziari, per verificarne l'ambito di applicazione anche per i conglomerati FinTech e TechFin. Per chiarezza con l'espressione imprese Fintech si intendono quelle tradizionalmente operanti nel settore finanziario che iniziano a servirsi della tecnologia come fattore produttivo per l'offerta in via esclusiva di servizi finanziari. Mentre per quelle Techfin, al contrario, si considerano le imprese originariamente attive nel settore tecnologico e che soltanto successivamente sviluppano applicativi e servizi finanziari. Sul punto, si v. D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, J.N. BARBERIS, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, in *EBI Working Paper Series*, n. 6, 2017.

<sup>15</sup> Sostituendo la moneta legale e scritturale con la compensazione fra debito e credito, alcuni strumenti finanziari digitali possono incidere sulla base monetaria e, di conseguenza, sulla manovra della base monetaria affidata alle banche centrali. Alcuni di questi sistemi, per le loro dimensioni, hanno natura sistemica, e possono riflettersi sull'andamento della base monetaria ed essere conseguentemente anche fonti di crisi economiche nel caso di cattivo funzionamento. Donde l'immediato interesse delle banche centrali a sottoporli a controlli di “stabilità”, cioè a controlli aventi finalità analoghe alla vigilanza sulle imprese bancarie e finanziarie.

ziario in grado di ridurre i rischi, ma anche di migliorare le operazioni di raccolta dei capitali delle PMI. La creazione da parte della Commissione di un quadro normativo che permetta e incentivi l'innovazione digitale in campo finanziario viene considerata una grande opportunità per favorire la BCE nel velocizzare l'attuazione di un potenziale progetto di un euro digitale<sup>16</sup>.

Ci sono tuttavia alcune sostanziali differenze tra questi strumenti da tenere in considerazione. I crypto-asset sono rappresentazioni digitali di valori o diritti, che vengono trasferiti e conservati elettronicamente. Mentre un euro digitale offrirebbe un'alternativa all'uso delle "monete stabili" per i pagamenti al dettaglio in Europa, evitando così una massiccia migrazione verso valute digitali private. Integrando (ed eventualmente assumendo) la funzione di ancoraggio del contante in euro tangibile, l'euro digitale contribuirebbe a salvaguardare il meccanismo di trasmissione monetaria e quindi il controllo della BCE sulla politica monetaria.

Un euro digitale emesso dall'Eurosistema potrebbe essere utilizzato dal pubblico nella vita quotidiana, sarebbe in altre parole un equivalente digitale delle banconote in euro. Fornendo un accesso senza costi a un mezzo di pagamento e a una riserva di valore semplici, universalmente accettati, privi di rischio di credito e affidabili, l'euro digitale potrebbe rappresentare un importante bene pubblico per i cittadini europei. La digitalizzazione della moneta potrebbe avvenire sotto forma di gettoni immateriali, registrati nel lato delle passività dei bilanci delle banche centrali, in grado di circolare nell'economia attraverso il trasferimento di questi gettoni (cioè un euro digitale basato sui gettoni). Il tema delle modalità di circolazione dell'euro digitale rappresenta, comunque, una questione cruciale. Una tra le possibilità studiate dalla BCE e dalla Commissione è l'eventualità che i cittadini aprano conti presso la stessa Banca Centrale, la quale potrebbe arrivare a gestire la quasi totalità dei pagamenti nell'eurozona, il che sarebbe in grado di procurare un danno significativo al settore bancario commerciale<sup>17</sup>.

---

<sup>16</sup> Negli ultimi mesi sono stati fatti grandi passi in avanti verso una possibile CBDC (*Central Bank Digital Currency*) della Banca centrale europea. Dopo una lunga fase di consultazione, il 14 luglio 2021 il Consiglio direttivo della BCE ha deciso di avviare la fase di indagine di un progetto sull'euro digitale della durata di due anni. Gli obiettivi di partenza dichiarati da Christine Lagarde nel *Rapporto sull'euro digitale* del 24 ottobre 2020 sono: «sostenere la digitalizzazione dell'economia europea e l'indipendenza strategica dell'UE, rispondere al significativo declino del ruolo del contante come mezzo di pagamento, creare un nuovo canale di trasmissione della politica monetaria, mitigare i rischi per la normale erogazione di servizi di pagamento, promuovere il ruolo internazionale dell'euro, e favorire il miglioramento dei costi complessivi e dell'impronta ecologica dei sistemi monetario e dei pagamenti».

<sup>17</sup> Un rischio nel passaggio all'euro digitale è quello di ridimensionare il ruolo delle banche commerciali nella creazione di moneta e nell'assunzione di depositi. In effetti, entrambe le cose

La loro natura immateriale rende le banconote digitali molto più versatili di quelle cartacee e ne consente l'utilizzo per altre funzioni, comprese alcune che potrebbero ancora non essere previste. L'emissione di un euro digitale si affiancherebbe al contante, senza sostituirlo. I cripto-asset invece si qualificano come strumenti finanziari, la loro regolazione serve a preservare la stabilità finanziaria e a proteggere gli investitori, soprattutto quelli retail. Questi asset possono servire come chiave d'accesso a un servizio, ma possono anche facilitare i pagamenti o essere anche concepiti come veri e propri mezzi finanziari. L'efficienza di entrambi dipende dalla sicurezza e dalla stabilità dei sistemi di funzionamento, nonché dagli strumenti di protezione per l'ottenimento di forme di tutela legale.

Ambedue questi strumenti possono incidere sulla base monetaria e avere effetti di politica monetaria, rappresentando un pericolo per la stabilità (monetaria). Per questa ragione, in occasione del riesame della PSD2, la Commissione appare intenzionata ad allineare i quadri della PSD2 e della EMD2 includendo l'emissione di moneta elettronica come servizio di pagamento nella PSD2. Nella proposta di regolamento sui mercati delle cripto-attività, è inoltre contenuta una iniziativa diretta a imporre agli emittenti di *token* di moneta elettronica disposizioni aggiuntive integrative della EMD2, al fine di garantire, ove necessario, collegamenti adeguati tra la vigilanza dei servizi di pagamento e la sorveglianza di sistemi, schemi e strumenti di pagamento<sup>18</sup>.

Dal punto di vista tecnico, le banconote digitali potrebbero addirittura aprire nuovi orizzonti nella conduzione della politica monetaria<sup>19</sup>. Potrebbero essere concepite in modo da consentire alla BCE di influenzare la domanda del pubblico, anche pagando o riscuotendo interessi sulle banconote digitali e imponendo limiti al loro possesso o utilizzo: ciò potrebbe migliorare la trasmissione delle variazioni dei tassi di interesse. Un interes-

---

potrebbero avere implicazioni per la stabilità finanziaria. Il passaggio dalle banche commerciali alla detenzione di tutti gli euro digitali potrebbe aumentare il costo della raccolta per le banche e comportare un aumento dei tassi di interesse sui prestiti bancari, riducendo potenzialmente il volume del credito bancario nell'economia. Sul tema, BCE, *Rapporto su euro digitale*, 2020.

<sup>18</sup> I sistemi di pagamento non sono solo un pericolo per la stabilità monetaria, sono anche delle strutture imprenditoriali la cui efficienza dipende, come per tutte le imprese, dal loro grado di concorrenzialità. E poiché la compensazione multilaterale dei debiti e dei crediti è, come la circolazione della moneta, una metastruttura dell'economia reale, è estremamente importante che i sistemi di pagamento siano sicuri ed efficienti.

<sup>19</sup> A fronte di tali innovazioni e in considerazione dei rischi a cui sono esposti i sistemi di pagamento basati sulle monete legali, le principali Banche Centrali mondiali (Cina e USA) stanno progettando lo sviluppo di una versione digitale delle monete legali: il progetto più avanzato è quello relativo allo Yuan digitale, giunto a fine 2020 alla fase di sperimentazione.

se negativo sulle banconote digitali potrebbe in circostanze estreme fornire uno stimolo monetario.

È pacifico che l'Eurosistema abbia il potere di emettere un euro digitale nell'ambito della sua funzione di emissione di moneta pubblica ai sensi dell'art. 128, par. 1, TFUE e dell'art. 16 Statuto del SEBC, sulla base dell'attuale interpretazione del Trattato. Nella sezione 3 si afferma che tali poteri europei sono necessariamente esclusivi e devono prevalere sulla competenza degli Stati membri di emettere monete metalliche tangibili ai sensi dell'art. 128, par. 2, TFUE. In altre parole, il quadro normativo vigente consente chiaramente l'emissione di un euro digitale che imiti nella sua struttura le funzioni del contante tangibile.

Ciò preclude, di converso, la possibilità di concepire l'euro digitale come strumento di politica monetaria, ad esempio come portatore di interessi. In altre parole, come il contante tangibile, l'euro digitale contribuirebbe (e dovrebbe contribuire) a salvaguardare i meccanismi di trasmissione della politica monetaria, ma non potrebbe essere utilizzato per alterare il meccanismo stesso.

Anche se l'espressione letterale "uso dell'euro" fosse interpretata in senso ampio al fine di includere l'impiego dell'euro digitale come strumento di trasmissione di impulsi monetari, il diritto derivato non potrebbe comunque aggirare le limitazioni imposte dall'art. 128, par. 1, TFUE in termini di funzioni che le banconote devono svolgere. Ne consegue, in conclusione, che unicamente una modifica dei trattati potrebbe stabilire che l'euro digitale possa servire contemporaneamente come riserva di valore e mezzo di pagamento per il pubblico, nonché come strumento di politica monetaria<sup>20</sup>.

## 5. La centralità della dimensione pubblicistica

L'impatto della transizione tecnologica e il potenziale trasformativo dell'intelligenza artificiale nel settore finanziario stanno dimostrando come sia poco praticabile affidarsi unicamente all'autonomia dei privati, ricorren-

---

<sup>20</sup> «La moneta è la passività dello Stato che ciascun cittadino ha nel suo portafoglio: la garanzia ultima della sua affidabilità è nella sostenibilità dei conti pubblici. In caso contrario, l'armonia si spezza», data la catena di relazione che esiste tra politica di bilancio e rischio inflazionistico. Ciò significa che le politiche pubbliche devono essere coerenti con una credibile prospettiva che il debito pubblico sia sostenibile. Altrimenti, la capacità della banca centrale di difendere la stabilità del valore della moneta che emette si incrina. Così in D. MASCIANDARO, *Rischio inflazione e disciplina fiscale, una catena (e un monito) da ricordare*, in *Il Sole 24 ore*, 29 settembre 2022.

do all'opzione zero del *business as usual*, per affrontare i rischi e le insidie di questi mercati emergenti. Preso atto di ciò, diventano necessarie forme di regolazione, come visto, non solo a tutela del cittadino o del consumatore risparmiatore, ma anche della stabilità finanziaria nel suo complesso.

L'impiego dei big data espande la regolazione in questi servizi innovativi, obbligando gli operatori dell'ecosistema digitale a informare correttamente i risparmiatori, a valutare il merito creditizio su dati qualitativamente validi, a far valere l'accountability dei titolari dei trattamenti. Non solo. Si intende anche imporre alle piattaforme l'obbligo regolatorio di condivisione dei dati con i concorrenti, quale strumento per evitare la monopolizzazione endogena del mercato dei dati da parte delle piattaforme che su essi basano il proprio business. A questa logica condivisione su larga scala di dati finanziari risponde quello spazio comune di dati finanziari, che garantirebbe una migliore condivisione degli stessi tra i paesi dell'Unione.

Gli emittenti di crypto-attività oppure i prestatori di servizi che li hanno ad oggetto sono assoggettati a meccanismi di vigilanza: per cui sono soggetti ad un regime di autorizzazione preventiva; devono notificare un white paper che informi sui rischi di questi investimenti; sono tenuti al rispetto di regole funzionali a garantire l'integrità del mercato.

Oltre a ciò, quando le crypto-attività imitano eccessivamente i meccanismi monetari, proponendosi come sostituti, interviene una disciplina più stringente a tutela della stabilità finanziaria e ad evitare eventuali effetti di politica monetaria. Questa regola vale soprattutto per gli stablecoins, cioè gli asset reference token (ART) e gli e-money token assoggettati (quando significativi) alla vigilanza dell'EBA unitamente alla BCE.

Non mancano, infine, conseguenze sotto il profilo istituzionale, dal momento che si espandono i poteri di controllo e di sorveglianza in capo alla banca centrale o alle autorità europee.

La regolazione in materia di Fintech appare, insomma, volta a salvaguardare la dimensione pubblicistica in tutti i suoi aspetti, dalla tutela del risparmio all'effetto moltiplicatore del denaro bancario, e ciò avviene perché i sistemi di intelligenza artificiale «riflettono e producono relazioni sociali e comprensioni del mondo»<sup>21</sup>. E lo fa sommando entrambe le tecniche di intervento: sia l'applicazione di norme viventi ad attività innovative ma funzionalmente analoghe ed equiparabili, sia l'introduzione di nuovi presidi regolamentari. Ciò dimostra ancora una volta che, quando un mercato non c'è o quello stesso mercato fallisce – perché non riesce ad orientare corret-

---

<sup>21</sup> K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA*, il Mulino, Bologna, 2021, 16.

tamente le scelte dei produttori e dei consumatori – il mercato viene ad essere sostituito con la regolazione in una dimensione pubblicistica.

Non va sottaciuto, in conclusione, che se queste tecnologie hanno avuto finora un ruolo *disruptive* nella finanza, ciò è in parte dovuto all'assenza di regole e di intermediazione che ne hanno caratterizzato l'operatività. Per questa ragione, scegliere di inserire queste tecnologie all'interno del paradigma finanziario classico, caratterizzato dall'intermediazione e da discipline normative rigide, può avere un "costo" che merita di essere considerato. Esso consiste nel conseguente rischio di frenare lo sviluppo dei mercati finanziari grazie alle potenzialità di queste tecnologie oppure, più probabile, nel pericolo che gli operatori rispondano in maniera negativa alla regolamentazione abbandonando l'utilizzo e l'emissione di alcune delle categorie disciplinate ovvero tendano a localizzare questi strumenti al di fuori dell'Unione.



Maria Antonietta Scopelliti

## È ancora possibile la neutralità della tecnologica della normativa?

SOMMARIO: 1. Introduzione. – 2. Ogni sistema di IA è uguale solo a sé stesso (framework OCSE) – 3. La via Europea alla Regolamentazione dell’IA. – 4. L’Approccio sperimentale anche per i Regolatori e le pubbliche Autorità. – 5. L’Approccio della CONSOB. – 5.1. L’Esperimento KID. – 5.2. L’Esperimento Abusi di Mercato. – 5.3. Nuovi progetti.

### 1. Introduzione

La tecnologia pone sempre problemi complessi a chi elabora o amministra le norme: finché è stato possibile le norme hanno voluto e potuto essere tecnologicamente neutrali<sup>1</sup>. La stessa Commissione europea, nella proposta di Regolamento sull’IA, ammette che la definizione di sistema di IA mira ad essere il più possibile neutrale dal punto di vista tecnologico, con ciò arrendendosi all’impossibilità di osservare il principio in termini assoluti. Anche molti giuristi si domandano se la neutralità tecnologica è ancora perseguibile di fronte a strumenti tecnologici che “scompigliano” alcuni principi cardine del diritto, ad esempio in materia contrattuale (*smart contract*) o di responsabilità (chi è responsabile dei danni causati dall’applicazione di un algoritmo elaborato e fornito da terzi rispetto ai contraenti?<sup>2</sup>). Secondo auto-

---

<sup>1</sup> L’Università di Stanford ha elaborato un interessante indice che valorizza il numero di atti legislativi legati all’intelligenza Artificiale di 25 paesi (2022-AI-Index-Report Master.pdf). “More Global Legislation on AI than ever” – Complessivamente il numero di leggi approvate nel quinquennio 2016-2021 è stato pari a 55 (nel 2016 il numero era 11), dominano gli USA con 13 leggi, seguiti da Russia, Belgio, Spagna e Regno Unito. Nel 2021 Spagna, UK e Stati Uniti sono stabili ai primi posti con 3 leggi ciascuno. Le norme riguardano vari campi di attività: da quello etico, a quello medico a quello finanziario.

<sup>2</sup> Il Parlamento Europeo con la Risoluzione del 20 ottobre 2020 ha formulato delle Racco-

revoli esperti di *computer science* (Silvio Micali dell' MIT), è ormai inevitabile la previsione di regole che riguardano direttamente i requisiti di infrastrutture tecnologiche (ad esempio requisiti di governance per le ormai decine di migliaia di blockchain esistenti o requisiti dei sistemi di crittografia), a prescindere dal loro ambito di utilizzo.

## 2. Ogni sistema di IA è uguale solo a sé stesso (framework OCSE)

Gli elementi costitutivi dell'IA di ieri non sono quelli di oggi e cambieranno ulteriormente domani, e sono comunque molto diversi fra loro anche nello stesso istante temporale. Anche il nostro Consiglio di Stato, in una recente sentenza del novembre 2021 ha distinto tra algoritmi tradizionali e algoritmi avanzati e intelligenza artificiale, affermando che *“Non v'è dubbio che la nozione comune e generale di algoritmo riporti alla mente ‘semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato’ [...] Cosa diversa è l'intelligenza artificiale. In questo caso, l'algoritmo contempla meccanismi di machine learning e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati – come fa invece l'algoritmo ‘tradizionale’ – ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico”*<sup>3</sup>.

Agli albori la logica degli algoritmi era lineare e dava sempre risposte coerenti con i dati immessi e gli input impostati. Oggi i sistemi, sulla base della programmazione iniziale, sono capaci grazie all'esperienza di evolversi e magari correggere alcune impostazioni iniziali (*machine learning*). L'algoritmo di machine learning può inoltre analizzare dati già perfettamente catalogati o strutturati dall'essere umano (*supervised*) oppure può essere chiamato a trovare nuove correlazioni e quindi a introdurre nuovi cataloghi di dati e informazioni (*unsupervised*). In sostanza, se prima si alimentavano i sistemi con dati e regole per elaborarli, per ottenere risposte conseguenti, oggi si immettono nel sistema dati e risposte desiderate per ottenere regole di elaborazione.

---

mandazioni alla Commissione per prevedere un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL).

<sup>3</sup> Sentenza 25 novembre 2021, n. 7891 del Consiglio di Stato, sezione III.

Di fronte a queste evoluzioni, le manovre delle pubbliche autorità non possono che avere natura sperimentale ed essere manovre di accerchiamento con incursioni contemporanee su più fronti.

Quest'anno è stato apprezzabile lo sforzo dell'OCSE che, in un recente paper del febbraio 2022<sup>4</sup>, ha messo in guardia dal considerare l'IA un mondo unitario e proprio per questo, ha elaborato alcuni principi e criteri di policy pubblica per valutare singolarmente ogni sistema di IA, i suoi benefici e i suoi rischi.

Il *framework* OCSE vuole fornire un metodo alle autorità pubbliche:

1. Per capire quali sono le caratteristiche più importanti da valutare.
2. Per stabilire come organizzare registri o albi dei sistemi e degli algoritmi.
3. Per capire come affrontare le specialità di ciascun settore.
4. Per supportare la valutazione dei rischi e quindi la loro mitigazione.
5. Per supportare il risk management durante tutto il ciclo di vita dei sistemi di IA, incluse misure di governance.

L'OCSE introduce poi criteri distinti per l'IA di laboratorio, cioè relativa al momento della costruzione e dello sviluppo del modello, che dipende moltissimo dalla qualità dei dati utilizzati, dai test di funzionamento e dagli obiettivi ipotizzati. Anche la dimensione conta, perché la complessità dei modelli incide sulla spiegabilità<sup>5</sup> e sulle altre caratteristiche-chiave, come la robustezza e la tutela dei diritti personali. Per esempio, i sistemi a reti neurali, considerati molto accurati dagli scienziati, possono essere più difficilmente spiegabili di altri.

L'altra circostanza ormai acquisita, e confermata dall'OCSE, è che tra gli attori-chiave della nuova dimensione tecnologica rientrano con certezza anche gli sviluppatori dei modelli, ponendosi nuovi problemi di governance e di articolazione delle responsabilità in caso di danni a terzi.

---

<sup>4</sup>OECD, *Framework for the classification of ai systems*, in *Oecd digital economy papers*, February 2022, No. 323.

<sup>5</sup>L'AI spiegabile (eXplainable Artificial Intelligence, XAI) è un insieme di metodi e processi che consentono agli utenti di comprendere e considerare attendibili i risultati e l'output creati dagli algoritmi di machine learning.

### 3. La via Europea alla Regolamentazione dell'IA

Sappiamo che la proposta di regolamento sull'Intelligenza Artificiale della Commissione europea (aprile 2021) ha utilizzato un approccio *risk-based* centrato sulla tutela dei diritti della persona<sup>6</sup>.

L'UE, come per la protezione dei dati (GDPR), si è quindi distinta radicalmente dal modello liberale anglosassone e da quello interventista cinese, tentando di percorrere una terza via.

L'opzione normativa prescelta è stata quella di vietare sistemi dal rischio inaccettabile, normare i sistemi ad alto rischio (rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone) e dare possibilità a tutti i fornitori di sistemi non ad alto rischio di aderire ad un codice di condotta.

I requisiti per i sistemi ad alto rischio riguarderanno i dati, la documentazione, la tracciabilità, la trasparenza, la sorveglianza umana, nonché la robustezza e la precisione.

Anche gli attori sono definiti e comprendono fornitori e utenti, operatori privati e pubblici. Nel Regno Unito, ad esempio, è già in corso di elaborazione (e reso pubblico per la consultazione) uno standard di trasparenza che le istituzioni pubbliche devono adottare per spiegare se e come usano algoritmi nel loro processo decisionale. Lo standard prevede che vengano fornite informazioni sulla proprietà e la responsabilità dell'algoritmo; descrizioni dettagliate e il rationale del suo utilizzo; informazioni su come l'algoritmo si inserisce nel processo decisionale e sulla natura dell'intervento umano. Si aggiungono specifiche tecniche dei sistemi e informazioni sui dati utilizzati e sui rischi. Lo standard è in via di sperimentazione con alcuni esercizi-pilota che coinvolgono autorità pubbliche.

---

<sup>6</sup> Ai fini del regolamento, un "sistema di intelligenza artificiale" è definito come un software che può generare contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono; e che utilizza – semplificando un po' – approcci di apprendimento automatico (supervisionato, non supervisionato e per rinforzo) con metodi, tra cui l'apprendimento profondo (deep learning); approcci basati sulla logica e approcci basati sulla conoscenza, approcci statistici, metodi di ricerca e ottimizzazione.

#### 4. L'approccio sperimentale anche per i Regolatori e le pubbliche Autorità

Tra le misure per sostenere l'innovazione, l'UE ha previsto uno spazio di sperimentazione normativa anche per l'IA. È recentissima (di novembre 2022) la notizia dell'avvio di un Centro Europeo sulla trasparenza degli algoritmi (che avrà sede a Siviglia), che dovrà supportare la Commissione europea nella vigilanza sui sistemi algoritmici utilizzati dalle grandi piattaforme on-line e dai motori di ricerca, dando attuazione agli obblighi di gestione dei rischi previsti dal *Digital Services Act*<sup>7</sup> appena entrato in vigore. Il Centro dovrebbe divenire operativo nel 2023 ed è in corso il reclutamento di esperti. Come un vero laboratorio dinamico, rappresenta un ponte tra accademia, gruppi di ricerca, istituzioni e imprese.

Un risultato concreto molto importante è che le sperimentazioni creano delle contaminazioni dei saperi, facendo nascere nuove figure organizzative. Il mondo dell'IA ha infatti bisogno di "interpreti" delle applicazioni che siano in grado di connettere gli scienziati dei dati e gli esperti dei singoli settori di attività e quindi di spiegare il funzionamento dei modelli.

#### 5. L'approccio della CONSOB

Questa visione di laboratorio dinamico ha ispirato anche la CONSOB nel suo Piano Strategico e nelle sue prime sperimentazioni.

La CONSOB ha individuato le aree più adatte per iniziare la sperimentazione: la vigilanza sulle negoziazioni e la vigilanza sui documenti informativi dei prodotti complessi. L'IA e il *machine-learning* hanno bisogno, infatti, di grandi volumi di dati affidabili per restituire modelli robusti fondati su più parametri e testati con profondità temporale. Anche se va detto che la gestione di applicazioni di IA su grandi volumi richiede notevoli investimenti in infrastrutture e che il problema dell'adeguatezza delle infrastrutture nella PA rimane "l'elefante nella stanza".

---

<sup>7</sup> Il *Digital Services Act* è il nuovo regolamento sui servizi digitali, approvato dal Parlamento europeo il 5 luglio 2022, insieme al Digital Markets Act. Il Digital Service Act è stato pubblicato sulla Gazzetta Ufficiale europea in data 27 ottobre 2022 ed è entrato in vigore 20 giorni dopo la sua pubblicazione ed è applicabile dal 17 febbraio 2024

## 5.1. L'Esperimento KID

La prima sperimentazione è stata applicata a supporto dell'attività di vigilanza dei documenti (KID – *Key Information Document*) che illustrano le caratteristiche principali dei prodotti finanziari preassemblati destinati agli investitori al dettaglio (PRIIPs – *Packaged Retail and Insurance-based Investment Products*).

La numerosità dei documenti (oltre un milione e mezzo di documenti notificati nel 2021) rende impossibile uno loro scrutinio completo e, come in altri settori, rende necessario l'utilizzo di criteri di selezione basati su parametri di rischio. Gli esperti CONSOB hanno selezionato il set di dati strutturati che consentono di individuare indicatori sintetici di rischio. La CONSOB ha quindi definito regole di mappatura ed estrazione precise e spiegabili. In tal modo si è resa possibile l'estrazione automatizzata di informazioni qualificate dai documenti e la definizione di una sorta di tassonomia dei prodotti. Ai 20 minuti circa di lettura di un singolo KID da parte di un funzionario CONSOB si sostituiscono i soli 3 secondi della macchina. Successivamente il sistema intelligente clusterizza i diversi tipi di prodotti. Il primo *Proof of Concept* (PoC), in partnership con un team di esperti de La Sapienza, ha applicato tecniche di analisi del linguaggio naturale; il test condotto su 17.000 documenti ha dimostrato un grado di precisione e accuratezza elevatissimo, pari al 99%. A questo primo passo seguirà l'applicazione di una tecnologia di machine learning per avere come risultato una raccomandazione sulle priorità delle azioni di vigilanza, attraverso uno screening automatico.

## 5.2. L'Esperimento Abusi di Mercato

La seconda sperimentazione ha coinvolto la Normale di Pisa, ha riguardato la vigilanza sulle transazioni e ha dato risultati notevoli (appena pubblicati sul sito CONSOB<sup>8</sup>). Il lavoro di analisi e preparazione dei dati è stato cruciale. I dati devono infatti avere molte caratteristiche: appropriatezza rispetto all'obiettivo; rappresentatività, granularità, completezza e coerenza, poco "rumore" di fondo (anomalie, imprecisioni, incongruenze, errori). La data quality ha implicazioni importantissime in termini di sicurezza del sistema e qualità del risultato (*garbage-in, garbage-out*). Nel no-

---

<sup>8</sup> Cfr. *Quaderno FinTech* n. 11, novembre 2022.

stro esperimento la pulizia dei dati, pur già ragionevolmente strutturati e catalogati, ha assorbito il tempo maggiore nello sviluppo del modello. Analogamente, la catalogazione dei dati richiede la conoscenza umana e quindi gli esperti di quel settore o di quell'ambiente. Attribuire la giusta etichetta ai dati significa già fornire nuovi input al sistema. Ad esempio, se i dati soffrono di bias, anche il modello di IA ne soffrirà. Il cuore dei problemi e della loro soluzione va sempre cercato nei dati.

Obiettivo del modello è stato quello di dedurre un possibile evento dalla connessione di molti dati. Anche in questo caso, parliamo di estrarre nuove informazioni dai dati disponibili in una fase preistrutturata. La decisione di avviare o non avviare un'istruttoria rimarrebbe sempre affidata alla mente umana.

La ricerca di un evento o di un'anomalia è quello che fanno ordinariamente le autorità di vigilanza. Infatti, la CONSOB già opera con principi di vigilanza risk-based che restituiscono allarmi e segnalazioni, poi analizzati e qualificati con l'intervento umano, ma è consapevole dell'immenso beneficio che proprio a questo tipo di vigilanza può apportare l'IA. Abbiamo seguito un approccio interdisciplinare, che coinvolge Università e Centri di Ricerca, essendo consapevoli che le sole competenze interne non sarebbero allo stato sufficienti e che sul mercato non possono esistere prodotti adatti alle esigenze di un'autorità di vigilanza.

Il progetto mira alla prevenzione degli abusi di mercato, analizzando i comportamenti degli investitori prima della rivelazione di eventi "price sensitive". Alcune caratteristiche comportamentali degli investitori possono infatti essere determinate da intenti abusivi. Lo studio, sviluppato su data set anonimi, descrive le caratteristiche di due *proof of concept* che, impiegando metodi di *artificial intelligence* di tipo *unsupervised machine learning*, potrebbero utilmente supportare, una volta ultimata la sperimentazione, le analisi preliminari per l'individuazione di soggetti sospetti, cui potrà seguire l'attività di indagine volta a raccogliere ulteriori elementi utili per ipotizzare singole fattispecie di abuso.

Il primo modello utilizza un metodo di *clustering analysis*. Questo metodo consente di identificare quei gruppi di investitori la cui attività di trading in prossimità di un evento price sensitive risulta non solo svolta in direzione premiante, ma anche caratterizzata da discontinuità operativa sia rispetto alla precedente storia di trading sia rispetto all'operatività tipica del gruppo di appartenenza. In particolare, la *clustering analysis* elabora in primo luogo il modello di trading di ciascun investitore sulla base di selezionati parametri quantitativi. Elaborando tali parametri, la metodologia identifica gruppi omogenei di investitori con riferimento a uno specifico

orizzonte temporale. Infine, attraverso l'analisi dell'evoluzione nel tempo della posizione assunta da ciascun investitore, l'analisi distingue i soggetti che, in prossimità di un evento price sensitive, risultano aver modificato il loro comportamento di trading. Graficamente si produce una scatola (che abbiamo chiamato la scatola di Pandora) che colora i punti di discontinuità sui quali svolgere analisi ulteriori (slide). Per costruire questa scatola la macchina impiega 10 minuti; abbiamo stimato che un funzionario CONSOB impiegherebbe dalle 2 alle 3 settimane per ottenere lo stesso risultato.

Il secondo modello (che abbiamo chiamato la tela di Penelope) mira a identificare piccoli gruppi di investitori che ottengono profitti operando in modo sincronizzato in prossimità di una notizia price sensitive. La metodologia prima caratterizza l'attività di trading di ogni investitore in possibili stati (compratore, venditore, sia compratore che venditore) e poi costruisce una rete di investitori caratterizzati da un'attività sincrona in termini di stati e di tempistica di trading. Partendo da una rete di investitori statisticamente validata vengono infine individuati gruppi omogenei di soggetti con attività simile che hanno operato con beneficio rispetto ad un evento price sensitive. Su questi gruppi di soggetti interverrà l'analista umano per valutare se vi siano i presupposti per proseguire l'attività ed avviare un'istruttoria di vigilanza.

Come è chiaro, il beneficio centrale di questi modelli è quello di poter gestire grandi volumi di dati con una velocità e un grado di coerenza irraggiungibili dalla mente umana. Con humour tutto anglosassone è stato detto che il bello degli algoritmi è che “non si stancano mai e non hanno bisogno di vacanze”<sup>9</sup>.

### 5.3. Nuovi progetti

Nel nostro piano strategico abbiamo individuato altre possibili aree di sperimentazione, tra le quali la creazione di una sorta di massimario della giurisprudenza dell'Arbitro per le Controversie Finanziarie che possa essere di supporto alle decisioni e ai risparmiatori e l'analisi della rendicontazione di sostenibilità per combattere il rischio di *greenwashing*.

Il primo progetto è finalizzato, in prima battuta, ad estrarre dalle decisioni già assunte gli orientamenti ricorrenti dell'Arbitro. In una seconda fase, l'obiettivo sarà quello di sperimentare se l'applicazione di strumenti

---

<sup>9</sup>“Government by Algorithm: The Myths, Challenges and Opportunities” -Briefing posted on 25th January 2021 by multiple authors of Tony Blair Institute for Global Change).

di IA nell'analisi della documentazione relativa ad un ricorso consenta di ottenere prime indicazioni sulla possibile soluzione del ricorso, anche alla luce dei precedenti.

Per quanto riguarda il progetto sulla sostenibilità, l'intenzione è quella di creare un modello di verifica automatica dell'informativa di sostenibilità, resa sia nelle Dichiarazioni Non Finanziarie sia nei documenti di offerta di strumenti finanziari come i green bond. La definizione di metriche di difformità potrebbe, infatti, essere utile per intercettare fenomeni di *greenwashing*, anche grazie al confronto con le informazioni diffuse in altri ambiti da uno stesso emittente o da fonti esterne (score, rating di sostenibilità e così via).

Tutti i progetti in campo non prevedono al momento lo sviluppo di algoritmi predittivi le cui implicazioni nell'ambito dell'attività della PA sono ancora più delicate e complesse. In futuro, tuttavia, sulla linea di quanto detto circa l'opportunità di distinguere sempre le caratteristiche di ogni singola applicazione, dovremo essere capaci di aprire anche questa pagina per coglierne le enormi opportunità, fronteggiando adeguatamente i rischi.



Anna Genovese

# La circolazione dei valori mobiliari su *blockchain*

SOMMARIO: 1. Introduzione. – 2. Le condizioni per la circolazione dei valori mobiliari su *blockchain*. – 3. Dalla dematerializzazione alla tokenizzazione dei valori mobiliari. – 4. Le scelte di regolazione di rilievo gius-commercialistico. – 5. Note conclusive.

## 1. Introduzione

La trasformazione digitale dei prodotti e dei processi è una potente leva di penetrazione dell'innovazione e della concorrenza nel settore finanziario. Dall'innovazione digitale della finanza possono venire nuove funzionalità e opportunità, ma certamente anche nuovi rischi, micro e macro. La regolazione finanziaria deve perciò definire, nell'interesse generale, le coordinate di riferimento di questa trasformazione. Peraltro, a proposito dei rapporti fra regolazione e “fintech”, e fra rischi e opportunità della finanza digitale, sarebbe necessario fare molti distinguo, in ragione dell'eterogeneità dei fenomeni così etichettabili.

Con riguardo alle opportunità e ai rischi dell'impiego in finanza delle tecnologie digitali “distribuite” e della *blockchain*, sono da considerare, su un piatto della bilancia, le possibilità di efficientamento, sviluppo e inclusione; e sull'altro piatto, alcuni specifici rischi micro e macro<sup>1</sup>. I principali rischi micro si riferiscono alla tenuta delle operazioni finanziarie disintermedate e quindi all'effettività della tutela giuridica essenziale, informativa

---

<sup>1</sup> Cfr. da ultimo, anche per ulteriori riferimenti bibliografici, M. DE MARI, G. GASPARRI, T.N. POLI, *Introduzione: DLT e cripto attività*, in P. CARRIÈRE, N. DE LUCA, M. DE MARI, G. GASPARRI, T.N. POLI, con presentazione di A. STAGNA D'ALCONTRES, *Tokenizzazione di azioni e azioni tokens*, in *Quaderno Giuridico Consob*, Roma, 2023, 11 ss.

e sostanziale, degli investitori. I rischi macro principali si riferiscono ai possibili contraccolpi di instabilità della finanza disintermediata<sup>2</sup>; rischi di grande rilievo posto che il comparto finanziario è sempre strategico e include *asset* che, in UE, possono normativamente rilevare come “infrastruttura critica” per la sicurezza<sup>3</sup>.

A fronte di ciò, va ricordato che tradizionalmente l’approccio dell’Unione europea nei confronti dell’innovazione finanziaria e della concorrenza nel settore finanziario, è stato a lungo tutt’altro che aperto. Ciò, fra l’altro, ha contribuito alla conformazione “bancocentrica” del comparto finanziario europeo e al limitato ricorso delle imprese europee ai finanziamenti del mercato dei capitali. Con innegabili perdite di opportunità di crescita. Per altro verso, però, come comunemente riconosciuto, è indubbio che proprio l’arretratezza del sistema finanziario europeo abbia concorso ad attutire gli effetti dell’ultima grave crisi finanziaria globale del 2008.

In questa fase storica, e con riferimento alla trasformazione digitale dell’economia e della finanza, un approccio regolatorio solo conservativo, però, non è più sufficiente e non è più condiviso. La digitalizzazione e la conseguente apertura del settore finanziario anche a modelli decentrati di operatività sono percepite come una necessità. La digitalizzazione del settore finanziario è avvertita sia dalle istituzioni UE sia dai maggiori *player* come una trasformazione economica, industriale e sociale non solo ineludibile, ma potenzialmente vantaggiosa per la crescita economica dell’eurozona e del Mercato Unico. Sono state assunte perciò numerose iniziative di apertura alla trasformazione digitale dei servizi, dei prodotti e dei mercati finanziari. Fra queste iniziative, il varo nel 2021 del *Digital Finance Package*<sup>4</sup> ha

---

<sup>2</sup> Il 16 febbraio 2023 l’FSB ha pubblicato un rapporto (*The Financial Stability Risks of Decentralised Finance*) che analizza alcuni rischi macroeconomici della innovazione digitale finanziaria e segnatamente della finanza decentralizzata (DeFI).

<sup>3</sup> Con il d.l. n. 21/2012 (“*Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell’energia, dei trasporti e delle comunicazioni*”, c.d. “Decreto Golden Power”, convertito nella legge n. 56/2012) è stata ridefinita la disciplina sui poteri speciali che il Governo può esercitare con riferimento alle società che operano in settori di rilevanza strategica e di interesse nazionale, individuando – anche mediante alcuni atti di normazione secondaria – l’ambito oggettivo e soggettivo di applicazione, i presupposti e le procedure per l’esercizio dei suddetti poteri. La normativa introdotta nel 2012 non si riferiva al settore finanziario ma si è nel tempo accresciuta e stratificata. Attualmente il settore finanziario è incluso fra quelli strategici dall’art. 4 del regolamento UE n. 452/2019, come specificato dagli artt. 2 e 8 del d.p.c.m. del 18 dicembre 2020, che classifica “critiche” le infrastrutture che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione.

<sup>4</sup> Il *Digital Finance Package* pubblicato dalla Commissione UE comprende alcune Comuni-

segnato una vera svolta di approccio anche per ciò che riguarda la finanza decentrata.

Il corposo documento della Commissione europea delinea un piano di interventi di regolazione che traccia l'orizzonte della trasformazione digitale della finanza UE. Le misure prospettate nel "Pacchetto digitale" vanno poste in relazione anche con la Comunicazione della Commissione europea sulla *Open Strategic Autonomy* nel settore finanziario (19 gennaio 2021). È questa, infatti, a segnare quel cambio di postura dell'UE rispetto alle sfide esterne anche di matrice tecnologica che prelude al nuovo corso regolatorio di cui fa parte il "Pacchetto".

Il *Digital Finance Package* include molteplici interventi di regolazione per la finanza digitale. Questa regolazione punta a mitigare rischi di cui appare ineludibile l'accettazione e a rendere la finanza digitale una leva strategica di sviluppo del Mercato Unico. Il complesso degli interventi ambisce a convertire il potenziale di mercato della finanza digitale decentrata in potenziale di crescita delle relazioni economiche transfrontaliere. Segnatamente, le misure del Pacchetto UE sono volte a sfruttare anche l'innovazione digitale per il superamento della frammentazione dei mercati dei capitali in UE. La prospettiva è dunque apertamente favorevole all'innovazione finanziaria, anche a quella che consegue all'utilizzo della tecnologia di registro distribuito (oltre che dell'intelligenza artificiale).

Le previsioni contemplate dal "Pacchetto digitale", peraltro, per quanto innovative, non si situano fuori dal sistema o dal solco degli obiettivi e dei mezzi della regolazione finanziaria europea. Tali previsioni intersecano diverse altre discipline UE sulle attività finanziarie e sulla protezione dei consumatori e degli investitori. Sono altresì collegate ai "terminali" di diritto dei contratti e delle obbligazioni tuttora definiti dagli Stati Membri e a livello di singoli ordinamenti nazionali.

Tali connessioni sono molteplici e di assoluta pregnanza. Nel presente contributo vorrei accennare ad alcune di esse. Vorrei in particolare soffermarmi sugli aspetti di diritto interno che possono far rilevare come finanza decentrata l'emissione e la circolazione su *blockchain* di valori mobiliari.

---

cazioni (la *Digital Finance Strategy* e la *Retail Payment Strategy*) oltre a quattro proposte legislative: il regolamento c.d. MiCA, il regolamento c.d. PILOT *Regime*, la direttiva che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (EU) 2015/2366 e UE/2016/2341 e il regolamento c.d. DORA sulla resilienza operativa digitale per il settore finanziario che modifica i regolamenti (CE) nn. 1060/2009, (UE) 648/2012, (UE) 600/2014 e (UE) 909/2014.

## 2. Le condizioni per la circolazione dei valori mobiliari su *blockchain*

Il pacchetto UE di regole sulla finanza digitale non dispone, quanto “presuppone”, che la tecnologia *blockchain* sia utilizzata anche per l’emissione e per la circolazione di strumenti finanziari e di valori mobiliari. Non interviene direttamente né sul regime di emissione digitale dello strumento finanziario, né su quello della sua circolazione digitalizzata. Le previsioni di MiCAR e PILOT assumono però indirettamente rilievo a questo riguardo.

Segnatamente, il MiCAR introduce una disciplina del mercato di determinati cripto *asset* e dei relativi servizi<sup>5</sup>. Il MiCAR si riferisce, oltre che agli *e-money token*, a tutti i *crypto-asset* che non sono regolati da altre fonti UE e che sono “diversi dagli strumenti finanziari”. Dal canto suo, il PI-

---

<sup>5</sup>Il regolamento MiCA (in procinto di approvazione) si propone l’obiettivo di fornire certezza/legale, supportare l’innovazione, proteggere i consumatori e l’integrità del mercato, garantire la stabilità finanziaria e mitigare i rischi all’efficace trasmissione della politica monetaria e alla sovranità monetaria. A tal fine la proposta normativa intende introdurre norme uniformi direttamente applicabili agli attori di questo nuovo mercato identificati negli emittenti di *crypto-asset* e nei prestatori di servizi su *crypto-asset*, e a determinate fasi della creazione di questo mercato. Le norme UE prevalgono su quelle nazionali eventualmente già vigenti, in tema di: a) trasparenza e obblighi di *disclosure* inerenti all’emissione e ammissione alle negoziazioni di *crypto-asset*; b) autorizzazione e vigilanza dei fornitori di servizi su *crypto-asset*, degli emittenti di *asset-referenced token* e degli emittenti di *token* moneta elettronica; c) gestione, organizzazione e *governance* degli emittenti di *asset-referenced token*, degli emittenti di *token* moneta elettronica e dei fornitori di servizi su *crypto-asset*; d) protezione dei consumatori in relazione all’emissione, negoziazione, scambio e custodia di *crypto-asset*; e) prevenzione di *market abuse* per assicurare l’integrità dei mercati di *crypto-asset* che siano scambiati su una piattaforma di *trading*. Il Regolamento MiCA prevede un regime differenziato per l’offerta dei *crypto-asset* diversi dagli *asset-referenced token* (“ART”) e dagli *e-money token* (“EMT”); e l’offerta di ART e EMT. Nel primo caso, l’emittente di CA diversi è tenuto a redigere e pubblicare un *white paper* il cui contenuto è stabilito dal Regolamento MiCA. Per il *white paper* non è contemplata una preventiva autorizzazione ad opera delle Autorità di vigilanza, bensì un regime di mera notifica preventiva all’Autorità dello Stato membro di origine dell’emittente. L’Autorità dispone del potere di richiedere integrazioni e modifiche al *white paper*, ovvero di sospendere e vietare l’offerta in caso di violazione del MiCAR. Per gli ART, invece, si prevede una preventiva autorizzazione con riferimento sia all’emittente sia al *white paper*. Tale autorizzazione può essere richiesta solamente da una persona giuridica avente sede nell’Unione europea ed è rilasciata dall’Autorità dello Stato membro di origine, in stretto raccordo con le Autorità europee di vigilanza. Nel caso in cui gli ART siano particolarmente significativi per il mercato interno la vigilanza è attribuita all’EBA. Da ultimo, gli EMT possono essere emessi unicamente da banche o da istituti di moneta elettronica. I citati soggetti, oltre a rispettare la disciplina loro ordinariamente applicabile, sono tenuti anche a conformarsi ai requisiti del MiCAR. Il Regolamento MiCA accorda il passaporto europeo sia agli emittenti di *crypto-asset* sia ai prestatori di servizi su cripto-attività, creando così un mercato integrato a livello europeo. Sulla tassonomia delle criptoattività che è alla base del Pacchetto e per altre indicazioni cfr. M. DE MARI, G. GASPARRI, T.N. POLI, *op. cit.*, 20 ss.

LOT (entrato in vigore il 22 giugno 2022 e applicabile a partire dal 23 marzo 2023) permette, a livello di singoli Stati, di testare (per massimo 5 anni) lo svolgimento delle funzioni di *trading* e *post-trading* (per il mercato secondario) di strumenti finanziari “tokenizzati”, ossia emessi nativi digitali o digitalizzati. Sicché con PILOT evidentemente l’UE si prepara a un successivo adeguamento della regolamentazione complessiva in materia di servizi e di strumenti finanziari, che includerà quelli emessi e negoziati tramite la *blockchain*<sup>6</sup>.

Il pacchetto regolatorio UE, quindi, non reca alcuna disciplina riferita alla emissione e alla circolazione degli strumenti finanziari su *blockchain*. Esso però presuppone chiaramente che tali emissioni e che tale circolazione vi possano essere (vi siano in futuro e in atto). Per cui, strumenti finanziari e valori mobiliari sono interessati dal nuovo diritto UE sulla finanza digitale solo se e in quanto, dal punto di vista contenutistico e contrattuale, la loro tokenizzazione sia già regolata da altre fonti.

La nuova regolazione europea quindi interpella gli ordinamenti nazionali su varie questioni aperte. *In primis* le questioni che afferiscono alla compatibilità fra la natura giuridica dei *token*, il regime della loro circolazione su *blockchain* e la categoria dei valori mobiliari<sup>7</sup>. Fra le questioni giuridiche che il “Pacchetto Digitale” pone c’è poi quella che attiene alla possibilità e, in tal caso, al regime della circolazione su *blockchain* di valori mobiliari, segnatamente azioni e obbligazioni native digitali o digitalizzate<sup>8</sup>. Nello speci-

---

<sup>6</sup>Cfr. M. CIAN, *La nozione di criptoattività nella prospettiva del MiCAR. Dallo strumento finanziario al Token, e ritorno*, in ODCC, 2022, Numero Speciale, a cura di G. GITTI e M. MAUGERI, p. 59 ss. e anche per ulteriori riferimenti M. DE MARI, G. GASPARRI, T.N. POLI, *op. cit.*, 16, testo 20 e note.

<sup>7</sup>La normativa unionale e nazionale pone specifica attenzione al regime di circolazione cartolare dello strumento e all’idoneità delle formalità stabilite per questa circolazione. La disciplina, che tiene conto del diritto societario a cui è soggetto l’emittente “società per azioni” e del ruolo degli intermediari. Nell’ordinamento interno, la definizione di strumento finanziario è contenuta all’art. 1, comma 2, TUF (in combinato disposto con l’Allegato C, che richiama le definizioni di MIFID II). In questa definizione rientrano i valori mobiliari (titoli che possono essere negoziati nel mercato dei capitali), gli strumenti negoziati nel mercato monetario, le quote di un OICR e i contratti derivati. I valori mobiliari più comuni, azioni e obbligazioni, a loro volta, sono sottoposti a specifica disciplina nazionale di emissione e circolazione cartolare dematerializzata tramite coinvolgimento di intermediari che aderiscono al sistema di gestione accentrata Monte Titoli SpA: sulla centralità ricostruttiva del valore mobiliare nel diritto finanziario cfr. F. ANNUNZIATA, *La disciplina del mercato mobiliare*, 11<sup>a</sup> ed., Torino, 2021, 7 ss.

<sup>8</sup>Cfr. P. CARRIÈRE, *Cripto attività quali rappresentazioni “originarie” o “derivative”. Profili di diritto societario e dei mercati finanziari*, in P. CARRIÈRE, N. DE LUCA, M. DE MARI, G. GASPARRI, T.N. POLI, *op. cit.*, 77 ss.

fico, se possano circolare sulla *blockchain*, con gli effetti cartolari della circolazione dei titoli di credito, anche azioni e obbligazioni.

Su tale ipotesi di lavoro vorrei soffermarmi.

Ritengo che la trattazione del tema debba muovere dalla definizione delle condizioni fattuali e giuridiche di questa circolazione. Tali condizioni afferiscono, in primo luogo, alle caratteristiche tecnologiche dello strumento *blockchain* e della circolazione degli *asset* digitali criptati; poi alla valenza socio economica dell'utilizzo della *blockchain* per scopi finanziari; infine, al quadro normativo entro cui lo specifico fenomeno socio-economico deve essere sussunto. Cominciamo considerando le caratteristiche tecnologiche della circolazione su *blockchain*.

Le caratteristiche tecnologiche della circolazione su *blockchain* si desumono da quelle dello strumento. In quanto strumento, la *blockchain* fa parte delle *distributed ledger technologies* (DLT) che si sono affermate con lo sviluppo del Bitcoin e delle *criptocurrencies*, a partire dal 2008. La *blockchain* nasce come strumento idoneo a supportare la creazione e una circolazione scritturale facile e sicura di *asset* digitali criptati. La *blockchain* si può sommariamente descrivere come una tecnologia basata su una catena di blocchi e su registri distribuiti. La catena e i registri garantiscono l'integrità dei dati informatici condivisi e prodotti in occasione della creazione o della utilizzazione (anche tramite cessione) dell'*asset* digitale. La *blockchain* è dunque potenzialmente idonea ad assicurare una circolazione sicura e veloce ad *asset* digitali che danno a loro volta l'accesso "automatizzato" a determinate utilità. La circolazione digitale sulla *blockchain* è attivata da specifici algoritmi (protocolli informatici di esecuzione automatizzata) chiamati *smart contracts*<sup>9</sup>. Il collegamento fra *token* o *cripto asset*, *smart contract* e *blockchain* è strutturale. Grazie alle funzionalità dello *smart contract*, e ai sistemi di criptazione, la *blockchain* realizza una nuova e inedita forma di "incorporazione digitale" di un diritto in un *asset* digitale. Infatti, l'*asset* criptato dà, a chi ne possiede "la chiave", accesso a controprestazioni "automatizzate" (e per questo prive di rischio controparte); e dà anche la possibilità di cedere la prerogativa all'interno di una *community* di utilizzatori della *blockchain*.

Si può dire, quindi, che una delle innovazioni della DLT consiste nel mettere a disposizione degli operatori economici un nuovo bene strumentale (la *blockchain*) e una nuova forma di rappresentazione e di circolazione (digitale, agile e sicura) di posizioni giuridiche date (il *token*). L'incor-

---

<sup>9</sup>In argomento si rinvia a M. MAUGERI, *Smart Contracts e disciplina dei contratti*, Bologna, 2021, *passim*.

porazione del diritto nel veicolo che ne consente l'agevole circolazione consegue peraltro alle stesse caratteristiche del mezzo. In sostanza, il protocollo informatico di progettazione del *token* determina gli effetti del suo utilizzo tramite *blockchain* come effetti "autoattuativi" dell'interesse del creditore/titolare. Il modello perciò, per molti aspetti, somiglia a quello che ha storicamente determinato il successo dei titoli di credito. Il veicolo *token* è tendenzialmente in grado di garantire al creditore/titolare che lo possiede (a titolo originario o derivativo) un adempimento che azzerà o per lo meno riduce sensibilmente i rischi contrattuali di controparte.

Queste caratteristiche portano a collocare la *blockchain* nel novero di strumenti negoziali (fisici o digitali) ideati, come a suo tempo lo furono i titoli di credito documentali, per soddisfare un'esigenza storicamente ricorrente. L'esigenza di innovazioni capaci di sostenere la fiducia e le relazioni commerciali fra soggetti sconosciuti e distanti nello spazio e nel tempo. Esigenza economica, moderna e vieppiù contemporanea, di cui l'esperienza di mercato del "commiato dai titoli di credito" cartacei non attesta certo il tramonto quanto la trasformazione<sup>10</sup>.

Fra le potenzialità giuridiche della *blockchain*, dunque, ci può essere anche l'incorporazione e la circolazione di diritti finanziari come quelli che competono al titolare di una azione o di una obbligazione. Occorre però chiedersi a quali condizioni, e con quali effetti, titoli come le azioni o le obbligazioni possano circolare sulla *blockchain*. Ciò anche alla luce del fatto che istituzioni come la Banca Europea degli Investimenti e alcune società azionarie private (anche italiane) hanno già proceduto ad emettere su una *blockchain* obbligazioni sottoscritte da investitori professionali.

In sostanza, riguardo l'ipotesi avanzata, occorre appurare se e a quale regime giuridico può essere convenzionalmente assoggettata la circolazione digitale su *blockchain* di *criptoasset* azionari o obbligazionari.

A quadro normativo dato, quando è in procinto di finire il 2022, la possibilità e il regime giuridico (di forma e di effetti) della circolazione di drit-

---

<sup>10</sup> Cfr. M. LIBERTINI, *I titoli di credito nella dottrina giuscommercialistica italiana. In memoria di A. Pavone La Rosa*, in *Impresa e Società nell'opera di Antonio Pavone La Rosa*, Milano, 2017, a p. 85: «Il fenomeno del "commiato dai titoli di credito" che la dottrina ha in vario modo celebrato, non va inteso soltanto come abbandono dello strumento cartaceo, sulla linea di quella *e-substitution* che porta ovunque (dalle comunicazioni postali alle ricette mediche, eccetera) al superamento della trasmissione di strumenti cartacei mediante l'impiego di strumenti di comunicazione elettroniche, pur nella costanza delle strutture contenutistiche fondamentali della comunicazione. Quello che è avvenuto è un fenomeno più radicale, di scomparsa dei mercati in cui circolavano i titoli cartacei negoziabili: le funzioni economiche un tempo svolte da questi mercati sono ormai svolte da imprese specializzate nei diversi servizi e i conflitti di interessi che nascono nello svolgimento di tali servizi sono affrontati nell'ambito di discipline contrattuali bilaterali».

ti tokenizzati sulla *blockchain* ha la sua fonte nell'autonomia privata (art. 1322 c.c.), con le sue potenzialità conformative ma anche con i suoi limiti. Anche per ciò che riguarda azioni o obbligazioni, la *blockchain* può essere convenzionalmente scelta dalle parti – oltre che per l'esecuzione di una controprestazione, anche – per formalizzare la cessione dei diritti verso la controparte. La circolazione digitale, quindi, può essere convenzionalmente individuata come forma necessaria e sufficiente per l'efficacia fra le parti (cedente,essionario e controparte ceduta) del trasferimento di un diritto di credito. Gli effetti della cessione saranno tuttavia solo quelli propri dell'acquisto a titolo derivativo in capo all'acquirente dei diritti che facevano capo al cedente. La convenzione in esame non può far assumere rilievo cartolare a formalità di cessione che non sono già contemplate come tali dall'ordinamento.

In proposito giova ricordare che, malgrado possa considerarsi ormai superata la prospettiva di tipicità dei titoli di credito<sup>11</sup>, non possa dirsi parimenti superata la conformazione tipizzata delle “forme” della circolazione cartolare dei titoli di credito. Ne consegue che formalità diverse da quelle già contemplate come “leggi di circolazione” di titoli di credito fisici o dematerializzati non possono produrre gli effetti della circolazione cartolare. Le formalità della circolazione su *blockchain* non possono produrre gli effetti della circolazione cartolare. Esse, infatti, sono diverse sia dalle formalità della circolazione dei titoli di credito documentali (al portatore, all'ordine o nominativi), sia dalle formalità scritturali di circolazione previste per i titoli di credito dematerializzati dal d.lgs. n. 213/1998<sup>12</sup>.

Le notazioni svolte portano a ritenere preclusa, oggi e a quadro normativo dato, la circolazione cartolare di valori mobiliari come le azioni o le obbligazioni su *blockchain*. In altri termini, il diritto cartolare e quello del mercato mobiliare opererebbero come barriere normative alla circolazione cartolare di strumenti finanziari tokenizzati, pur non precludendo la tokenizzazione (incorporazione digitale) di azioni e di obbligazioni e la loro cessione, su base convenzionale, solo o anche su *blockchain*<sup>13</sup>.

---

<sup>11</sup> Come è noto, dopo l'accesso dibattito risalente alla seconda metà del secolo scorso, oggi si ritiene che, ad eccezione dei titoli al portatore contenenti l'obbligo di pagare una somma di denaro, ammessi solo nei casi previsti dalla legge (cfr. l'art. 2004 c.c.) che l'autonomia privata sia libera di creare nuovi titoli di credito: cfr., per tutti, F. MARTORANO, *Titoli di credito*, 3<sup>a</sup> ed., Milano, 1997, 169 ss.; A. STAGNO D'ALCONTRES, *Il titolo di credito. Ricostruzione di una disciplina*, Torino, 1996, 225 ss.

<sup>12</sup> Cfr. G. GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca Borsa tit. cred.*, n. 1, 2020, 13 ss.

<sup>13</sup> Cfr. N. DE LUCA, M. DE MARI, *Azioni tokens come fattispecie “nativa”*, in P. CARRIÈRE, N. DE LUCA, M. DE MARI, G. GASPARRI, T.N. POLI, *op. cit.*, 95 ss.

Il nuovo quadro normativo europeo sollecita però il legislatore italiano anche ad adeguare le leggi interne sulla circolazione cartolare di titoli di credito digitali. L'adeguamento è essenziale per cogliere, su un piano differente da quello armonizzato, opportunità giuridiche ed economiche di finanza digitale altrimenti precluse. Opportunità riferite al "contenuto" di liquidabilità di diritti finanziari tokenizzati.

### 3. Dalla dematerializzazione alla tokenizzazione dei valori mobiliari

L'Italia non è fra le nazioni europee che già si sono dotate di discipline in materia di emissione e di circolazione cartolare di *token*. Come detto, il diritto nazionale vigente ha a mente solo determinati titoli di credito dematerializzati: sono i valori mobiliari emessi e negoziati in una determinata modalità "analogica" da intermediari autorizzati che li conferiscono alla gestione accentrata in base alle previsioni del d.lgs. n. 213/1998. Per il resto, il diritto dei titoli di credito conosce solo leggi di circolazione (titolo al portatore, all'ordine e nominativo) che presuppongono un veicolo documentale di incorporazione del diritto.

Questo però è ormai un dato che stride con il quadro UE definito dalle misure del *Digital Finance Package* e con il fatto che la tecnologia offre e la prassi si avvale di nuovi meccanismi di emissione e di circolazione dematerializzata di diritti di contenuto finanziario. L'intervento del legislatore è peraltro possibile oltre che imprescindibile e vantaggioso.

La possibilità dell'intervento consegue all'idoneità della tecnologia e della dematerializzazione a cui essa conduce, per la facilità e la sicurezza della circolazione della pretesa e della sua soddisfazione (vedi *supra*). Ossia consegue alle stesse caratteristiche tecniche della circolazione sulla *blockchain* degli *asset* digitali criptati. Per altro verso, l'intervento del legislatore è anche imprescindibile. L'idoneità del mezzo non basta per assimilare la dematerializzazione digitale a quella scritturale e la circolazione digitale e decentralizzata su *blockchain* a quella elettronica e centralizzata di cui al d.lgs. n. 213/998. Da questo punto di vista, la tokenizzazione di titoli inclusi nella nozione di valori mobiliari non può essere assimilata o equiparata alla dematerializzazione dei medesimi titoli introdotta dal decreto legislativo citato a suo tempo. Questo intervento, infatti, si riferisce solo a una determinata forma di dematerializzazione di determinati titoli e servizi. Ammette solo titoli suscettibili di circolazione scritturale presso una gestione accentrata con cui si rapportano gli intermediari autorizzati.

Dunque, fra le riflessioni più urgenti a cui deve portare la normativa UE, e specialmente il PILOT, c'è quella che verte sul "se", "come" e "quando" modificare le norme di diritto interno sulla circolazione cartolare di valori mobiliari dematerializzati. Nella consapevolezza che, fino ad allora, permarranno barriere regolamentari all'ingresso della tecnologia *blockchain* nelle operazioni di investimento più diffuse e di specifico interesse per le imprese azionarie e per il mercato.

Va peraltro segnalato come siano già state assunte alcune iniziative in questa direzione. Nel 2021, Consob, dopo essersi confrontata con il mercato, ha elaborato e messo a disposizione del Ministero dell'Economia, e degli altri interlocutori istituzionali, una proposta per adeguare il diritto cartolare italiano alle possibilità di tokenizzazione offerte dalla *blockchain*. C'è dunque una base da cui partire, se si vorrà procedere.

#### 4. Le scelte di regolazione di rilievo gius-commercialistico

Come detto, già nel 2021, Consob ha presentato al Ministero dell'Economia una proposta di legislazione in materia di tokenizzazione di titoli inclusi nella categoria dei valori mobiliari. La proposta è stata elaborata sulla falsariga di quella legislazione che nel 1998 ha disciplinato gli effetti cartolari dell'emissione dematerializzata e della circolazione accentrata dei valori mobiliari presso Monte Titoli SpA. L'intervento normativo per la tokenizzazione di titoli inclusi nella categoria dei valori mobiliari richiede però una istruttoria verosimilmente più lunga e complessa di quella che ebbe luogo nel 1998 per la dematerializzazione (in gestione accentrata) dei titoli quotati. L'intervento oggi è richiesto da obblighi europei in scadenza (come lo fu quello del 1998) riferiti al Regolamento Pilot, ma implica l'esercizio di diverse opzioni. Questi fattori verosimilmente hanno contribuito sin qui ad allungare i tempi d'istruttoria dell'intervento.

Fra le delicate opzioni di rilievo gius-commercialistico che sono da vagliare, ne voglio citare tre.

La prima riguarda il perimetro dell'intervento. L'intervento può limitarsi all'essenziale, disciplinando gli effetti cartolari della emissione e della circolazione in DLT di alcuni più semplici strumenti finanziari, come le obbligazioni societarie. Oppure può prendere in considerazione gli aspetti cartolari riferiti alla tokenizzazione di tutti i valori mobiliari e anche delle azioni, favorendo così altre trasformazioni di processo riferite alla costituzione e al governo societario (c.d. *corptech*)<sup>14</sup>. Oppure può, in termini an-

<sup>14</sup>Cfr. P. CARRIÈRE, *op. cit.*, 90 ss.; N. ABRIANI, *Rappresentazione e circolazione di participa-*

cora più dirompenti per il sistema, non porre alcun confine alla tokenizzazione dei diritti connessi a contratti finanziari. Questa scelta porterebbe a riconoscere le formalità di cessione sulla *blockchain* come “legge di circolazione” cartolare applicabile a qualunque titolo di credito e prodotto finanziario.

La seconda opzione riguarda le definizioni dei requisiti dello strumento tecnico della *blockchain* e del DLT. Tali requisiti devono assicurare la integrità, autenticità, non ripudiabilità, non duplicazione delle registrazioni. Devono consentire la riconducibilità di uno specifico quantitativo di *asset* digitali a un determinato soggetto “titolare” di essi. Il nostro ordinamento in effetti contiene all’art. 8 *ter* del decreto semplificazioni del 14 dicembre 2018, n. 135 una definizione di *blockchain* e di *smart contract* che fa esplicito riferimento alla DLT. Teoricamente però le caratteristiche dei registri elettronici distribuiti potrebbero essere riscontrate anche da tecnologie diverse dalla DLT e oggi in fase di sviluppo. Occorre quindi effettuare anche una scelta sulla tecnologia della finanza decentrata, con implicazioni per la concorrenza e la futura struttura del comparto.

La terza questione riguarda la possibilità ed eventualmente le modalità della contemporanea presenza sui mercati regolamentati di strumenti dematerializzati e accentrati e di strumenti finanziari tokenizzati e decentrati.

L’adeguamento legislativo dovrà altresì dipanare numerose altre questioni tecniche. Ne cito solo alcune. Stabilite le caratteristiche tecniche che ciascun registro *blockchain* dovrà avere per garantire per supportare il nuovo regime di circolazione, con effetti equivalenti alla non riproducibilità del “titolo” e all’esclusività del “possesso” proprie del mondo cartolare, si dovrà individuare il soggetto in capo al quale sono posti l’obbligo e la responsabilità di tale garanzia. Tale ruolo potrebbe essere rivestito dall’emittente o da una società terza individuata dall’emittente stesso, come specializzata nella “tenuta” di registri per conto altrui. Con molteplici differenze a valle.

Parimenti deve essere delineata una disciplina per l’ipotesi dell’impossibilità di accesso dell’investitore alla propria posizione sul registro (in particolare per smarrimento della “chiave privata” della cripto attività). Si dovrà quindi prevedere una disciplina delle informazioni da associare al valore digitale al momento dell’emissione e dovranno essere introdotti anche presidi pubblicistici e standard di sicurezza dei depositi (per i c.d. servizi

---

*zioni di società di capitali mediante tecnologia DLT*, in ODCC, 2022, Numero Speciale a cura di G. GITTI, M. MAUGERI, p. 359 ss. e N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla «Fintech» alla «Corptech»*, Bologna, 2021, *passim*.

di portafoglio digitale “*wallet*”), nel rispetto del principio di proporzionalità e di altri principi internazionali comuni che sono in via di definizione<sup>15</sup>.

## 5. Note conclusive

Il varo del pacchetto UE sulla finanza digitale segna una importante discontinuità nel processo di penetrazione della trasformazione digitale nella finanza europea. Molti effetti di questa regolazione saranno immediati e diretti, altri seguiranno, secondo l’agenda UE. Alcuni effetti però, eventuali e indiretti, incrociano l’agenda del legislatore nazionale. Fra questi ci sono quelli che possono coinvolgere i valori mobiliari e la loro circolazione presso un ampio pubblico di investitori. Tali effetti, infatti, richiedono di essere supportati da interventi nazionali sulla legislazione cartolare.

In Italia è in corso una istruttoria su questo intervento. È importante che l’istruttoria si svolga in modo approfondito. C’è però da valutare anche il fattore tempo e la competitività. Va in particolare considerato che alcuni Stati UE hanno già introdotto regole specifiche per le emissioni e la circolazione dei titoli di credito su DLT. In tal senso si è mossa per prima, sin dal 2017, la Francia<sup>16</sup>, seguita da Lussemburgo<sup>17</sup>, Liechtenstein<sup>18</sup> e Germania<sup>19</sup>. Una disciplina sui titoli di credito in DLT è stata introdotta anche nella vicina Svizzera<sup>20</sup>.

Gli Stati citati hanno colmato le lacune dispositive del proprio diritto cartolare riferite alla emissione dei *token* come incorporazione di diritti in

---

<sup>15</sup> L’*United Nations Commission On International Trade Law* (UNICITRAL) ha intrapreso un percorso riferito alla “legge modello” sui titoli di credito elettronici, nella quale sono formulati principi compatibili con la tecnologia dei registri distribuiti: cfr. G. FINOCCHIARO, L. CASTELLANI, *La legge modello dell’UNICITRAL sui titoli di credito elettronici*, in *Contr. impr.*, 2021, 38 ss.

<sup>16</sup> Cfr., in particolare, l’*Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l’utilisation d’un dispositif d’enregistrement électronique partagé pour la représentation et la transmission de titres financiers* e il *Décret n° 2018-1226 du 24 décembre 2018, relatif à l’utilisation d’un dispositif d’enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l’émission et la cession de minibons*.

<sup>17</sup> *Loi du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres. Loi du 22 janvier 2021 portant modification : 1° de la Loi modifiée du 5 avril 1993 relative au secteur financier; 2° de la Loi du 6 avril 2013 relative aux titres dématérialisés.*

<sup>18</sup> *Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister.*

<sup>19</sup> *Gesetz zur Einführung von elektronischen Wertpapieren Vom 3. Juni 2021.*

<sup>20</sup> Cfr. la legge federale svizzera del 25 settembre 2020.

un veicolo idoneo alla circolazione cartolare. Tali ordinamenti hanno scelto di edificare il pilastro cartolare della finanza digitale prima e autonomamente dalla edificazione del pilastro UE riferito ai servizi e ai mercati finanziari digitalizzati. La scelta evidentemente serve ad attrarre nella giurisdizione nuove industrie che possono iniziare a svolgere nuove attività. Giocando d'anticipo per acquisire vantaggi competitivi su scala regionale e globale.

Del resto, come dovrebbe insegnare tutta l'esperienza della *data economy*, anche la partita della finanza digitale europea si giocherà fra chi riuscirà a condurre il gioco dal versante dello sviluppo e dell'offerta innovativa di processi e prodotti finanziari "digitali", e chi diventerà il mercato di sbocco di questi prodotti e servizi. Fra chi potrà avere competenze ed esperienza per esercitare una influenza sulla regolazione UE dei nuovi mercati e chi non avrà queste competenze e opportunità. Ed è evidente da quale parte sia più conveniente cercare di posizionarsi. Tanto più per l'Italia dove il risparmio privato suscettibile di tramutarsi in investimento è così elevato e di interesse per l'industria finanziaria e per l'economia reale<sup>21</sup>.

---

<sup>21</sup> Quando questo scritto era già in bozze, il 17 marzo 2023, è stato pubblicato in Gazzetta Ufficiale il Decreto Legge n. 25 (Decreto Fintech) recante una disciplina cartolare della circolazione su *blockchain* di determinati strumenti finanziari. Il Decreto Legge risulta in attesa di conversione quando le bozze vengono licenziate per la stampa.



Francesco Di Ciommo\*

## Smart Contract, robo advisor e mercati finanziari

SOMMARIO: 1. Trading algoritmico ed Internet of Things: fenomenologia del mondo che cambia. – 2. Gli Smart Contract: una categoria (non giuridica). – 3. La Blockchain a servizio degli Smart Contract. – 4. I mercati finanziari dall'Algorithmic Trading (AT) all'High Frequency Trading (HFT) – 4.1. Velocità e intensità delle negoziazioni come fattori concorrenziali. – 4.2. HFT e rischi di market abuse. – 4.3. I primi tentativi di regolare il fenomeno. – 4.4. Gli AT e gli HFT alla luce delle direttive MIFID I e II. – 5. La consulenza finanziaria e la c.d. robo advisor.

### 1. Trading algoritmico e Internet of Things: fenomenologia del mondo che cambia

Sovente accade, in particolar modo nell'ambito delle scienze c.d. sociali, che tra gli studiosi si alimenti un dibattito in ragione della emersione nella prassi di questioni inedite, rispetto alle quali la prima reazione ordinante consiste nella individuazione di una categoria concettuale che ambisce a definire, e dunque in qualche modo inquadrare, il nuovo fenomeno, con l'intento, più o meno esplicito, di ricondurlo a sistema e, dunque, di facilitarne l'analisi e, nel caso del diritto, magari anche di individuarne i tratti disciplinari<sup>1</sup>.

---

\* Una prima, e diversa, versione di questo lavoro è pubblicata, con il titolo *Gli Smart Contract e lo smarrimento del giurista nel mondo che cambia. Il caso dell'High Frequency Trading (HFT) finanziario*, in F. FIMMANÒ, G. FALCONE (a cura di), *Fintech*, Napoli, 2019, 157. Una seconda, e ulteriormente diversa, versione è pubblicata in *Nuovo dir. civ.*, 2019, 25, con il titolo *Smart Contract e (non)diritto. Il caso dei mercati finanziari*. Infine, una versione ulteriormente diversa della riflessione da cui origina questo scritto è pubblicata in inglese, con il titolo *Smart Contract and (Non-)Law. The case of the Financial Markets*, in *Law and Economics Yearly Review*, 2018, v. 7, II, 291.

<sup>1</sup>Nella tradizione filosofica risalente ad Aristotele le categorie (dal greco *katēgoría*) sono considerate concetti generali entro cui si può assumere ogni realtà attraverso predicati (*Κατηγορίαι*, IV sec. a.C., contenuta nell'*Organon* di Andronico di Rodi). Un approccio com-

A ben vedere, l'evoluzione del sapere storicamente è stata ampiamente favorita da tali dinamiche. Ciò, per l'appunto, è accaduto (e accade) anche nella letteratura giuridica e, più in generale, nel mondo del diritto. Gli esempi a riguardo potrebbero essere molteplici. Basta pensare, per restare nel recinto civilistico, alla significativa vicenda della categoria dei diritti della personalità, enucleata per la prima volta da Otto von Gierke alla fine dell'Ottocento; ovvero al fondamentale sviluppo della teoria del negozio giuridico, alimentato dall'emanazione del BGB nel 1896<sup>2</sup>. In entrambi i casi, constatata la sopravvenienza di istanze sociali di tutela di nuovi interessi individuali o di regolazione di questioni sino a quel momento trascurate, i giuristi reagirono creando categorie attorno alle quali si produsse un dibattito serrato ed in ragione delle quali si definì successivamente anche l'atteggiamento dei legislatori e dei giudici.

Qualcosa di simile sta accadendo proprio adesso, e da qualche anno, riguardo al complesso, e sempre più rilevante, tema delle operazioni economiche concluse e/o eseguite, in tutto o in parte, autonomamente da *software* (dunque, da algoritmi) per via telematica, e cioè direttamente da computer (o anche da robot o da automi) tra loro collegati, per lo più attraverso il *cyberspace*, senza l'intervento umano.

Tali operazioni convenzionalmente vengono oramai, da più parti (e cioè sia in ambito tecnologico che giuridico e sociologico) ed a livello planetario, qualificate "*trading* algoritmico" e identificate con l'espressione (atecnica) di "*smart contract*" (ovvero, letteralmente, contratti intelligenti) e ricondotte nell'alveo della relativa neo-nata categoria, che a ben vedere, tuttavia, non ricomprende esclusivamente contratti, ed anzi per lo più riguarda soltanto una o più fasi esecutive di un precedente contratto, spesso consegnato come contratto quadro o come contratto per adesione.

Più precisamente, con la locuzione *smart contract* si fa generalmente riferimento a situazioni in cui sono tradotte e trasposte in codice informatico –

---

pletamente diverso al tema fu dato da Kant, il quale nella *Critica della ragion pura* dimostrò come le categorie non siano determinazioni della realtà, ma solo della conoscenza in quanto rappresentano modi di operare dell'intelletto umano che si applicano al materiale (di origine empirica) dato nell'intuizione sensibile. Più di recente, appare degno di nota l'approccio seguito, in ambito neoempiristico, da Gilbert Ryle, il quale – in *The concept of mind* (1949) – ha definito "categorie di un concetto" il gruppo di regole che presiedono al suo uso.

<sup>2</sup>Sconfinata è la letteratura sui due temi accennati. Per tutti, v., rispettivamente, D. MESSINETTI, *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, 354; AA.VV., *Categorie giuridiche e rapporti sociali. Il problema del negozio giuridico*, Milano, 1978; F. GALGANO, *Il negozio giuridico*, in *Tratt. Cicu-Messineo*, Milano, 1988; G. STOLFI, *Teoria del negozio giuridico*, Padova, 1961; e R. SACCO, *Negozio giuridico. Circolazione del modello*, in *Dig. disc. priv.*, Sez. civ., XII, Torino, 1995.

sì da risultare intellegibili per il *software* (che opera attraverso uno o più algoritmi<sup>3</sup>) tramite il quale l'operazione deve svolgersi – non solo le regole che formano quello che possiamo (con una qualche approssimazione) indicare come il regolamento (para)contrattuale, ma anche le circostanze fattuali in presenza delle quali deve eseguirsi automaticamente, in tutto o in parte, una prestazione prevista da dette regole, o comunque deve verificarsi un qualsiasi effetto connesso all'operazione secondo le impostazioni iniziali<sup>4</sup>.

In altre parole, per come la locuzione in esame viene utilizzata comunemente oggi, può qualificarsi *smart contract* qualsiasi operazione economica, o pezzo di operazione economica, coinvolgente due o più parti, che possa operare, e dunque snodarsi e sviluppare i suoi effetti, indipendentemente dall'intervento umano, sulla base delle regole date e delle informazioni esterne acquisite in corso d'opera dal congegno automatizzato tramite il quale l'operazione si svolge. E, dunque, sulla base dell'accertamento automatico che il relativo *software* compie circa l'avverarsi, o meno, di determinate condizioni, a cui fa seguito l'automatica esecuzione delle azioni collegate a detto accertamento.

La caratteristica appena evidenziata fa sì che, in un ambiente tecnologico sano (c.d. neutro), e cioè al riparo da condizionamenti esterni fuorvianti, il rischio che il percorso predeterminato entro il quale l'operazione deve svolgersi venga deviato – ad esempio, il rischio di un eventuale inadempimento – è contenuto entro limiti bassissimi perché gli automi, come detto, si atterrano (o dovrebbero attenersi<sup>5</sup>) agli ordini ricevuti, sicché in presenza delle condizioni prefissate eseguiranno la prestazione, o comunque realizzeranno gli effetti voluti dalle regole in base alle quali sono impostati i propri algoritmi.

Inoltre, l'algoritmo generalmente è programmato per gestire ogni sopravvenienza (e proprio per questo si parla di *contract* “intelligenti”) e

---

<sup>3</sup>Per una sintetica e chiara riflessione su cosa sono e quanto siano importanti gli algoritmi nella c.d. società digitale, v. G.F. ITALIANO, *Dixit algorithmi. Breve Storia del nostro futuro*, disponibile on-line all'indirizzo «<http://open.luiss.it/2019/01/23/dixit-algorithmi/>».

<sup>4</sup>Cfr. S. ASHARAF, S. ADARSH (a cura di), *Decentralized Computing Using Blockchain Technologies and Smart Contracts, Emerging research and opportunities*, IGI Global, Hershey, PA (USA), 2017.

<sup>5</sup>In realtà, non è remota l'ipotesi che l'operato dell'algoritmo non rispecchi fedelmente la volontà delle parti a causa della “traduzione” informatica inesatta dell'accordo da eseguire ovvero perché l'algoritmo assume iniziative in qualche modo non previste da chi lo ha progettato, visto che – come si dirà anche più avanti nel testo – molti algoritmi si alimentano delle esperienze che maturano momento per momento. Sul punto, *ex multis*, cfr. Ed Finn, *What Algorithms Want. Imaginagion in the Age of Computing*, Mit Ed., Boston (Mass., USA), 2017.

dunque per ridurre al minimo, *rectius* tendenzialmente (o auspicabilmente) per eliminare, la possibilità che a seguito di fatti nuovi le parti possano entrare in disaccordo o comunque possa alterarsi imprevedibilmente l'equilibrio del rapporto.

Infine, va da sé che lo svolgimento dell'operazione economica tramite l'algoritmo consente di ridurre enormemente tempi e costi di ogni transazione.

Per tutti questi motivi gli *smart contract* stanno riscontrando un grandissimo successo nel mercato, in quanto, per volontà delle imprese, sono utilizzati sempre più spesso sia nell'ambito del commercio *business to consumer* che nell'ambito dei rapporti *business to business*.

Evidentemente, una descrizione del fenomeno così ampia consente subito di ribadire che all'interno della categoria degli *smart contract* possono farsi rientrate tanto veri e propri contratti, che vengono perfezionati ed eseguiti (più o meno) integralmente dai sistemi automatizzati, quanto singole fasi di una operazione contrattuale, o anche solo di un'operazione economica. Questa seconda ipotesi si verifica, ad esempio, quando è soltanto l'esecuzione di tutte o di alcune prestazioni ad essere rimessa all'accertamento, da parte del sistema automatizzato, del verificarsi dei presupposti fattuali a cui l'esecuzione è condizionata, ovvero come ad esempio avviene quando è la sola conclusione del contratto ad essere rimessa all'accertamento automatico delle condizioni in presenza delle quali le parti vogliono che quel contratto si perfezioni.

A tal proposito è bene precisare sin d'ora che quando il contratto si conclude esclusivamente attraverso l'attività di uno o più *software*, l'accertamento automatizzato dei presupposti fattuali di perfezionamento dello stesso dovrà svolgersi in ossequio a regole prefissate dalle parti, a monte, in un contratto quadro o, comunque, in un regolamento contrattuale (normalmente destinato ad operare per un certo periodo). Tale regolamento, per l'appunto, esprime la comune volontà delle parti di pervenire alla conclusione dei contratti a valle, attraverso sistemi automatizzati, in presenza di determinati presupposti, e magari a certe condizioni piuttosto che ad altre a seconda dell'accertamento del verificarsi di variabili prefissate.

Può, tuttavia avvenire, e nella prassi ciò accade molto spesso, che il regolamento contrattuale (che si è definito quadro) sia, in realtà, predisposto da una sola parte e sia aperto alla adesione della controparte, o meglio di innumerevoli altre potenziali controparti. La qual cosa, nelle moderne dinamiche di mercato, in genere avviene attraverso la realizzazione di attività materiali – tanto veloci nella loro esecuzione quanto immediate nella produzione di effetti – le quali, piuttosto che esprimere compiutamente una

volontà negoziale, concretizzano i fatti condizionanti l'efficacia dell'accordo contrattuale.

I brevi cenni appena svolti, sui quali si tornerà comunque più avanti, piuttosto che tentare di definire cosa comunemente oggi si intenda per *smart contract*, rappresentano il prodotto di uno sforzo descrittivo che in apertura della presente riflessione appare necessario per inquadrare la tematica analizzata, se pure con ampi margini di genericità ed approssimazione. Da tale primo inquadramento, infatti, emerge come lo sviluppo della telematica e, più in generale, le continue innovazioni che, giorno per giorno, segnano le più moderne tecnologie schiudono, anche (e forse soprattutto) per il mercato (*rectius*, i mercati) possibilità sino a poco tempo fa inimmaginabili.

Accade così che già da qualche tempo in tutto il mondo si discute intensamente di *Internet of things* e ciò per indicare come la rete Internet sempre più diventerà nei prossimi anni un veicolo (o un ambiente) attraverso il quale comunicheranno tra loro cose piuttosto che persone<sup>6</sup>. Le applicazioni concrete di tale tecnologia vanno dalla gestione di beni di consumo (durante la produzione, l'immagazzinamento, la distribuzione, la vendita o l'assistenza postvendita), al tracciamento di oggetti persi o rubati, alla gestione automatizzata di apparecchi tecnologici a distanza, ed altro ancora.

Secondo gli studi più accreditati nel 2008 il numero di oggetti connessi alla rete Internet ha superato la popolazione umana mondiale, mentre nel 2020 ci saranno circa cinquanta miliardi di oggetti connessi alla rete contro una popolazione mondiale di circa 9 miliardi di persone. E mentre la rete Internet cresce, e insieme ad essa le infinite altre reti di interconnessione, nuovi algoritmi si affermano, le potenze di calcolo aumentano continuamente e, in definitiva, il mondo che noi abitiamo cambia radicalmente e ad una velocità mai considerata prima.

## 2. Gli Smart Contract: una categoria (non giuridica) alla moda

Si ritiene oramai diffusamente che, operando insieme alla robotica, alla realtà aumentata e alla realtà virtuale, l'*Internet of things* accentuerà ulte-

---

<sup>6</sup>L'espressione «*Internet of things*» si ritiene sia stata coniata nel 1999 da Kevin Ashton (cfr. ID., *That "Internet of Things" thing*, in *RFID Journal*, 2012). Tra i tanti scritti in proposito, cfr. N. GERSHENFELD, R. KRİKORIAN, D. COHEN, *The Internet of Things*, in *Scientific American*, vol. 291, no. 4 (Ocotber 2004), 76-81; G. KORTUEM, F. KAWSAR, V. SUNDRAMOORTHY, D. FITTON, *Smart objects as building blocks for the Internet of things*, in *IEEE Internet Computing*, vol. 14, issue: 1, January-February 2010; e A. ZANELLA, N. BUI, A. CASTELLANI, L. VANGELISTA, M. ZORZI, *Internet of Things for Smart Cities*, vol. 1, Issue: 1, February 2014.

riormente l'interconnessione degli uomini, delle cose e degli ambienti e così determinerà nei prossimi anni la completa digitalizzazione e connessione in rete delle nostre vite<sup>7</sup>. Secondo i più ottimisti, questo renderà gli oggetti capaci di fare ciò che hanno fatto per l'uomo fino a oggi ma in maniera più efficiente e, in definitiva, per noi più utile.

Sennonché, lo sviluppo di tali tecnologie sta avvenendo in maniera talmente rapida, inclusiva, complessa e pervasiva che gli osservatori giuridici – ed ovviamente ancor più i legislatori – palesano, a tutte le latitudini del globo, forti e inevitabili incertezze nel trattare le relative problematiche.

Figlia di questa incertezza appare la moda di utilizzare la categoria *smart contract* – coniata dai tecnologi<sup>8</sup> – come se potesse avere una qualche valenza, quanto meno descrittiva, anche in ambito giuridico. Mentre, già dalle poche considerazioni sin qui esposte, appare evidente che, al di là di quanto genericamente osservato in questa sede, troppo eterogenei sono i contenuti della categoria in questione, e cioè troppo diverse tra loro sono le vicende, negoziali e non, che allo stato possono qualificarsi (o, se si preferisce, vengono ricomprese tra gli) *smart contract*, perché sul piano giuridico essa possa risultare effettivamente utile.

A rischio di risultare velleitari, dunque, sebbene animati dalle migliori intenzioni, appaiono al momento i tentativi – che pure si stanno compiendo – di svolgere ragionamenti sistematici o ordinanti attorno alla categoria in questione, disquisendo di formazione, natura, interpretazione, invalidità ed esecuzione degli *smart contract*, perché ogni diversa fattispecie annoverabile nella pseudo-categoria impone considerazioni peculiari, che mal si adattano, o che non si adattano affatto, alle altre ipotesi di contratti intelli-

---

<sup>7</sup> Il tema, in vero, è studiato già da alcuni decenni. Per una delle prime compiute riflessioni in materia, v. R. CAIRNCROSS, *The Death of Distance: How the Communications Revolutions Will Change Our Lives*, Boston, 1997. Per una prospettiva diacronica, di carattere giuridico, circa l'impatto che la telematica ha avuto sin qui nelle nostre vite, sia consentito rinviare, anche per i necessari riferimenti bibliografici e giurisprudenziali, a: F. DI CIOMMO, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. COMANDÉ (a cura di), *Persona e tutele giuridiche*, Torino, 2003, 3; ID., *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; ID., *Internet e crisi del diritto privato: globalizzazione, dematerializzazione e anonimato virtuale*, in *Riv. crit. dir. priv.*, 2003, 11; ID., *Civiltà tecnologica, mercato ed insicurezza*, in *Riv. crit. dir. priv.*, 2010, 565; e ID., *L'accesso ad Internet tra diritto e responsabilità*, in *Comunicazione digitale*, 2014, 29, ID., *Il diritto di accesso alle informazioni in Internet*, in C. PERLINGIERI, L. RUGGERI, *Internet e Diritto civile*, 2015, 77.

<sup>8</sup> Comunemente si ritiene che l'espressione sia stata coniata da N. SZABO nel suo *Smart Contracts: Building Blocks for digital market*, 1996, disponibile on-line all'indirizzo «[http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)». Per una riflessione critica circa la possibilità di definire compiutamente il fenomeno, v. E. MIK, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 9 *Law, Innovation & Technology*, 2017, 269.

genti<sup>9</sup>. Senza considerare che i tentativi in parola inevitabilmente alimentano il fraintendimento (favorito dalla infelice, seppure fortunata, locuzione inglese) circa il fatto che quando si parla di *smart contract* si faccia necessariamente riferimento a contratti, mentre, come visto, non è affatto così.

A conferma della cennata incertezza vi è, tra l'altro, il fatto che spesso quando si vuole fare un esempio di *smart contract* si fa riferimento a ciò che avviene nel mercato delle assicurazioni per autoveicoli, laddove, sulla base di dati rilevati grazie ad apparecchiature tecnologiche collocate a bordo delle vetture, il *software* in uso presso la compagnia assicurativa riceve informazioni sul comportamento del conducente (ad esempio, il superamento costante dei limiti di velocità) che possono influenzare i contenuti del relativo rapporto negoziale in quanto possono creare determinate condizioni che attivano o disattivano clausole di vantaggio o svantaggio (o facendo aumentare il premio assicurativo)<sup>10</sup>. Sennonché, come evidente, nel caso di specie l'apporto della tecnologia è limitato a fornire informazioni ad una piattaforma tecnologica che, sulla base delle pattuizioni negoziali in origine intervenute tra le parti, eventualmente anche con modalità del tutto tradizionali, concretizza gli effetti del contratto condizionati da quelle informazioni.

---

<sup>9</sup>Per la dottrina giuridica che sin qui è occupata del tema, *ex ceteris*, oltre agli studi citati nelle altre note, cfr. M.B. FOX, L.R. GLOSTEN, G.V. RAUTERBERG, *The New Stock Market: Sense and Nonsense*, in 65 *Duke Law Journal*, 2015, 191; W. REIJERS, F. O'BROLCHÁIN, P. HAYNES, *Governance in Blockchain Technologies & Social Contract Theories*, in 1 *Ledger* 134, 2016; M. KÓLVART, M. POOLA, A. RULL, *Smart Contracts*, in T. KERIKMÄE, A. RULL (eds), *The Future of Law and eTechnologies*, Springer, 2016, 133; K.E.C. LEVY, *Bopok Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law*, in 2 *Engagin Science, Technology, and Society*, 1, 2017; L.H. SCHOLZ, *Algorithmic Contracts*, in 20 *Stan. Tech. L. Rev.*, 128, 2017; K. WERBACH, N. CORNELL, *Contracts Ex Machina*, in 67 *Duke Law Journal*, 313, 2017; M. RASKIN, *The Law and Legality of Smart Contracts*, in 1 *Geo. L. Tech. Rev.*, 305, 2017; C. TUR FAÜNDEZ, *Smart contracts. Análisis jurídico*, Editorial Reus, Madrid, 2018; A.J. KOLBER, *Not-so-Smart Blockchain Contracts and Artificial Responsibility*, in 21 *Stan. Tech. L. Rev.* 198, 2018.

Per gli studi italiani più interessanti, v. R. PARDOLESI, A. DAVOLA, "Smart contract" e innovazione a tutti i costi, in corso di pubblicazione in *Foro it.*, V, letto per gentile concessione degli autori; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. e proc. civ.*, 2018, 441; L. PAROLA, P. MERATI, G. GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, 681; I.A. CAGGIANO, *Il contratto del mondo digitale*, in *Nuova giur. civ.*, 2018, II, 1152; P. CUCCURU, *Blockchain e automazione contrattuale. Riflessioni sugli smart contracts*, 2017, II, 107; V. PASQUINO, *Smart Contracts: caratteristiche, vantaggi e problematiche*, in *Diritto e processo*, 2017, 11; e D. SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contr. e impr.*, 2017, 378, ma anche in G. PERLINGIERI, A. FACHECHI (a cura di), *Ragionevolezza e proporzionalità nel diritto contemporaneo*, Napoli, 2017, 387.

<sup>10</sup>M. BELLINI, *Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*, disponibile on-line all'indirizzo «<https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/>».

Dunque, a ben vedere, in questo caso siamo nell'ambito di una vicenda che non appare creare particolari problemi sul piano giuridico, in quanto potrà essere gestita attraverso l'applicazione delle comuni e tradizionali regole contrattuali; mentre solleva questioni tecniche in quanto, ovviamente, è necessario garantire che i dati siano raccolti e comunicati in modo corretto e che la conseguente automatica modulazione degli effetti del contratto tra le parti corrisponda effettivamente a quanto in origine pattuito tra le stesse.

Del tutto diversa è, invece, l'ipotesi che si realizza quando a decidere se stipulare il contratto sono due o più *software* che, sulla base degli algoritmi con cui sono programmati, assumono decisioni autonomamente, e cioè compiono, o non compiono, determinate azioni al verificarsi, o meno, di circostanze prefissate. Tali *software*, infatti, possono tra loro comunicare e, sulla base dell'analisi dei dati a loro disposizione, trattare una determinata operazione economica in via esclusivamente automatizzata, per altro acquisendo, operazione dopo operazione, tecniche e modalità decisionali (*rectius*, comportamentali) anche molto diverse rispetto a quelle originariamente scritte nell'algoritmo di riferimento. E questo perché tali *software* sono spesso programmati per memorizzare le esperienze acquisite sul campo e conformare i propri comportamenti futuri alle informazioni così acquisite. Attraverso questi processi di apprendimento e di affinamento, i *software* si formano, giorno dopo giorno, autonomamente attraverso l'acquisizione di informazioni, sicché il loro operato molto difficilmente può essere ricondotto ad una precisa volontà umana o alla responsabilità del programmatore. Il settore in cui questa tipologia di operazioni economiche – c.d. algoritmiche – ha trovato recentemente la sua maggiore applicazione è quello finanziario, come si evidenzierà nei paragrafi a seguire.

Anche alla luce di queste ultime considerazioni, in definitiva si può ribadire quanto già sopra affermato circa il fatto che, al momento, sul piano strettamente giuridico, al concetto di *smart contract* appare riconducibile una gamma di fattispecie talmente vasta che, per la sua varietà ed eterogeneità, non si presta compiutamente ad una trattazione unitaria, se non in termini meramente ricognitivi e assai generici.

Non a caso, del resto, anche nella primissima dottrina europea che si è occupata del tema, il concetto di *smart contract* viene descritto e declinato in termini molto eterogenei<sup>11</sup>.

La stessa incertezza, finanche definitoria, si sconta nella dottrina americana che si sta occupando degli *smart contract(s)*, la quale, però, concentra

---

<sup>11</sup> *Ex ceteris*, v. CUCCURU, *op. cit.*; DI SABATO, *op. cit.*; PAROLA, MERATI, GAVOTTI, *op. cit.*

la sua attenzione su alcuni macro-temi che, in effetti, possono riferirsi, più o meno, a tutte le tipologie di operazioni rientranti nella (pseudo)categoria in rassegna, e che dunque, in ogni caso, val la pena esaminare. E così si indaga la questione della presunta autosufficienza degli *smart contract* rispetto agli istituti giuridici ed ai tribunali, in particolare relativamente al fatto che gli algoritmi, in molti casi, ambirebbero a gestire automaticamente anche problemi esecutivi sopravvenuti e, persino, dispute tra le parti<sup>12</sup>. Si esamina il problema delle responsabilità concernenti l'operato degli *smart contract*, in particolare con riferimento alle operazioni che coinvolgono i c.d. "*black box algorithmic agents*" o comunque nelle quali il processo decisionale dell'automa risulti non del tutto prevedibile *ex ante* dalle parti o da chi imposta l'algoritmo<sup>13</sup>. Ed infine, tra l'altro, si approfondisce il nodo del rapporto tra volontà umana e funzionamento dell'algoritmo, e si osserva a riguardo che la rigidità propria dell'automatismo necessariamente relega la volontà a puro enunciato, con conseguenti criticità in tema di applicazione della disciplina giuridica tradizionale in materia di contratti<sup>14</sup>.

### 3. La Blockchain a servizio degli Smart Contract

Un ulteriore tema va necessariamente considerato, se pure sinteticamente, per inquadrare con qualche pretesa di compiutezza l'argomento *smart contract*. E ciò anche al fine di sottolineare come il tentativo di approfondire, in una prospettiva giuridica, il funzionamento e la disciplina dei congegni operativi sopra cennati appare oggi, non solo particolarmente arduo vista la segnalata eterogenia di questi ultimi, ma anche a rischio di risultare, nel breve volgere di qualche mese o qualche anno, sostanzialmente inutile a causa della rapidità con cui, in ragione della sopravvenuta obsolescenza tecnologica, protocolli e algoritmi informatici vengono continuamente modificati o sostituiti da chi ne detiene il controllo.

---

<sup>12</sup> Cfr. RASKIN, *op. cit.*; ma anche, *ex multis*, R. KOULU, *Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement*, in *ScriptEd*, vol. 13, iss. 1, 2016; P. ORTOLANI, *Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin*, in 36 *Oxford J. Legal Studies* 529, 2016.

<sup>13</sup> Cfr. KOLBER, *op. cit.*; SHOLZ, *op. cit.*; ma anche, *ex ceteris*, T. GILLESPIE, *Can an Algorithm Be Wrong?*, in *LIMN*, 2, disponibile on-line all'indirizzo «<http://limn.it/can-an-algorithm-be-wrong>», 2012».

<sup>14</sup> Cfr. WERBACH, CORNELL, *op. cit.*; ma anche, *ex multis*, K.E. DAVIS, *Contracts As Technology*, in 88 *N.Y.U. L. Rev.* 83, 2013; D.H. HOFFMAN, *Relational Contracts of Adhesion*, in 85 *U. Chi. L. Rev.* 1396, 2018.

Al discorso sin qui condotto, va, dunque, aggiunta una riflessione sul rapporto tra *smart contract* e *blockchain* in quanto alcuni preconizzano nel prossimo futuro un uso sempre crescente dei c.d. contratti intelligenti in ragione dello sviluppo e della diffusione che la *blockchain* ha avuto di recente, e che ci si aspetta abbia ancora di più di qui in avanti<sup>15</sup>.

Per comprendere la questione, almeno per sommi capi, occorre chiarire che, come noto, la *blockchain* è una tecnologia basata sulla condivisione – da parte degli utenti di una rete telematica – di un *date base* distribuito tra i medesimi<sup>16</sup>, con l’obiettivo di consentire la gestione di transazioni tra questi mediante il succedersi di una catena di operazioni che avvengono tra diversi nodi della rete. In altre parole, attraverso l’uso di un registro (il *date base*) pubblico a cui gli utenti possono accedere, e che viene aggiornato automaticamente in forza del funzionamento dei *client* che partecipano alla catena (c.d. nodi), si attribuisce certezza, verificabilità e conoscibilità a determinate circostanze.

Più in dettaglio, va detto che il registro pubblico condiviso è «strutturato in blocchi, ognuno dei quali rappresenta un numero di transazioni la cui provenienza e ora di esecuzione sono attribuite in modo indelebile e immutabile, rispettivamente, attraverso un meccanismo di crittografia a chiave asimmetrica e una marcatura temporale (il c.d. *timestamping*). Ciascun blocco è collegato irreversibilmente a quello precedente tramite una particolare operazione algoritmica (la c.d. funzione di *hash*) e forma, in tal modo, la catena dei blocchi (il *blockchain* appunto) accessibile e consultabile da tutti i nodi della rete. Prima di essere aggiunto alla catena, ogni blocco è controllato, validato e crittografato da alcuni nodi (c.d. *miner*) tramite la soluzione di un’operazione matematica e risulta così a prova di manomissione»<sup>17</sup>.

---

<sup>15</sup> Cfr., *ex ceteris*, M. GIANCASPRO, *Is a ‘smart contract’ really a smart idea? Insights from a legal perspective*, in 33 *Computer Law & Security Rev.* 825, 2017; L. LUU, D.H. CHU, H. OLICKEL *et al.*, *Making Smart Contracts Smarter*, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security – CCS’16*, New York, USA, ACM Press, 2016, 254; R. HOLDEN, A. MALANI, *Can Blockchain Solve the Holdup Problem in Contracts?*, in *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper* No. 846, 2017, disponibile on-line all’indirizzo <https://ssrn.com/abstract=3093879>; nonché P. D. FILIPPI, A. WRIGHT, *Blockchain and the Law: The Rule of Code*, Harvard University Press, Cambridge, 2018.

<sup>16</sup> La *blockchain* costituisce l’applicazione più nota della c.d. *distributed ledgers technology* (DLT), e cioè della tecnologia che si basa, per l’appunto, sulla distribuzione e la condivisione, tra gli utenti di una rete, di informazioni di uso e utilità comune. La filosofia alla base della DLT si contrappone alla tradizionale logica della gestione accentrata e centralizzata delle informazioni e dei protocolli.

<sup>17</sup> Così PAROLA, MERATI, GAVOTTI, *op. cit.*

Dunque, si ritiene che la *blockchain* consenta di attribuire certezza e immodificabilità a dati e documenti, senza necessità di ricorrere ad autorità, a istituzioni o comunque a soggetti terzi e, quindi, senza alcuna intermediazione ed a livello decentrato.

La prima e più importante applicazione della tecnologia *blockchain* ha riguardato, a partire dal 2009, la moneta virtuale c.d. *bitcoin*, che ha conosciuto una grande fortuna negli scorsi anni, salvo subire un forte ridimensionamento del suo valore di scambio nel corso del 2018<sup>18</sup>. È evidente, tuttavia, che la *blockchain* offre le condizioni ideali sul piano tecnico (sia informatico, che latamente giuridico) per favorire l'uso degli *smart contract*, e ciò in quanto – come detto – essa consente di attribuire (sempre che il sistema funzioni e non presenti falle) certezza in ordine ai contenuti e alla data di una certa attività, e dunque anche di un certo documento, e di assicurarne la immodificabilità<sup>19</sup>.

Senonché, ad oggi, tanto in Europa, quanto nel resto del mondo, non esistono norme di legge o anche di rango regolamentare che riguardino la *blockchain*<sup>20</sup>. Dunque, nessuna certezza attualmente si ha, né si può avere,

---

<sup>18</sup> A metà dicembre 2018 la capitalizzazione totale delle criptovalute conosciute nei mercati mondiali ha toccato i 104 miliardi di dollari, risultando fortemente in flessione rispetto ai picchi registrati nel corso dell'anno ma ancora in linea con il valore dall'inizio di agosto 2017. L'indice di dominanza del *bitcoin*, rispetto alle altre criptovalute, si attesta oltre il 55%, mentre il suo prezzo, il 27 gennaio 2019, si attesta sugli euro 3.107,00, dopo aver toccato massimi di euro 9.183,00 a gennaio 2018 ed il suo massimo storico, di euro 16.721,00, il 15 dicembre 2017. Tra le altre criptovalute, da segnalare anche il caso di *ethereum*, il cui valore il 27 gennaio 2019 si attesta sugli euro 99,86, dopo aver toccato i suoi massimi storici di euro 1.136,27 il 12 gennaio 2018. Per uno studio aggiornato in tema di questioni giuridiche legate al fenomeno delle criptovalute, cfr. S. CAPACCIOLI, *Bitcoin e criptovalute*, in G. CASSANO, N. TILLI, G. VACIAO, *Tutele e risarcimento nel diritto dei mercati e degli intermediari*, Milano, 2018, 445.

<sup>19</sup> Per un primo tentativo di individuazione ed inquadramento delle principali problematiche giuridiche nella letteratura *hain*, nella letteratura italiana cfr. F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018. Il tema, nella particolare prospettiva delle criptomonete e dell'attività delle relative autorità di vigilanza, è trattato anche da M. PELLEGRINI, F. DI PERNA, *Cryptocurrency (and Bitcoin): a new challenge for the regulator*, in *Open Review of Management, Banking and Finance*, 2018, 318.

<sup>20</sup> In verità, qualcosa, tanto negli Stati Uniti quanto in Europa si muove. Il 1° febbraio 2018 la Commissione europea, con il sostegno del Parlamento, ha dato vita all'Osservatorio e Forum sul *blockchain*. 10 aprile 2018, su iniziativa di 22 Paesi europei, tra cui non c'è l'Italia (che però vi ha aderito subito dopo), è stata creata la *European Blockchain Partnership* con l'obiettivo di armonizzare l'approccio al tema tra i diversi Stati. Inoltre, il 3 ottobre 2018 il Parlamento europeo ha approvato una risoluzione intitolata "*Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione*", nella quale, tra l'altro, il Parlamento sottolinea la necessità di una valutazione approfondita delle potenzialità e delle implicazioni giuridiche degli *smart contract*. In più, in Francia con l'ordinanza governativa n. 1674 dell'8 dicembre 2017 è stato introdotta la possibilità di utilizzare la *blockchain* per registrare la proprietà e il trasferire

circa le applicazioni concrete che di tale tecnologia si fanno e si faranno in futuro, così come, ovviamente, circa il fatto che a breve non arrivi una novità che superi la *blockchain*. Il che, tuttavia, non sembra costituire un problema per gli *smart contract* posto che questi ultimi possono operare del tutto indipendentemente dalla *blockchain*, visto che ogni sistema informatico può dotarsi di tecnologie in grado di attribuire (un certo grado di) certezza e verificabilità ai contenuti di una data operazione negoziale, comprese identità delle parti, date e quant'altro.

Tanto è vero che nella prassi solo una frazione, tutto sommato modesta, delle operazioni economiche automatizzate realizzate in Internet, o comunque tramite strumenti telematici, si avvale della *blockchain*, mentre tutti gli altri *smart contract* risolvono attraverso altri congegni, la cui conformazione ed operatività dipende dalle scelte degli operatori interessati e dalle capacità dei sistemi tecnici coinvolti, i problemi legati alla certezza della data, alla affidabilità e alla verificabilità delle informazioni trattate in automatico, alla immodificabilità dei contenuti e più in generale alla sicurezza della relativa operazione.

Dunque, è errato considerare gli *smart contract* figli della *blockchain*, o comunque necessariamente collegati a tale tecnologia, così come appare sbagliato affermare che «la tecnologia *blockchain* permette la *self enforceability* del contratto»<sup>21</sup>. Ed infatti, l'automatismo di esecuzione delle pattuizioni contrattuali «al verificarsi degli eventi predeterminati dalle parti e iscritti nel codice» non dipende dall'uso della *blockchain*, ma – come visto sopra – è conseguenza della condivisione che le parti fanno di un sistema informatico automatizzato al quale entrambe rimettono l'esecuzione del rapporto in forza dell'accordo quadro che hanno negoziato e concluso precedentemente, ovvero che, sempre in precedenza, una parte ha proposto ed al quale l'altra parte abbia aderito<sup>22</sup>.

---

mento di titoli mobiliari non quotati (l'ordinanza è disponibile on-line sul sito governativo "Legifrance" all'indirizzo «<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908>»; cfr., *ex ceteris*, M. GARDENAL, S. MARCHESE, *Il blockchain ammesso nelle operazioni di M&A*, in *Il Sole 24Ore*, disponibile on-line all'indirizzo «<http://www.diritto24.it/sole24ore.com/art/avvocatoAffari/mercatiImpresa/2018-03-15/francia-blockchain-ammesso-operazioni-ma-123710.php>»).

<sup>21</sup> Nei termini virgolettati nel testo si esprimono PAROLA, MERATI, GAROTTI, *op. cit.*, in part. 684.

<sup>22</sup> Dunque, si può sostenere che la *blockchain* faciliti (ma, comunque, non che consenta) la *self-enforceability* dell'accordo contrattuale solo se, attraverso tale affermazione, si intende sottolineare che più le parti confidano nell'attendibilità del sistema automatico, più le stesse saranno indotte ad affidare a detto sistema la realizzazione di una o più fasi dell'operazione economica a cui sono interessate.

Tale dato consente di prevedere serenamente che gli *smart contract* sopravviveranno anche al declino e al superamento che, tra pochi mesi o molti anni, inevitabilmente (come accade ad ogni tecnologia) avrà la *blockchain*. A tal proposito, giova sottolineare che le criticità legate alla *blockchain*, e che ne hanno finora impedito un uso più diffuso, sono molteplici e significative, a partire dal fatto che l'esecuzione delle transazioni tramite tale tecnologia risulta non veloce<sup>23</sup>, senza considerare che l'attività di verifica e di validazione dei blocchi di dati risulta molto costosa sul piano organizzativo e in termini di consumo energetico<sup>24</sup>, ed inoltre senza considerare che non vi è allo stato alcuna certezza su quanto durerà, e cioè resterà perfettamente in funzione, il sistema basato sulle catene di blocchi, e dunque sulle migliaia e migliaia di *server*, disseminati in tutto il mondo, che elaborano, validano e conservano i relativi dati senza pause, tutti i giorni per ventiquattro ore al giorno.

Evidenza empirica di quanto appena sottolineato circa l'indipendenza degli *smart contract* rispetto alla *blockchain* si rinviene nell'esperienza maturata negli scorsi lustri nel settore delle transazioni finanziarie. In tale ambito, infatti, sin dalla seconda metà degli anni Novanta del secolo scorso, ci si avvale – in misura sino ad oggi sempre crescente – degli automi (e, dunque, degli algoritmi) e delle reti telematiche per raccogliere informazioni, pianificare strategie, assumere decisioni di *trading* ed eseguire operazioni sui mercati. Il tutto prima ed anche oggi in via del tutto indipendente rispetto alla *blockchain*.

---

<sup>23</sup> Allo stato, il tempo medio per effettuare una transazione sul sistema *bitcoin* è stimato di dieci minuti in quanto così è organizzato il protocollo che gestisce la validazione dei blocchi. Cfr. i testi a disposizione on-line rispettivamente all'indirizzo «<https://www.tokens24.com/it/cryptopedia/basics/come-funzionano-le-transazioni-bitcoin>» e all'indirizzo «<https://support.conio.com/hc/it/articles/115001186449-quanto-tempo-impiega-una-transazione-ad-essere-con-fermata->».

<sup>24</sup> Secondo alcune stime accreditate, l'elettricità complessiva utilizzata annualmente per produrre *bitcoin* supera i 32 *terawatt*, ben superiore ai consumi annuali di un Paese delle proporzioni dell'Irlanda che si attestano sui 25 *terawatt*. Cfr. E. MARRO, *Come lavorano e quanto guadagnano i «minatori» del Bitcoin*, su *Il Sole 24Ore*, 20 dicembre 2017, disponibile on-line all'indirizzo <https://www.ilsole24ore.com/art/notizie/2017-12-19/come-lavorano-e-quanto-guadagnano-minatori-bitcoin-163810.shtml?uid=AEVOppUD>.

#### 4. I mercati finanziari dall'Algorithmic Trading (AT) all'High Frequency Trading (HFT)

Per quanto la vicenda sia stata, sin qui, sostanzialmente poco approfondita, come cennato, gli *smart contract* già da tempo hanno trovato nel settore delle transazioni finanziarie il loro naturale ambito di sviluppo e applicazione<sup>25</sup>.

Nei mercati mobiliari di tutto il mondo, infatti, già a partire dagli Anni Novanta dello scorso secolo, si è imposto, via via in misura sempre crescente, l'uso di algoritmi che consentono la realizzazione di transazioni in automatico, e cioè senza l'intervento dell'uomo.

Per dare un'idea dell'importanza del fenomeno, giova da subito osservare che, secondo stime accreditate, già nel 2009 le transazioni algoritmiche hanno rappresentato circa il 75% del volume di scambi azionari realizzati negli Stati Uniti<sup>26</sup>. La circostanza è confermata da quanto accadde il 6 maggio 2010, allorché il *Dow Jones* subì, in soli dieci minuti, un repentino crollo (*flash crash*) scendendo dai 10.650 punti fino a meno di 10 mila, per poi ritornare nei successivi 10 minuti a 10.520 punti<sup>27</sup>. E tutto ciò in ragione di un enorme numero di scambi, tra loro reciprocamente condi-

---

<sup>25</sup> Tra gli scritti più recenti ed efficaci che indagano il fenomeno sotto l'aspetto squisitamente finanziario, v. AA.VV., *Computerized and High-Frequency Trading*, in *The Financial Review*, vol. 49 (2014), Issue 2, 173-433; e O. LINTON, S. MAHMOODZADEH, *Implications of High-Frequency Trading for Security Markets*, in *USC-INET Research Paper* n. 18-02, del 30 gennaio 2018, Univ. Of Southern California, CA (USA), disponibile on-line all'indirizzo «[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3112978](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112978)», ma anche in *Annual Review of Economics*, vol. 10 (2018), 237. Cfr., inoltre, *ex ceteris*, G. CESPÀ, X. VIVES, *High Frequency Trading and fragility*, in *ECB Working Paper* n. 2020, Febbraio 2017, disponibile on-line all'indirizzo «<https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp2020.en.pdf?853c8630ef920d9429e31ff85b2682>»; L.M. CAL-CAGNIBILE, G. BORMETTI, M. TRECCANI, S. MARMI, F. LILLO, *Collective synchronization and high frequency systemic instabilities in financial markets*, 2015, disponibile on-line all'indirizzo della Cornell University «<https://arxiv.org/pdf/1505.00704.pdf>»; nonché P. HOFFMANN, *A dynamic limit order market with fast and slow traders*, in *Working Paper Series* n. 1526, marzo 2013, European Central Bank, disponibile on-line all'indirizzo «<https://ssrn.com/abstract=1969392>»; V. CAIVANO *et al.*, *High frequency trading. Caratteristiche, effetti, questioni di policy*, in *Consob Discussion papers*, 5 December 2012, disponibile on-line all'indirizzo «<http://www.consob.it/documents/11973/219968/dp5.pdf/04c93f02-d620-456c-b0a1-868233013f6e>»; e, infine, D. FRICKE, A. GERIG, *Too Fast or Too Slow? Determining the Optimal Speed of Financial Markets*, disponibile on-line all'indirizzo «[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2363114](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2363114)».

<sup>26</sup> Vedi T. HENDERSHOTT, C. JONES, A. MENKVELD, *Does algorithmic trading improve liquidity*, in *Journal of Finance*, vol. 66, 2011, 1.

<sup>27</sup> Cfr. CONSOB, *Il trading ad alta frequenza. Caratteristiche, effetti, questioni di policy*, dicembre 2012.

zionanti, che si svolsero in quel frangente, la cui frequenza di realizzazione rese da subito evidente il coinvolgimento di automi in luogo della classica attività di *trading* svolta dall'uomo<sup>28</sup>. Fu in quell'occasione che i fari della SEC (*Security and Exchange Commission*) si accesero per la prima volta sugli *smart contract*<sup>29</sup>.

In Europa, e dunque anche in Italia, l'uso degli agenti automatici per effettuare transazioni finanziarie, benché in crescita, appare ancora contenuto<sup>30</sup>. Ed infatti, in Borsa Italiana il numero di transazioni riconducibili ad agenti automatici, che adottano strategie di negoziazione c.d. ad alta frequenza, nel 2016 e nel 2017 è stato pari a quasi il 30% dell'intero montante dei controvalori scambiati: in crescita rispetto al 2014, allorquando la percentuale si era fermata al 25,4%, e al 2015, quando la percentuale era stata del 28,7%<sup>31</sup>, ma ancora, tutto sommato, modesto, sia in valori assolu-

---

<sup>28</sup> Le indagini della Sec (l'organismo di controllo dei mercati Usa) e della Cftc (*Commodity Futures Trading Commission*) hanno successivamente appurato che il *flash crash* del 6 maggio 2010 era stato avviato da un unico ordine di vendita di *future* sull'indice S&P 500 per 4,5 miliardi di dollari: un ordine verosimilmente errato, anche perché senza indicazioni sul prezzo e sull'arco temporale, che la liquidità presente sul mercato non fu in grado di assorbire, così innescando una spirale ribassista a sua volta potenziata dallo scattare degli ordini automatici.

<sup>29</sup> Come è stato puntualmente notato, in realtà, sebbene la SEC (cfr. la nota n. 25) abbia accertato che i sistemi di *trading* ad alta frequenza sono stati coinvolti nel singolare (e piuttosto eccezionale) andamento *intraday* dell'indice principale del *Dow Jones* del 6 maggio 2010, «risulta complesso provare se essi hanno avuto un impatto positivo o negativo sul funzionamento del mercato in quella situazione, e ciò in quanto la presenza di sistemi capaci di effettuare operazioni ad altissima velocità ha sicuramente acerbato la fase di discesa dei prezzi, ma, nel momento in cui il *trend* negativo si è interrotto, gli stessi sistemi hanno permesso il vigoroso recupero dei successivi 10 minuti. Si tenga presente che dopo il famoso crollo azionario del 1987, l'indice Dow Jones impiegò più di un anno per recuperare una percentuale di perdita paragonabile a quella recuperata in soli 10 minuti nel 2010. La semplice constatazione degli effetti contrastanti che i sistemi ad alta frequenza possono aver causato in un episodio della durata di meno di un'ora è un segnale della complessità dell'argomento». Così A. PUORRO, *High Frequency Trading: una panoramica*, in *Questioni di Economia e Finanza (Occasional paper)*, Banca d'Italia, n. 198 – settembre 2013, in part. 5. Giova a riguardo aggiungere che, come si evidenzierà anche più avanti nel corso della presente riflessione, proprio il massivo utilizzo dell'HFT negli ultimi anni ha reso molto più volatili i mercati finanziari e meno eccezionali fenomeni di rapida perdita e altrettanto rapido recupero degli indici di borsa. Cfr. anche J. PAULIN, A. CALINESCU, M. WOOLDRIDGE, *Understanding Flash Crash Contagion and Systemic Risk: A Micro-Macro Agent-Based Approach*, in *Journal of Economic Dynamics and Control*, 10.1016/j.jedc.2018.12.008 (2019).

<sup>30</sup> Secondo alcuni, i robot *trader* gestiscono il 66% dei volumi globali negoziati sui mercati finanziari di tutto il mondo. Cfr. V. CARLINI, *Borse, come il robot trader «cavalca» il populismo e sfrutta lo spread*, in *Il Sole24 Ore*, 5 ottobre 2018, disponibile on-line all'indirizzo <<https://www.ilsole24ore.com/art/finanza-e-mercati/2018-10-02/-borse-come-robot-trader-cavalca-il-populismo-212907.shtml?uuiid=AEIROKFG>>.

<sup>31</sup> Cfr. *Relazione Consob per l'anno 2016*, del 31 marzo 2017, 48; *Relazione Consob per*

ti che in termini di *trand* di crescita, rispetto ai risultati registrati nei mercati più evoluti e dinamici, senza dimenticare che ad operare in Italia in alta frequenza sono per la quasi totalità *trader* stranieri<sup>32</sup>.

Dagli Stati Uniti – dove il fenomeno ha preso piede già alla fine degli anni Novanta dello scorso secolo – provengono le locuzioni *Algorithmic Trading* (AT) e *High Frequency Trading* (HFT), coniate rispettivamente per individuare le transazioni gestite da un automa tramite un algoritmo (ed ecco il concetto di *smart contract* che torna) e le transazioni ad alta frequenza che hanno come elemento caratterizzante la velocità.

Più precisamente, il concetto di HFT è normalmente associato ad un ampio spettro di strategie operative automatizzate utilizzate nei mercati finanziari, che rappresentano una sorta di passo avanti evolutivo rispetto al semplice AT. Esse, infatti, valorizzano principalmente l'aspetto della velocità di esecuzione delle operazioni e cercano di massimizzare il plusvalore competitivo che può derivare proprio da tale velocità, oltre che dalla possibilità di immettere numerosissimi ordini simili o identici (di vendita, di acquisto, di prenotazione, di cancellazione, di revoca e quant'altro) nel medesimo momento e così determinare immediate reazioni di contesto da parte degli altri operatori, per lo più anch'essi costituiti da sistemi automatizzati, i quali percepiscono il relativo momento di mercato e operano di conseguenza.

Come anticipato, più le scelte di mercato sono compiute da automi, più è possibile realizzare in poco tempo numerosissime transazioni. E questo perché l'accresciuta capacità di raccolta dati e di calcolo dei moderni elaboratori elettronici, insieme al potenziamento delle strutture di comunicazione su cui transitano i dati e allo sviluppo della scienza che studia le modalità di analisi degli stessi, consente oggi ai sistemi automatizzati di assumere autonomamente, se dotati degli algoritmi giusti e se in possesso del più ampio e coerente set di informazioni<sup>33</sup>, le scelte più coerenti con l'im-

---

*l'anno 2017*, del 31 marzo 2018, 52; e *Relazione Borsa Italiana*, marzo 2018, 23. V. anche M. CHIAMENTI, *Esma mette la museruola all'high frequency trading*, disponibile on-line all'indirizzo <[www.bluerating.com/mercati/540483/esma-porta-lhigh-frequency-trading-vero-la-regolamentazione](http://www.bluerating.com/mercati/540483/esma-porta-lhigh-frequency-trading-vero-la-regolamentazione)>, il quale, tra l'altro, segnala che una maggiore incidenza dell'HFT (64,2% del totale nel 2014 e 68% nel 2015, fonte *Relazione Consob per l'anno 2015*, del 31 marzo 2016) si registra in Italia nel mercato IDEM, dove sono negoziati i *mini futures*.

<sup>32</sup> Su un totale del 29% circa dei controvalori scambiati attraverso HFT sull'MTA (Mercato telematico azionario di Borsa italiana), il 92% di questi è attribuibile a *traders* stranieri (cfr. *Relazione Consob per l'anno 2017*, cit., 52).

<sup>33</sup> Gli automi che operano come *trader* finanziari si basano su analisi statistiche e serie storiche di almeno 10 anni, ma si alimentano istante per istante e costantemente di nuove informazioni che ricevono o che ricercano – anche attraverso la c.d. analisi semantica (cfr. M. LEWIS,

postazione ricevuta in una frazione di secondo, e di moltiplicare quelle scelte infinite volte in pochissimo tempo, variando le condizioni dell'operazione al variare della situazione<sup>34</sup>.

Tanto è vero che gli HFT costituiscono una evoluzione dei semplici AT, che spesso gli HFT sono programmati con il preciso scopo, tra l'altro, di trarre vantaggio economico/finanziario dalla presenza sui *book* di contrattazione di sistemi algoritmici meno evoluti e più facilmente prevedibili<sup>35</sup>.

Un precursore del THF, e dunque un primo esempio di AT, viene comunemente individuato nel fenomeno dei c.d. *SOES bandits*, e cioè di quella categoria di *trader*, sviluppatasi a metà degli anni Novanta dello scorso secolo, che effettuava numerose operazioni al giorno con lo scopo di trarre vantaggio da minime oscillazioni dei prezzi o dai ritardi dei *market maker* ad aggiornare i prezzi offerti in denaro o in lettera<sup>36</sup>. La vicenda in parola fu facilitata dalla decisione della *Securities and Exchange Commission* americana di consentire l'utilizzo di sistemi di *trading* alternativi e paralleli rispetto ai mercati regolamentati. Tali sistemi, in quanto operavano attraverso piattaforme informatiche senza passare attraverso i servizi offerti dai *broker-dealer*, presero il nome di *Electronic Communications Networks* (ECN). Essi corrispondono sostanzialmente agli MTF (*Multilateral Trading Facility*) disciplinati oggi in Europa dalla MIFID.

La natura parallela degli ECN rispetto ai mercati regolamentati dipendeva dal fatto che, per espressa previsione normativa, gli ordini impartiti sui primi non potevano essere eseguiti nei secondi. Di conseguenza, il *best price* a cui poteva essere eseguita una transazione su un ECN poteva anche

---

*Flash Boys. A Wall Street Revolt*, W.W. Norton & Co., USA, 2014) – sulle piattaforme più disperate, scandagliano la rete Internet, e in particolare i *social network*, per rilevare prima dei *competitor* fatti che possono avere un qualche impatto sui mercati e finanche l'umore degli investitori.

<sup>34</sup> Secondo le acquisizioni scientifiche più recenti, un soggetto impiega circa 5 minuti a leggere un articolo di giornale e 3 secondi a scrivere un c.d. "tweet" di 140 caratteri. Diversi ovviamente sono i tempi di operatività delle macchine algoritmiche, la cui velocità di negoziazione dipende dalla potenza dei processori utilizzati e trova il limite della velocità della luce, rispetto al quale la distanza fisica tra i due nodi della rete di comunicazione incide sul tempo di trasferimento di un dato da un nodo all'altro. Dunque, per i sistemi che usano l'HFT risulta determinante non solo dotarsi dei *software* e degli *hardware* più potenti, ma anche riuscire ad abbattere le distanze fisiche dai centri di negoziazione in quanto ciò consente di ridurre ulteriormente i tempi di c.d. latenza e permette la conclusione di una negoziazione profittevole (*ex multis*, cfr. J.J. ANGEL, *When Finance Meets Physics: The Impact of the Speed of Light on Financial Markets and Their Regulation*, in *The Financial Review*, 2014, 273).

<sup>35</sup> In questi termini ancora PUORRO, *op. cit.*, in part. 9.

<sup>36</sup> Cfr. J.H. HARRIS, P.H. SHULTZ, *The trading profits of SOES bandits*, in *Journal of Financial Economics*, vol. 50, 1997, 39.

essere più basso rispetto al *best price* che in quello stesso momento esprimeva, sul medesimo prodotto, il mercato regolamentato, con conseguente danno per l'investitore che aveva scelto di operare su una piattaforma alternativa al mercato regolamentato.

Proprio l'esigenza di ridurre il rischio inefficienza per i sistemi automatizzati che operavano sugli ECN, diede impulso allo sviluppo di AT dotati di algoritmi e infrastrutture tecnologiche che potessero consentire loro di operare in modo molto rapido. La potenziale presenza sul mercato di prezzi diversi per gli stessi strumenti finanziari aumentava, infatti, le possibilità di sfruttare l'arbitraggio, a tutto vantaggio degli operatori che, operando più rapidamente degli altri e potendo elaborare più efficacemente le informazioni presenti nei vari mercati, riuscivano a utilizzare a proprio favore le discrepanze di prezzo che concretamente, di volta in volta, si formavano. E così l'operatore più rapido e informato poteva, nello stesso momento, comprare al prezzo più basso presente sul mercato, spesso offerto dal *trader* meno informato, e vendere al prezzo più alto. In tal modo egli realizzava un guadagno a rischio zero, sfruttando a proprio vantaggio tanto le differenze di prezzo quanto l'asimmetria informativa che, come visto, dipendevano dalla struttura stessa dei mercati. Per contrastare questo fenomeno nel 1997 la SEC impose ai *market maker* l'obbligo del *Limit Order Display*, e cioè di mostrare a tutti i *trader* quale fosse il miglior prezzo di acquisto e vendita presente in qualsiasi momento sull'intero mercato, ECN compresi.

Un ulteriore importante impulso allo sviluppo della tecnologia alla base dell'HFT è rinvenibile nell'intervento normativo, che si ebbe negli Stati Uniti nel 2007, denominato *Regulation National Market System* (Regulation NMS). Con tale intervento, vennero emanate due regole che ebbero un impatto notevole sul fenomeno in parola<sup>37</sup>.

Con la prima – denominata *Sub Penny Rule* (Rule 612) – la SEC statunitense impose a tutti i mercati di utilizzare il sistema decimale per calcolare le quotazioni dei prezzi dei titoli azionari superiori o uguali all'unità. Ciò limitò il c.d. *bid-ask spread*, riducendo il costo della singola compravendita azionaria per l'investitore e spingendo al contempo i *trader* a sviluppare sistemi algoritmici di negoziazione sempre più sofisticati per poter approfittare di oscillazioni minime di prezzo.

Con la seconda regola – denominata *Order Protection Rule* (Rule 611) – la SEC superò i problemi legati all'inefficienza strutturale delle ECN, lega-

---

<sup>37</sup> Cfr. R. PANCS, *Designing Order-book transparency*, in *Electronic Communication Network*, in J. Eur. Econ. Association, 2014, 24.

ti alla mancanza di scambi informativi, e, al contempo, sostituì il concetto di *best execution* con quello di *best price*, a tenore del quale il *broker* che riceve un ordine di acquisto o di vendita è obbligato a trasferirlo sul mercato dove sia presente il miglior prezzo di mercato, se nel mercato in cui egli opera non vi è la possibilità di offrire il prezzo migliore.

#### 4.1. Velocità e intensità delle negoziazioni come fattori concorrenziali

A ben vedere, le vicende normative appena ricordate, se pure piuttosto recenti, appaiono già pezzi di storia, tanto rapidamente si sono evoluti i mercati finanziari negli ultimi lustri. A riguardo, basti pensare che soltanto negli Stati Uniti – dove sino a poco fa, come detto, si operava soltanto sui mercati regolamentati – ci sono attualmente oltre sessanta sedi di negoziazione per i titoli azionari che operano tra loro in concorrenza.

Questo contesto, oltre a risultare del tutto innovativo rispetto al passato, spiana la strada alla possibilità – per chi svolge *trading* in alta frequenza e riesce ad essere più abile e veloce dei concorrenti – di ottenere ottimi risultati anche minimizzando, per le ragioni sopra indicate, i rischi<sup>38</sup>.

Per tale ragione, oggi, l'attenzione degli operatori di mercato più organizzati e aggressivi è fortemente concentrata sulla possibilità di ottenere, dai propri strumenti tecnologici di *trading*, *performance* sempre più alte in termini di velocità di assunzione ed esecuzione di una decisione negoziale sul mercato così come in termini di volumi di operazioni negoziali effettuate nel minor tempo possibile. È evidente, infatti, che quante più operazioni il singolo *trader* riuscirà ad effettuare nel minor tempo possibile per condizionare l'operato dei suoi concorrenti, o anche solo per anticiparlo, tanto più esso riuscirà a trarre utilità da quelle operazioni. E ciò risulterà ancora più chiaro alla luce di quanto si evidenzierà nel paragrafo che segue circa le più comuni strategie adottate da chi effettua HFT.

In questa prospettiva, ferma la determinante rilevanza della potenza dei *software* e degli *hardware* utilizzati dal singolo operatore, fondamentale risulta anche l'abbattimento dei c.d. tempi di latenza dovuti alla distanza fisica tra i *server* dei *trader* e le piattaforme di mercato<sup>39</sup>.

---

<sup>38</sup> Cfr., sul punto, M.B. FOX, L.R. GLOSTEN, G.V. RAUTERBERG, *High-Frequency Trading and the New Stock Market: Sense and Nonsense*, cit.

<sup>39</sup> Per latenza si intende il tempo che si impiega a realizzare la serie di operazioni necessaria a tramutare una decisione nella sua esecuzione. Nei mercati finanziari, per come oggi struttura-

In altre parole, posto che gli ordini di borsa sono impulsi elettrici che, pur viaggiando a velocità altissime, incontrano i limiti dello spazio fisico da percorrere, come già anticipato<sup>40</sup>, per un *trader* che voglia essere all'avanguardia, dotarsi di un sistema basato su un efficiente algoritmo ed un potente processore informatico potrebbe non bastare a vincere la concorrenza con gli altri operatori di mercato. E ciò perché la distanza fisica dalle piattaforme dove i titoli vengono effettivamente negoziati impedisce ad una decisione, che pure sia stata assunta in modo efficiente e rapido, di arrivare sul mercato altrettanto rapidamente. Inoltre, la stessa distanza può rallentare anche l'attività di acquisizione delle informazioni di mercato che il *software* deve svolgere momento per momento. Il che aggrava ulteriormente il processo decisionale ed esecutivo che l'automa deve compiere per raggiungere il risultato profittevole perseguito.

Per ovviare a questi problemi, diverse società private hanno realizzato, o stanno realizzando, infrastrutture di rete sempre più moderne e sicure per accelerare e rendere meno rischioso il trasferimento dei dati da un punto della rete ad un altro così da favorire *performance* ancora più concorrenziali agli operatori di HFT. Determinante, tuttavia, è avere un *server* fisicamente non lontano dalla piattaforma di negoziazione preferita.

In questo contesto è emerso il fenomeno della c.d. *co-location*, e cioè del servizio commerciale, offerto dalle stesse piattaforme di negoziazione, che consente ai partecipanti al mercato, o comunque a qualsiasi interessato, di prendere in locazione spazi (c.d. *racks*) in prossimità delle piattaforme di mercato al fine di collocarvi i propri *server*. Un'alternativa alla *co-location* è il c.d. *proximity central hosting*, e cioè un servizio di ospitalità informatica che un soggetto terzo offre agli interessati per consentire a questi ultimi di operare i propri ordini di mercato da una posizione fisica prossima a quella della piattaforma prescelta. Su entrambe le questioni – *co-location* e *proximity central hosting* – si registrano, anche in Europa, recenti interventi regolatori finalizzati a garantire agli operatori la parità di condizioni di accesso ai diversi servizi, come più avanti sinteticamente si evidenzierà.

---

ti, la latenza, al netto dei discorsi già fatti sulla velocità di elaborazione dei dati e di assunzione della decisione di investimento (o disinvestimento), è molto importante in relazione al tempo che intercorre fra l'assunzione di una tale decisione da parte dell'operatore e la ricezione del relativo ordine da parte del *broker*, e poi in relazione al tempo necessario a quest'ultimo per processare l'ordine (e dunque comprenderlo in tutte le sue componenti) e per inviarlo al mercato in cui è trattato lo strumento finanziario oggetto dell'ordine stesso, e infine in relazione al tempo intercorrente tra la ricezione dell'ordine da parte del mercato e la divulgazione del dato a tutti i partecipanti allo stesso.

<sup>40</sup> Cfr. nota 34.

## 4.2. HFT e rischi di market abuse

La sempre più diffusa operatività del *trading* finanziario ad alta frequenza ha determinato l'insorgenza sul mercato, o comunque l'aggravamento, di alcune situazioni considerate patologiche e cioè non idonee a favorire adeguate condizioni di sviluppo del mercato stesso, oltre che la possibilità di compiere abusi da parte degli operatori più spregiudicati a danno degli investitori meno avvertiti ed organizzati.

Il primo problema osservato a riguardo – e che, se pure non esclusivamente attribuibile agli HFT, è strettamente correlato (anche) all'uso delle tecnologie di negoziazione più dinamiche e aggressive – è quello della c.d. “*ghost liquidity*”. In breve, può accadere che, grazie all'uso delle tecnologie di *trading* ad alta frequenza più moderne, in un dato momento – e ciò accade soprattutto quando sui mercati c'è turbolenza – si impennino i volumi scambiati, e ciò in ragione del fatto che: 1) gli automi, in un tale contesto, per minimizzare i rischi possono decidere di porre in essere strategie di brevissimo periodo (compro e vendo in pochi minuti); e 2) gli automi tra loro si condizionano inevitabilmente, sicché, se un automa decide di comprare in modo massiccio un certo titolo, gli altri automi, che raccolgono in tempo reale l'informazione sul mercato e la relativa oscillazione del prezzo, possono decidere di comprare anch'essi, quel titolo o altri titoli, e così può succedere che si determini un momento positivo di borsa ed anche che un momento positivo si trasforma in momento di euforia. Ciò genera la sensazione che nel mercato sia entrata nuova liquidità, quando invece tale liquidità non c'è, tanto che di lì a poco, in ragione della strategia di breve periodo di cui si diceva, è probabile che gli automi comincino a vendere per monetizzare il guadagno (e cioè l'aumento di prezzo del titolo) e che anche questa dinamica ribassista, per lo stesso meccanismo di condizionamento appena cennato, si produca rapidamente.

La teoria economica, inoltre, ha individuato alcune strategie, tipicamente adottate da chi opera sui mercati finanziari in alta frequenza, che, se poste in essere da operatori dotati di portafogli considerevoli o forte liquidità e tecnologie all'avanguardia, sono in grado di generare rappresentazioni distorte del c.d. *book* di negoziazione e, di conseguenza, abusi di mercato da parte degli stessi.

Tra queste, le più conosciute sono il c.d. *stuffing*, il c.d. *smoking*, il c.d. *spoofing*, il c.d. *layering* e il c.d. *front running*.

Con il termine *stuffing* si fa riferimento alla pratica consistente nell'immettere, attraverso sistemi di *trading* ad alta frequenza, un elevato numero di ordini nel mercato nello stesso momento così da creare un effetto “neb-

bia”, e cioè così da impedire agli *slow traders*, e quindi agli operatori che non usano tecnologie avanzate, l'immediata esatta percezione di ciò che sta avvenendo; il tutto al fine di utilizzare la paralisi dei concorrenti per compiere operazioni profittevoli.

Lo *smoking* è, invece, la pratica consistente nella immissione sul mercato di ordini allettanti su uno o più prodotti – c.d. ordini civetta o “fumo senza arrosto” – con l'obiettivo di attrarre l'attenzione degli altri operatori, e soprattutto degli *slow traders*, per poi, subito dopo, modificare le condizioni di *trading* relative ai prodotti in questione e approfittare della lentezza con cui gli altri operatori si accorgono della modifica occorsa.

Con il termine *spoofing* si identificano le operazioni compiute dai *trader* al fine di alterare l'andamento del prezzo di un prodotto target (o comunque le condizioni di negoziazione dello stesso). In estrema sintesi, se un *trader* ha intenzione di vendere un prodotto del suo portafoglio, al fine di farne salire il prezzo e vendere ad un prezzo più alto rispetto al miglior prezzo espresso in quel momento dal mercato, può immettere nel sistema ordini massicci di acquisto di quel prodotto al fine di indurre i concorrenti a credere che vi sia realmente un aumentato interesse per quel prodotto, e dunque che vi siano buone probabilità che il titolo cresca di valore e che, di conseguenza, convenga comprarlo. La reattività che il mercato esprime rispetto a fenomeni del genere, anche in relazione al fatto che gli automi tra loro (come si è già osservato) si osservano e condizionano, più determinare in tempi rapidissimi una dinamica al rialzo del prezzo del prodotto in questione. Nel frattempo il *trader* che ha dato inizio a tale dinamica, sfruttando la velocità dei propri sistemi, avrà revocato gli ordini che aveva lanciato prima ancora che fossero eseguiti, ed avrà immesso nel sistema gli ordini di vendita ai quali era effettivamente interessato sin dal principio, concludendo operazioni per lui profittevoli in quanto le vendite si perfezioneranno, con tutta probabilità, ad un prezzo superiore a quello di partenza.

Il termine *layering* identifica una variazione della pratica appena descritta, consistente nel fatto che il *trader* interessato a ispirare un movimento del mercato di segno opposto rispetto all'operazione che egli ha intenzione di compiere su un certo prodotto, o su certi prodotti, piuttosto che immettere sul mercato i due diversi ordini, e cioè quello destinato ad essere revocato e quello effettivo, a distanza (se pure modesta) di tempo, li immette entrambi nello stesso istante, ma il primo in modo visibile agli altri operatori e il secondo come “ordine nascosto” (e dunque non visibile nel *book* di negoziazione). In tal modo con l'ordine palese si induce il mercato a credere in un certo movimento del mercato, mentre con l'ordine na-

scosto si opera in senso contrario e si approfitta della reazione avuta dal mercato all'ordine palese nel frattempo revocato.

L'ultima, e forse più avversata, pratica che qui merita di essere considerata è quella individuata dalla locuzione *front running*. Questa può essere posta in essere solo da intermediari che operano sul mercato sia in conto proprio che in conto di terzi. E consiste nel fatto che il *trader*, conoscendo l'ordine che per il suo cliente si accinge ad immettere sul mercato, sfrutta la velocità consentita dai propri sistemi informatici di negoziazione per immettere sul mercato un ordine in conto proprio (analogo o inverso a quello del cliente) pochi istanti prima di immettere sullo stesso mercato l'ordine del cliente.

Come evidente già da queste poche ed elementari annotazioni, l'uso dei sistemi di *trading* ad alta frequenza consente di porre in essere condotte manipolative dei mercati che, a brevissimo termine, possono realizzare grandi utilità per i *trader* più aggressivi e organizzati, ma che nel contempo, oltre a penalizzare gli altri operatori, rischiano di determinare effetti emulativi e, dunque, ulteriormente distorsivi dei mercati. Con la conseguenza, più in generale, di determinare, nel medio periodo e su tutti i mercati, condizioni di negoziazione non più efficienti<sup>41</sup>. Il tutto, va da sé, nella misura in cui le autorità competenti non risultino in grado di evitare il compimento delle pratiche in parola. Visto che, in caso contrario e come già accennato, secondo alcuni autori l'uso dei sistemi di negoziazione ad alta frequenza può addirittura migliorare la qualità dei mercati in termini di volatilità, liquidità, informazione e prezzi.

Proprio per evitare che gli algoritmi vengano utilizzati in modo fraudolento e cioè per determinare abusi di mercato, le autorità di regolazione dei mercati e i legislatori dei Paesi più evoluti sono intervenuti con apparati normativi che affrontano il tema del *trading* finanziario ad alta frequenza, come si evidenzierà nei prossimi due paragrafi.

---

<sup>41</sup> In ragione dei rischi legati all'uso del trading ad alta frequenza, e dunque al fine di perseguire la stabilità e la sicurezza dei mercati, negli Stati Uniti è nato, nel 2013, lo IEX, e cioè una piattaforma informatica – attualmente di proprietà di alcuni fondi di investimento – in cui è possibile compravendere titoli di borsa con modalità alternative rispetto a quelle permesse sulle altre piattaforme, e in particolare con modalità che ostacolano il *trading* ad alta frequenza. Ad esempio, per evitare l'arbitraggio predatorio si impone una latenza minima degli ordini (350 millisecondi ad operazione), si vieta la co-location e si impediscono gli accessi privilegiati alle informazioni del mercato da parte di alcuni operatori piuttosto che di altri. Cfr. E. PICARDO, *How IEX Is Combating Predatory Types of High-Frequency Traders*, in *Forbes – Investopedia*, disponibile on-line all'indirizzo «<https://www.forbes.com/sites/investopedia/2014/04/23/how-iex-is-combating-predatory-types-of-high-frequency-traders/>».

Resta da sottolineare un dato non banale nell'ambito della riflessione che qui si sta svolgendo: malgrado milioni siano ogni giorno le operazioni finanziarie rientranti nel concetto di *algorithmic trading*, non si registrano al momento – o, quanto meno, non sono balzati agli onori delle cronache, né si sono imposti all'attenzione degli studiosi – casi significativi di dispute tra le parti private di una transazione finanziaria conclusa attraverso automi.

Non si sono posti, dunque, nella prassi significativi problemi concernenti il cattivo funzionamento degli automi e le conseguenti responsabilità, con riguardo, ad esempio, al mancato perfezionamento del contratto, o al fraintendimento della volontà negoziale, o all'errore occorso nell'immettere una informazione nel sistema o nel dare esecuzione ad un impulso elettronico, o altro ancora<sup>42</sup>. E ciò perché, da un lato, chi utilizza gli algoritmi accetta i rischi inevitabilmente a questi connessi (ovviamente, cercando di ridurli al minimo possibile e assicurandosi contro l'eventualità che si verificano problemi), dall'altro la velocità degli scambi e l'importanza che fiducia e reputazione hanno nei mercati finanziari sconsigliano, quando non impediscono del tutto, che eventuali contestazioni circa la correttezza di una operazione automatizzata vengano dalle parti rese conoscibili per i terzi, essendo queste piuttosto trattate tra le parti stesse e risolte attraverso sistemi di composizione delle liti di carattere esclusivamente privato<sup>43</sup>.

Senza considerare, più in generale, le difficoltà riscontrate anche dalle autorità di vigilanza nel rintracciare il *software*, e dunque il sistema automatico, che ha determinato una certa dinamica di mercato, a valutarne l'operato in termini di liceità o illiceità, e ad attribuire le conseguenti responsabilità sia di carattere civile, che amministrativo e penale. Si può, sotto questo profilo, tranquillamente parlare di una evidente inefficienza delle regole giuridiche tradizionali a governare il fenomeno<sup>44</sup>.

---

<sup>42</sup>Le cronache in questi anni hanno raccontato numerosi casi di errori (o presunti tali) commessi dagli automi che operano sui mercati finanziari e che hanno determinato significativi movimenti di borsa e/o ingenti danni per i *trader* coinvolti. Più in generale, sul tema, cfr. I. ALDRIDGE – S. KRAWCIW, *Real-time Risk. What Investors Should Know about Fin-Tech, High Frequency Trading and Flash Crashes*, Hoboken, New Jersey, USA, 2017.

<sup>43</sup>Cfr., *ex ceteris*, T. ANDREOTTI, *Dispute resolution in transnational security transaction*, Hart Publishing Plc, Oxford and Portland (Oregon, USA), 2017.

<sup>44</sup>Per interessanti considerazioni circa le ragioni e le proporzioni di tale fallimento, v. Y. Yadav, *The Failure of Liability in Modern Markets*, in *Virginia Law Review*, vol. 102, 2016, 1031.

### 4.3. I primi tentativi di regolare gli HFT

I primi interventi normativi relativi all'HFT, come noto, risalgono al periodo in cui, dopo il *crash flash* del 2010 di cui si è detto, due organi fondamentali nella cornice regolamentare statunitense, la SEC e la *Commodity Futures Trading Commission* (CFTC), presentarono congiuntamente una relazione con l'obiettivo di rispondere prontamente all'episodio che aveva ingenerato nutriti timori sull'operatività del *trading* ad alta frequenza.

La prima risposta regolamentare statunitense consistette nella creazione di un meccanismo di identificazione dell'attività di soggetti – c.d. *large trader* – che, avendo volumi di negoziazione molto elevati, anche in ragione delle proprie capacità tecniche-informatiche e della propria organizzazione, con la loro attività possono condizionare il mercato dei prezzi<sup>45</sup>. E ciò al fine di rendere più semplice, per le autorità stesse, il controllo dell'attività di questi soggetti anche attraverso l'imposizione di obblighi informativi in capo a questi ultimi e a favore delle medesime autorità.

Tale intervento normativo trovò spazio nell'ampia riforma regolamentare, denominata “*Dodd-Frank Wall Street Reform and Consumer Protection Act*”, fortemente voluta dall'amministrazione di Barack Obama, al fine di promuovere una più completa regolazione dei mercati statunitensi e una miglior tutela dei consumatori<sup>46</sup>.

Tra le novità più significative che la riforma in parola esprime in materia di HFT, giova segnalare: a) la possibilità da parte della SEC di richiedere agli *hedge funds* di redigere report che contengano informazioni relative, ad esempio, ai tipi di asset posseduti o al loro ammontare, e renderli pubblici, oltre ad ogni altra informazione utile a valutare il fondo; b) l'istituzione di un nuovo istituto, denominato *Financial Stability Oversight Council* (FSOC), con compiti di supervisione sulla stabilità del mercato e sulla sorveglianza del sistema finanziario; c) una regolamentazione più stringente anche per il *Commodity Market*, nel quale si fa divieto di revocare o cancellare ordini.

---

<sup>45</sup> Cfr. R.E. PRASCH, *The Dodd-Frank Act: Financial Reform or Business as Usual*, in *J. Economic Issues*, 2012, 186; M. RICHARDSON, *Regulating Wall Street: the Dodd-Frank Act*, in *Economic Perspectives*, 2012, 45.

<sup>46</sup> Il documento ufficiale contenente la riforma denominata, dallo stesso legislatore americano, “*Dodd-Frank Wall Street Reform and Consumer Protection Act*” (12 USC 5301), ed approvata il 21 luglio 2010, può leggersi on-line all'indirizzo «<https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf>». Cfr., *ex multis*, M. RICHARDSON, *Regulating Wall Street: the Dodd-Frank Act*, in *Economic Perspectives*, 2012 199.

A ciò si aggiunga che la SEC, subito dopo l'entrata in vigore della riforma in parola, ha emanato due regole, la *Rule 13b* e la *Rule 13b-1190*, che prevedono: i) l'imposizione ai large trader di identificarsi come tali attraverso documentazione scritta per ottenere il *Large Trader Identification Number* (LTID), *conditio sine qua non* per operare in tale veste sui mercati; ii) l'obbligo per tali soggetti di presentare il proprio numero identificativo di *trader* di tal genere a tutti i *broker* e/o *dealer* attraverso i quali gli stessi effettuavano negoziazioni sul NMS; iii) l'imposizione per i *brokers* e/o *dealers* di fornire alla SEC su richiesta specifica ed entro la mattina del giorno successivo all'operazione suddetta, dati relativi alle transazioni effettuate dai large traders su NMS; iv) l'obbligo per i *brokers* e/o *dealers* di conservare e aggiornare costantemente libri contabili e scritture relative a tali negoziazioni<sup>47</sup>.

Le novità normative in parola, tuttavia, alla prova dei fatti hanno mostrato alcuni gravi limiti, dovuti principalmente al fatto che i sistemi algoritmici sono molto spesso, e sempre di più, talmente performanti, e cioè rapidi e chirurgici nel loro operare, da riuscire ad eludere i controlli delle autorità di vigilanza<sup>48</sup>.

Per questa ragione, negli Stati Uniti l'attuale amministrazione vorrebbe modificare le regole vigenti in materia di HFT, ma sulla direzione da prendere in questa prospettiva ancora non vi è alcuna certezza, posto che alcuni osservatori spingerebbero per l'introduzione di tempi obbligatori di latenza o di permanenza di un ordine sul mercato (e ciò per evitare i fenomeni dello *spoofing*, del *layering* e del *front running*), ed inoltre per imporre, ai *trader* che usano tecnologie finalizzate ad operare in alta frequenza, obblighi di comunicazione ai mercati di particolari notizie così da evitare che questi approfittino dell'asimmetria informativa a danno dei *low traders*, mentre altri osservatori propugnano l'opportunità di una sostanziale deregolamentazione del fenomeno, e ciò per favorire la concorrenza basata sulla competizione tecnologica.

---

<sup>47</sup> Cfr. M. KINI, M.P. HARREL, G.J. LYONS, *Federal Reserve adopts key Dodd-Frank Act definition*, in *Banking Law Journal*, 2013, 47.

<sup>48</sup> Circa l'attuale inadeguatezza del complessivo quadro regolatorio (non solo europeo) rispetto all'impatto che la tecnologia sta avendo sui mercati finanziari, v. anche quanto opportunamente sostenuto da F. CAPRIGLIONE (*Non luoghi, sovranità, sovranismi. Alcune considerazioni*, in *Riv. trim. dir. econ.*, 4, 2018, 404), secondo il quale «il vigente quadro regolamentare si è rivelato presto inadeguato ad offrire soluzioni idonee a conciliare gli esiti positivi della innovazione informatica con l'esigenza di valutarne e controllarne i rischi potenziali».

#### 4.4. Gli AT e gli HFT alla luce delle direttive MIFID I e II

In Europa con le direttive MIFID I e MIFID II sono state introdotte regole significative in materia di operazioni finanziarie svolte attraverso sistemi informatici intelligenti<sup>49</sup>.

In particolare quest'ultima – riconoscendo espressamente gli effetti positivi che l'entrata in scena delle nuove tecnologie informatiche e telematiche ha sortito sui mercati – ha introdotto, o in certi casi definito in modo più completo, alcuni obblighi a carico dei *trader* che utilizzano sistemi di AT ed ulteriori per i *trader* che utilizzano sistemi di HFT.

Tra le novità più significative, in estrema sintesi, vi sono: a) la previsione per cui gli operatori che utilizzano tecniche di *trading* ad alta frequenza devono farsi identificare come tali dalle autorità di vigilanza e dagli altri operatori del mercato; b) l'obbligo a carico delle società di investimento che utilizzano tecniche di *trading* automatico di predisporre opportuni sistemi di organizzazione e di controllo al fine di garantire la resilienza dei propri sistemi di *trading*; c) l'obbligo, per tutte le società che utilizzano tecniche di TA, di svolgere in modo continuativo salvo particolari casi, l'attività di *market making*, e ciò al fine di fornire liquidità al mercato in modo regolare e trasparente; d) l'obbligo, per chi voglia offrire spazi fisici al fine di consentire ai *server* degli operatori di operare in prossimità rispetto alle piattaforme di negoziazione, di garantire a tutti gli operatori pari condizioni affinché la vicinanza non sia appannaggio solo di alcuni e non diventi un fattore competitivo condizionante il mercato; e) la raccomandazione, rivolta ai regolatori dei diversi mercati, a monitorare costantemente le attività svolte sistemi di AT e di HFT ed a favorire una più efficiente struttura delle commissioni degli operatori.

Al di là delle importanti novità appena segnalate, va sottolineato altresì che tra le principali innovazioni introdotte già dalla MIFID – e ribadite

---

<sup>49</sup> Come noto, si tratta della direttiva 2004/39/CE del Parlamento Europeo del 21 Aprile 2004 (denominata *Markets in Financial Instruments Directive*, da cui l'acronimo MIFID), la quale, dal 3 gennaio 2018 è stata sostituita dalla c.d. MIFID II, e cioè dalla MiFID II dalla direttiva (2014/65/EU) che – insieme alla MiFIR, e cioè al regolamento UE 600/2014 denominato *Markets in financial instruments regulation* – oggi costituisce la normativa europea di riferimento in materia. La letteratura in argomento è molto vasta. Tra i gli altri, per un inquadramento generale, sulla MIFID II, cfr. E. PEZZUTO, R. RAZZANTE, *MIFID II: Le novità per il mercato finanziario*, Torino, 2018; V. TROIANO, R. MOTRONI, *La MiFID II, Rapporti con la clientela-regole di governance-mercati*, Padova, 2016; e F. CAPRIGLIONE, *Prime riflessioni sulla MiFID II (tra aspettative degli investitori e realtà normativa)*, in *Riv. trim. dir. ec.*, 2015, 72; mentre sulla MIFID, cfr. F. CAPRIGLIONE, *Intermediari finanziari, investitori, mercati: il recepimento della MIFID. Profili sistematici*, Padova, 2008.

dalla MIFID II – vi sia il riconoscimento dei mercati alternativi a quelli regolamentati, con conseguente corollario costituito dal principio di liberalizzazione delle negoziazioni e con l'ulteriore previsione dell'obbligo di *best execution* nell'esecuzione degli ordini di negoziazione. Tale riconoscimento, per le ragioni già sopra cennate, ha notevolmente favorito l'AT, e in particolare l'HFT.

Dunque, si può tranquillamente dire che in Europa fu proprio la direttiva MIFID, combinata allo sviluppo dei mercati alternativi sopra menzionati e alla progressiva frammentazione del mercato, a dare l'impulso decisivo alla diffusione dell'HFT<sup>50</sup>.

Tornando al tema della differenziazione tra AT e HFT, giova precisare che la negoziazione algoritmica viene definita dall'art. 1 MIFID II come quell'insieme di tecniche di negoziazione dove la scelta dei parametri degli scambi – quali ad esempio, prezzo, quantità e momento in cui completare la negoziazione – vengono rilasciati alla “scelta” di un algoritmo altamente informatizzato. La decisione automatica che caratterizza l'AT, tra l'altro, non si limita ai parametri della singola contrattazione, ma si estende anche al “se inviare l'ordine” e come gestire la posizione una volta conclusa la negoziazione.

La MIFID II individua, quindi, come caratteristica fondamentale dell'AT la presenza nulla, o comunque minima, dell'intervento umano nelle transazioni aventi ad oggetto strumenti finanziari. Pertanto, sul piano regolatorio, devono essere incluse in questa categoria tutte le negoziazioni in cui un algoritmo informatico sostituisce l'attività decisionale dell'uomo, in ordine all'effettuazione di una scelta di *trading*. Lo stesso articolo considera, invece, estranei a tale fattispecie tutti i sistemi informatici utilizzati unicamente per: trasmettere ordini a una o più sedi di negoziazione, trattare ordini che non comportano la determinazione di parametri di *trading*; confermare ordini, nonché eseguire il trattamento post-negoziazione delle operazioni eseguite<sup>51</sup>.

Per quanto riguarda la negoziazione algoritmica ad alta frequenza, la MIFID II, ribadendo il concetto che l'HFT è una specie del più ampio *genus* dell'AT, individua una specifica e più vincolante regolamentazione per la fattispecie in parola. La stessa viene descritta e identificata come quel-

---

<sup>50</sup>In questo senso, cfr. ESMA, *High-frequency trading activity in EU equity markets*, *Economic Report*, nr. 1, 2014, in part. 5.

<sup>51</sup>Si escludono pertanto, l'insieme dei sistemi di *trading*, seppur altamente sofisticati e computerizzati, che servono esclusivamente per eseguire e gestire un insieme di ordini già parametrati. Ossia, dove il prezzo, la quantità dell'ordine, e il momento in cui effettuare lo scambio sono già stati impostati con intervento umano. Cfr. D. BUSCH, G. FERRARINI, *Regulation of the EU financial markets: MIFID 2 and MiFIR*, Oxford University Press, Oxford, 2017, in part. 137.

l'insieme di meccanismi di *trading* ad altissima velocità che vengono generalmente utilizzati da operatori che “operano per conto proprio” e che si servono di tale tipo di *trading* per attuare strategie di *market making* (con correlato rischio di *market abuse*) e/o strategie di arbitraggio. Lo stesso art. 1 della MIFID II specifica come tale fattispecie sia caratterizzata da: a) l' utilizzo di «infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, hosting di prossimità o accesso elettronico diretto a velocità elevata»; b) la «determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione»; e c) un «elevato traffico giornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni».

Come anticipato, la differenza ontologica tra le due tecniche di *trading* comporta una differente regolamentazione, soprattutto per quanto riguarda il regime delle esenzioni. Va ribadito, infatti, che l'HFT è considerato, in virtù delle sue caratteristiche e potenzialità, più pericoloso per il mercato (cfr. considerando n. 62 della MIFID II), tanto che l'applicazione di una tecnica di «negoziazione algoritmica ad alta frequenza» impone l'applicazione delle relative norme, di cui alla MIFID II, anche «alle persone che negoziano per conto proprio in strumenti finanziari diversi dagli strumenti derivati su merci o dalle quote di emissione o relativi strumenti derivati e che non prestano altri servizi di investimento o non esercitano altre attività di investimento in strumenti finanziari diversi dagli strumenti derivati su merci, dalle quote di emissione o relativi derivati». Mentre, laddove queste «persone» si limitino ad usare tecnologie informatiche non ad alta frequenza, alle stesse non sarà applicabile la disciplina relativa all'AT.

Le regole introdotte in sede di approvazione della MIFID II sono ispirate anche da (e in ogni caso riposano su) l'intenso lavoro che in tema di AT e di HFT sta compiendo l'ESMA sin dal 2010 (quando ancora operava come CESR). Nel 2010, infatti, fu diramata dall'autorità una *Call for Evidence* per sondare i problemi strutturali dei mercati finanziari alla luce dell'impatto delle nuove tecnologie, mentre nel 2011 la stessa pubblicò un documento di consultazione denominato «*Guidelines on systems and controls in a highly automated trading environment for trading platforms, investment firms and competent authorities*», al quale seguì il 24 febbraio 2012 la pubblicazione delle *Guidelines* (Orientamenti) ESMA in materia, con identico titolo<sup>52</sup>.

Tali orientamenti – giova precisarlo – sono espressamente dichiarati

---

<sup>52</sup>Le *Guidelines* sono disponibili on-line, nel sito Internet ufficiale dell'ESMA, all'indirizzo <[https://www.esma.europa.eu/sites/default/files/library/2015/11/esma\\_2012\\_122\\_en.pdf](https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf)>.

applicabili anche a soggetti che non sono imprese di investimento e che non sono soggetti alla MIFID, se ed in quanto trattasi di operatori che accedono in qualsiasi modo alle piattaforme di negoziazione, e cioè, direttamente ovvero tramite il c.d. *Direct Market Access* (e cioè tramite una forma di accesso elettronico che permette l'ingresso nel mercato a diversi soggetti, intermediari e non, senza che questi debbano divenire membri dello stesso, attraverso l'uso delle infrastrutture e dei sistemi messi a disposizione da uno o più partecipanti) ovvero ancora tramite il c.d. *Sponsored Access* (e cioè tramite un accordo in forza del quale un membro del mercato consente ai propri clienti di accedere al mercato usando il proprio ID, al fine di immettere direttamente sul mercato gli ordini, senza usufruire però dell'infrastruttura del membro stesso).

Sintetizzandone al massimo il contenuto, si può affermare che con essi l'ESMA ha voluto perseguire principalmente due obiettivi, e cioè: *in primis*, quello di garantire un equo e ordinato svolgimento delle negoziazioni, dando particolare rilievo alla sostanziale parità di condizioni e di informazioni tra tutti coloro che operano sul mercato; ed inoltre quello di evitare che gli utilizzatori di sistemi di *trading* ad alta frequenza possano porre in essere abusi di mercato<sup>53</sup>.

L'importanza delle *Guidelines* e del ruolo dell'ESMA negli assetti dei mercati finanziari europei è confermato dall'ampliamento dei poteri dell'autorità disposto dalla MIFID II, la quale stabilisce che l'ESMA, mantenendo comunque invariata la possibilità di emanare atti di *soft law* quali ad esempio quello di formulare "Raccomandazioni" e "Orientamenti", potrà e dovrà emanare vere e proprie norme tecniche di regolamentazione relativamente ad alcune aree del vasto tema della negoziazione algoritmica e più nello specifico della negoziazione algoritmica ad alta frequenza.

## 5. La consulenza finanziaria e la c.d. robo advisor

Nell'ambito finanziario uno dei campi in cui l'innovazione tecnologica – in particolare, intesa come applicazione dell'intelligenza artificiale, e dunque della scienza algoritmica e dei Big Data – sta avendo maggiore spazio è quello della consulenza in servizi finanziari<sup>54</sup>.

---

<sup>53</sup> Gli orientamenti in parola, ai sensi del d.lgs. n. 58/1998 (TUF) e relative disposizioni di attuazione contenute nel regolamento Consob n. 16191/2007, sono stati recepiti nel nostro Paese – se pure solo in parte – dalla Consob medesima con la Comunicazione del 4 aprile 2012.

<sup>54</sup> In Italia, sul tema al momento si segnalano M.T. PARACAMPO, *Robo-advisor, consulenza*

In estrema sintesi, per inquadrare il fenomeno va evidenziato che da alcuni anni nel mercato si stanno sviluppando e diffondendo *software* – disponibili principalmente su piattaforme digitali presenti in Internet e detti *robo advisor* – che puntano ad affiancare il cliente e supportarlo nelle decisioni di investimento finanziario, suggerendo a quest’ultimo le operazioni da svolgere per ottimizzare i risultati perseguiti. Così operando tali sistemi informatici sostanzialmente puntano a sostituire la figura del consulente finanziario e cioè di colui che, tradizionalmente, assiste il cliente, che abbia deciso di usufruire di tale servizio professionale, nelle sue scelte di investimento. Essi, infatti, in un primo momento raccolgono – dalla interazione con il cliente, ma non solo – quante più informazioni possibili circa quest’ultimo, la sua propensione all’investimento e al rischio, le sue disponibilità finanziarie, le sue conoscenze del mercato, la sua esperienza di investitore e quant’altro. Poi, sulla base di queste informazioni, propongono al cliente delle soluzioni di investimento elaborate in automatico dagli algoritmi.

In realtà, i *robo advisor* attualmente conosciuti presentano tra loro molte differenze strutturali ed operative, che rendono difficile una trattazione unitaria del fenomeno, in quanto alcuni software sono effettivamente rivolti ad assistere direttamente il cliente, mentre altri si propongono come ausiliari all’operatività del consulente finanziario, ed altri ancora appaiono come ibridi, e cioè come strumenti disponibili anche all’uso diretto da parte dei clienti ma più propriamente pensati per essere fruiti da un cliente esperto di mercati, e dunque tendenzialmente un professionista del settore<sup>55</sup>.

In ogni caso, secondo una recente analisi di mercato, a livello globale le attività finanziarie gestite attraverso sistemi di *robo advise*, a settembre

---

*finanziaria* e profili regolamentari, in *Riv. trim. dir. econ.*, supplemento al n. 4/2016, 256; ID., *La consulenza finanziaria automatizzata*, in M.T. PARACAMPO (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017, 127; ID., *L’adeguatezza della consulenza finanziaria automatizzata nelle linee guida dell’ESMA tra algogovernance e nuovi poteri di supervisione*, in *Riv. dir. bancario*, 2018, 8; F. SARTORI, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Riv. trim. dir. econ.*, 3, 2018, 269; R. LENER, *La digitalizzazione della consulenza finanziaria. I robo advise e le regole MIFID*, in *FCHub*, disponibile on-line, in Internet, alla pagina <https://fchub.it/la-digitalizzazione-della-consulenza-finanziaria-i-robo-advise-e-le-regole-mifid/>; R. LIACE, *Robo advisor e finanza comportamentale*, in F. FIMMANÒ, G. FALCONE (a cura di), *Fin-Tech*, Napoli, 2019, 195; e, nello stesso volume a cura di Fimmanò e Falcone, anche U. MORERA, *Consulenza finanziaria e robo advisor, profili cognitivi* (p. 203), e D. ROSSANO, *La consulenza finanziaria automatizzata e la tutela degli investitori* (p. 209).

<sup>55</sup> Tra le diverse pubblicazioni (non giuridiche) apparse in Italia circa il fenomeno dei *robo advisor* operanti nel mercato finanziario, particolarmente efficace per un primissimo inquadramento fenomenologico risulta l’agile lavoro a firma di E. MALVERTI, D. BULGARELLI e G. VILLA, *Fintech. La finanzia digitale. Strategie di investimento con i roboadvisor*, Hoepli, Milano, 2018.

2019, ammonterebbero a circa 980 miliardi di dollari americani<sup>56</sup>. In particolare, negli Stati Uniti – dove è nato, nel 2008, il concetto di consulenza finanziaria automatizzata (convenzionalmente si ritiene che il primo servizio di questo tipo, per quanto rudimentale, fu offerto da Bettermint) – il totale AuM (*Asset under Management*) gestito dai consulenti robotizzati ammonterebbe a quasi 750 miliardi di dollari (circa il 2% del mercato) e gli investitori coinvolti sarebbero poco più di 8 milioni (circa 8.230mila), con un ammontare medio di patrimonio per utente pari a circa 90.000 dollari.

Negli ultimi anni in Asia il settore ha visto un'enorme crescita grazie alla sua diffusione tra numerosissimi utenti della categoria *mass market*. Tuttavia, a settembre 2019 si stima esso esprima in Cina un valore complessivo pari a poco più di 179 miliardi di dollari, e dunque ancora molto lontano dal dato a stelle e strisce.

Nella speciale classifica degli Stati, stilata in funzione degli AuM gestiti da robot, dopo Stati Uniti e Cina ci sarebbero, nell'ordine, Regno Unito (con quasi 15 miliardi di dollari, per la precisione 14,803m), Germania (con 8,460 miliardi) e Canada (con 5,448 miliardi). Il dato italiano appare molto più modesto, attestandosi sui 413 milioni di dollari.

Si tratta, come evidente, di dati nettamente positivi, che segnano, a livello mondiale, la progressiva acquisizione di sempre maggiori spazi di mercato per la consulenza finanziaria automatizzata, la quale – come noto – promette agli utenti (e agli operatori) bassi costi, efficienza e azzeramento del rischio di comportamenti impropri da parte dei consulenti.

Senonché, per gli stessi analisti il *trend* di crescita della consulenza finanziaria robotizzata di qui al 2023 subirà una forte contrazione, avendo fatto segnare un +124,5% nel 2018 (sul 2017) ma solo un +76,1% nel 2019 (sul 2018), con (soprattutto) previsioni per gli anni a venire nell'ordine di +39,9% nel 2020, +20,8% nel 2022 e +5,8% nel 2023.

Le ragioni di questa ipotizzata contrazione, o meglio di questa attesa frenata della crescita di un fenomeno spesso guardato con grande sospetto dai regolatori e con grande timore dai consulenti finanziari, sono molteplici. Tra queste un ruolo particolarmente significativo spetta, probabilmente, ai limiti intrinseci che l'intelligenza artificiale (almeno ancora oggi) mostra allorquando viene applicata per supportare gli investitori nel compimento di scelte operative che necessitano di alta personalizzazione, e cioè che devono essere calibrate non solo sul patrimonio e sugli obiettivi di investi-

---

<sup>56</sup>Fonte "Statista". I dati riportati sono tutti disponibili on-line, Internet, alla pagina <https://www.statista.com/outlook/337/100/robo-advisors/worldwide>.

mento espressi dal singolo, ma anche sulla sua cultura, sulla sua personalità e sulla sua intima propensione sincronica al rischio.

Non a caso già nel 2017 nella dottrina italiana c'era chi, dopo aver valutato i servizi offerti da 44 operatori attivi nel nord-America e in Europa, osservava come la *robo-advise*, pur comportando un elevato contenuto relazionale e tecnico, venisse ancora tendenzialmente considerata dagli investitori come elitaria e esclusiva, in quanto la perseguita semplificazione (attraverso la riduzione ad algoritmi) di un'attività complessa qual è la consulenza finanziaria non viene percepita esattamente come tale dall'utente medio<sup>57</sup>.

In estrema sintesi, si può affermare, mutuando l'esperienza empirica raccolta in altri settori, che il consumatore se non ritiene un servizio o un prodotto sicuri (e cioè idonei a non esporlo a rischi superiori a quelli che egli accetta di volta in volta di correre), tende a non utilizzare quel servizio o a non comprare quel prodotto. E ciò, a maggior ragione, in un contesto sempre più complesso quale sono attualmente i mercati finanziari.

La complessità, infatti, viene percepita come rischio, oltre che come opportunità. E, di fronte ad un rischio che si assume crescente, la semplificazione del processo decisionale di investimento può indurre il cliente a rifuggire dal servizio *online* per rifugiarsi nel porto sicuro della relazione umana consolidata con il proprio consulente finanziario. Del resto, Jerry Kaplan – uno dei massimi esperti mondiali di intelligenza artificiale – nel suo *Artificial Intelligence. What Everyone Need to Know* (Oxford University Press, 2016), proprio per questa ragione, tra le attività professionali che meglio resisteranno all'automazione nel prossimo futuro, inserisce quella dei consulenti delle vendite.

Più recentemente, in una diversa prospettiva, un *working paper* dell'EBI ha affermato che la *robo-advise* rappresenta una concreta fonte di nuovi rischi sistemici per i mercati finanziari. Ciò in quanto la consulenza automatizzata, laddove basata su classificazioni generiche, predeterminate e di ampia portata, potrebbe non tenere conto delle preferenze individuali e delle reali esigenze dell'investitore<sup>58</sup>.

Partendo da tale assunto, e considerando l'assenza nell'attuale quadro normativo europeo di norme pensate *ad hoc* per arginare il rischio in parola, il citato lavoro dell'EBI, a firma di Wolf-George Ringe e Christopher Ruof, propone la creazione di un "sandbox regolatorio", e cioè uno spazio

---

<sup>57</sup> P. PIA, *La consulenza finanziaria automatizzata*, Franco Angeli, Roma, e-book, 2017.

<sup>58</sup> Si tratta del *working paper* n. 26/2018 dell'*European Banking Institute* di Francoforte, a firma di Wolf-George Ringe e Christopher Ruof.

di sperimentazione, guidato e vigilato dagli Stati membri e dalle istituzioni europee, in cui le aziende interessate possano sperimentare l'utilizzazione dei sistemi di consulenza robotizzata con investitori reali e su operazioni concrete, ma in modo protetto, e cioè sotto il controllo attento delle istituzioni e, dunque, con rischi limitati per gli investitori. L'esperimento dovrebbe, inoltre, consentire ai regolatori di comprendere meglio il fenomeno e di intervenire per regolarne gli aspetti più critici e così tutelare al meglio i soggetti più deboli. Il che deve necessariamente passare anche attraverso un inquadramento delle diverse tipologie di servizi di *robo-advice* attualmente presenti sul mercato, in quanto ognuno di questi servizi evidenzia caratteristiche e problematiche sue proprie, che richiedono risposte specifiche ed eterogenee sul piano giuridico<sup>59</sup>.

L'esigenza di inquadrare correttamente le tipologie di servizi attualmente prestati nel mercato sotto locuzione *robot advice* ha determinato la dottrina a individuare le tre seguenti categorie: il *robo-advice* c.d. puro, nel quale il servizio è effettivamente automatizzato in tutte le sue fasi; il *robo-advice* c.d. ibrido, in cui è previsto l'intervento umano a completamento di alcune attività svolte dal sistema informatico; e, infine, il c.d. *robo-advisor*, che può essere utilizzato solo da consulenti professionali e non dagli investitori.

Come evidente, con riguardo al servizio c.d. *robo-advice* puro un primo problema è costituito dalla necessaria acquisizione delle informazioni personali dell'utente in applicazione della *know your customer rule*. L'attività in questione, se realizzata in automatico, presenta infatti considerevoli profili di rischio, poiché si basa necessariamente su questionari compilati *online* dal cliente. Come è stato correttamente osservato, in tal caso il rischio dell'acquisizione di informazioni insufficienti, non veritiere o dell'uso parziale o scorretto delle stesse sembra imporre una doppia verifica: non solo su quali informazioni vengono raccolte e come, ma anche su come queste

---

<sup>59</sup> L'esperimento, in buona sostanza, suggerisce un approccio prudente alla regolamentazione di fenomeni complessi e in evoluzione. Approccio che sembra essere, tutto sommato, quello scelto dalla Commissione europea, tanto che SARTORI, *op. cit.*, ha notato come «la Commissione Europea nel Piano d'azione per le tecnologie finanziarie (Bruxelles, 8 marzo 2018 COM(2018) 109 final, consultabile sul sito <https://ec.europa.eu/>) [sostiene che, n.d.a.] i rapidi progressi delle tecnologie finanziarie stanno determinando cambiamenti strutturali nel settore finanziario. In un ambiente in così rapida evoluzione una regolamentazione eccessivamente prescrittiva e precipitosa rischia di produrre effetti indesiderati». Per una (parzialmente) diversa prospettiva, cfr. T. BAKER, B. DELLAERT, *Regulating robo advice across the financial services industry*, in *University of Pennsylvania Law School*, consultabile on-line alla pagina Internet <https://scholarship.law.upenn.edu/>, 2018, 14.

sono “autonomamente” valutate ai fini dell’individuazione del prodotto adatto al cliente<sup>60</sup>.

La circostanza è resa ancora più rilevante dal fatto che, come noto, la MIFID II ha imposto di utilizzare un tipo di questionario che cerca di guardare al “*financial behaviour*” per catturare le reali attitudini e conoscenze finanziarie del cliente. Il che ovviamente non toglie che un algoritmo ben costruito ed un questionario ben predisposto possano funzionare. Il problema, dunque, è la costruzione dell’algoritmo<sup>61</sup>. Tema questo rispetto al quale necessita che le autorità di regolazione e vigilanza si dotino degli strumenti idonei per poter sindacare la conformità del sistema informatico rispetto ai principi MIFID<sup>62</sup>.

Tra gli ulteriori profili da considerare e tenere sotto controllo, vi è la c.d. *cyber security*, giacché strutture prive di un sistema di trattamento dei dati e di *disaster recovery* adeguato, potrebbero porre a serio rischio tanto i dati personali del cliente, quanto la funzionalità e la fruibilità del servizio. Ed inoltre, la *indipendenza*, in quanto spesso i servizi di *robo-advice* sono spesso funzionalmente collegati con altri servizi offerti dall’intermediario o da società collegate, il che *ab externo* può minare la sussistenza del requisito in parola. Senza dimenticare la *trasparenza*, visto che il sistema automatizzato, per rispettare la MIFID, deve comunicare al cliente la tipologia di servizio che offre (precisando, tra l’altro, se offre una consulenza di base, generica o generale) e le regole di condotta che è tenuto a rispettare, oltre a chiarire: *i*) se la consulenza è fornita su base indipendente; *ii*) se la consulenza è basata su un’analisi di mercato ampia, e in particolare se è limitata agli strumenti finanziari emessi o collocati da soggetti che hanno stretti legami con l’impresa di investimento o altro significativo rapporto legale o economico, come un rapporto contrattuale, tale da comportare il rischio di comprometterne l’indipendenza; e, infine, *iii*) se l’impresa di investimento fornirà ai clienti la valutazione periodica dell’adeguatezza degli strumenti finanziari raccomandati.

---

<sup>60</sup> Così LENER, *op. cit.*

<sup>61</sup> Cfr. M. TERTILT, P. SCHOLZ, *To Advise, or Not to Advise – How Robo-Advisor Evaluate the Risk Preferences of Private Investors*, in *The Journal of Wealth Management*, 2018, 21.

<sup>62</sup> Su questo argomento, e più in generale sul tema della consulenza finanziaria automatizzata, cfr. anche lo studio CONSOB, *La digitalizzazione della consulenza in materia di servizi finanziari*, edito dal gruppo di lavoro Consob/Scuola Superiore Sant’Anna di Pisa e altre università, pubblicato il 3 gennaio 2019 e disponibile on-line alla pagina Internet [http://www.consob.it/documents/46180/46181/FinTech\\_3.pdf/64bcf8bd-7fda-459d-9e01-82b1504dc316](http://www.consob.it/documents/46180/46181/FinTech_3.pdf/64bcf8bd-7fda-459d-9e01-82b1504dc316).



Massimo Proverbio

# Strategia dei dati e Digital Finance Package in Intesa Sanpaolo

SOMMARIO: 1. Strategia dei Dati e Piano industriale di Intesa Sanpaolo. – 2. DORA e Cloud. – 3. Dati e Intelligenza Artificiale. – 4. Pagamenti Istantanei. – 5. Mondo Digitale. – 6. Prossime sfide e conclusioni.

## 1. Strategia dei Dati e Piano Industriale di Intesa Sanpaolo

Intesa Sanpaolo ha intrapreso da tempo un percorso di digitalizzazione dei propri processi e dei servizi alla clientela, sfruttando al meglio le tecnologie più innovative, introdotte con un attento presidio dei diversi profili di rischio (inclusi, ovviamente, quelli tecnologici e della cyber security), facendo leva su un ecosistema di attori nazionali e internazionali, in piena coerenza con le indicazioni dei propri piani industriali. Grazie a tale approccio la banca è stata in grado di anticipare e soddisfare le esigenze dei clienti di operare sui canali digitali (App, Internet Banking, Filiale Digitale, ecc.), abilitando appieno la possibilità di servire il cliente da remoto e migliorare il servizio complessivo fornito, riuscendo anche a ottenere notevoli riduzioni di costo.

Tra i riconoscimenti ottenuti da Intesa Sanpaolo nel 2022 vale la pena menzionare a titolo meramente esemplificativo: “*Global Mobile Banking Apps Leader*”<sup>1</sup> da Forrester (prima assoluta tra tutte le app di banking va-

---

<sup>1</sup>Il rapporto pubblicato, The Forrester Digital Experience Review: Global Mobile Banking Apps, Q4 2022, oltre a riconoscere la digital leadership, ha evidenziato come Intesa Sanpaolo sia *best practice* nelle seguenti categorie: gestione quotidiana delle proprie finanze (*Money Management*), per il supporto in termini di analisi che i clienti hanno in App per comprendere come e dove spendono e come possono ottimizzare la gestione delle proprie spese; navigazione (*Navigation*), per la facilità della navigazione, chiarezza nell’architettura delle informazioni e degli elementi esposti in pagina, che consentono una navigazione semplice e inclusiva; privacy e

lutate nel mondo, con le migliori funzionalità e customer experience); “Qorus Accenture Banking Innovation Awards 2022”<sup>2</sup> (terza banca al mondo per capacità d’innovare). In tale contesto, per continuare ad essere percepita dal mercato come azienda *tech-like*, capace di adeguarsi rapidamente ai cambiamenti tecnologici e di business, anche derivanti da circostanze imprevedibili (pandemie, guerre, crisi energetiche, ecc.), la banca dovrà governare diversi fattori chiave, come una gestione dei dati sempre più sofisticata e sicura (in primis *compliant* con il GDPR) e l’aumento dei rischi di sicurezza, in un contesto di continuo aumento della pressione regolamentare, dei cambi tecnologici e della competizione proveniente anche da FinTech e da BigTech.

Uno dei pillar costitutivi del piano industriale 2022-25<sup>3</sup> consiste nella riduzione strutturale dei costi, grazie allo sviluppo della tecnologia, con una stima di circa 2 miliardi di euro di risparmio di costi, a fronte di 5 miliardi di investimenti in tecnologia e crescita.

Tra le strategie messe in atto, che si auspica possano portare a una riduzione dei costi, anche in modalità indiretta, vi è il rafforzamento delle competenze IT core. Il mondo digitale sta evolvendo rapidamente e la competenza IT è sempre più importante per le aziende, in modo da sfruttare al meglio le opportunità offerte dalle tecnologie emergenti. Per raggiungere questo obiettivo, il percorso intrapreso da Intesa Sanpaolo si muove sulle direttrici di seguito illustrate.

---

contenuti informativi (*Privacy cues and content*), per la chiarezza e la trasparenza con cui l’App gestisce i contenuti legati a Privacy e permessi richiesti ai Clienti.

<sup>2</sup> Il Qorus-Accenture Banking Innovation Award mette in luce i progetti, le iniziative e le idee più innovative nel settore bancario a livello globale. I candidati vengono selezionati direttamente da un gruppo di loro concorrenti e da un pool internazionale di esperti, fattore che garantisce la credibilità dei premi, considerati gli ‘Oscar’ del settore. Nel 2022 Intesa Sanpaolo è stata premiata, unica tra le banche italiane, con il prestigioso Qorus-Accenture Banking Innovation Award nella categoria “Global Innovator 2022”. Intesa Sanpaolo si è distinta tra le realtà maggiormente impegnate in un processo di continua innovazione e trasformazione, nello sviluppo di un ampio ecosistema di partner oltre il settore bancario e nell’impiego delle tecnologie emergenti per migliorare l’esperienza dei propri clienti.

<sup>3</sup> Il piano industriale 2022-25 connota Intesa Sanpaolo come una banca solida per un mondo sostenibile, leader per *wealth management, protection & advisory*, a “zero npl”, digitale e focalizzata sui ricavi da commissioni, con forte impegno ESG. Tra le principali iniziative in ambito digitale sono incluse: investimenti pari a 7,1 miliardi di euro nel 2022-2025, di cui 5 miliardi per tecnologia e crescita; completa digitalizzazione del processo creditizio; forti investimenti in soluzioni digitali e di AI nella Compliance; sviluppo di prodotti e servizi digitali (es. RoboAdvisor, canali self-service); offerta internazionale distintiva della Divisione IMI Corporate & Investment Banking che include piattaforme digitali all’avanguardia (con una piattaforma digitale da “sportello unico” per l’attività di Transaction Banking).

❖ Internalizzare o riconvertire il personale verso ruoli IT e attività ad alto valore aggiunto: le aziende hanno bisogno di persone con competenze specializzate in ambito IT, come ad esempio ingegneri cloud e ingegneri in Intelligenza Artificiale (AI) oppure verso attività ad alto valore aggiunto, come la realizzazione di soluzioni software. Considerare l'internalizzazione o la riconversione del proprio personale verso questi ruoli e attività può essere un modo efficace per aumentare la competenza IT all'interno dell'azienda. Questo aiuta a garantire che la macchina IT sia sempre al passo con le esigenze aziendali e le tendenze del mercato.

❖ Ridisegnare il modello operativo della fabbrica IT secondo le *best practice* delle società BigTech: un modello operativo efficiente è fondamentale per sfruttare al meglio le opportunità offerte dalle tecnologie emergenti. Questo può includere la standardizzazione delle soluzioni, l'automazione dei processi e la riduzione dei costi.

❖ Creare centri di competenza per soluzioni IT all'avanguardia: la creazione di centri di competenza per soluzioni IT all'avanguardia è un'altra soluzione per rafforzare le competenze IT core. Questi centri possono contribuire alla formazione del personale, nonché allo sviluppo e alla gestione di soluzioni IT innovative. Questo aiuta a garantire che l'azienda usi sempre al meglio le tecnologie più innovative e le conoscenze più avanzate.

Gli investimenti previsti nel Piano Industriale 2022-25 riguarderanno diversi ambiti, tra cui principalmente *Advanced Analytics* e AI; *Customer Experience*; sostenibilità sociale e *Responsible Banking*. Tra le iniziative in ambito digitale finalizzate alla riduzione strutturale dei costi vi è la creazione della nuova banca digitale “*Isybank*”<sup>4</sup>, in cui la migliore gestione dei costi è potenziata dall'uso di *Advanced Analytics* e da una maggiore efficienza IT.

---

<sup>4</sup>Intesa Sanpaolo ha scelto Thought Machine come partner tecnologico per far nascere Isybank, la sua nuova piattaforma di digital banking che rappresenta uno degli elementi chiave del Piano di Impresa 2022-2025 recentemente presentato. Isybank, inizialmente, si pone l'obiettivo di servire – con un'ampia gamma di servizi di digital banking – i 4 milioni di clienti Intesa Sanpaolo retail in Italia che non utilizzano la rete di filiali. Per lo sviluppo e la crescita di Isybank, sono previsti investimenti per €650 milioni nell'arco di piano. La piattaforma Thought Machine di ultima generazione è interamente nativa per il cloud e permette la creazione di qualsiasi prodotto necessario in un mondo in rapida evoluzione. Intesa Sanpaolo ha inoltre manifestato l'intenzione di estendere la piattaforma core banking di Thought Machine alla più ampia infrastruttura del Gruppo – grazie alla sostituzione della tecnologia core basata su mainframe con l'infrastruttura cloud – continuando a investire massicciamente nella trasformazione digitale della Banca: sono previsti investimenti in Information Technology e un impegno che coinvolgerà 4.000 persone tra nuove assunzioni di profili particolarmente specifici e riconversioni professionali.

Isybank si propone come una soluzione in grado di combinare la capacità di competere con le FinTech più innovative con la fiducia e la solidità offerte da un Gruppo come Intesa Sanpaolo. Tra gli obiettivi di Isybank vale la pena menzionare: (i) il rinnovamento del core banking del Gruppo in ottica Cloud e digitale; (ii) la promozione di un nuovo modello di business affidabile, sostenibile e scalabile (24x7 *branch-independent, no back-office, full self-service*); (iii) l'offerta alla clientela di un modello di servizio digitale completo (App, contact center, ATM, Mooney) e di percorsi interamente digitali – questi ultimi resi possibili grazie ad una strategia di vendita sviluppata da AI Sales e dalla costituzione di un AI Lab, composto da circa 50 professionisti italiani e stranieri, dedicati allo sviluppo di nuove metodologie di analisi dei dati basate sull'AI.

L'efficienza IT, come detto, costituisce un fattore chiave per il successo di qualsiasi azienda e ottimizzare i sistemi di back-end è un modo importante per ottenere questo obiettivo. In tale ottica uno dei fattori chiave è la modernizzazione dei sistemi legacy migrati in Cloud.

La modernizzazione in Cloud, infatti, consente di migliorare la scalabilità, la disponibilità e la sicurezza dei sistemi IT, offrendo allo stesso tempo una maggiore flessibilità e una gestione più efficiente delle risorse. Inoltre, la modernizzazione in Cloud può anche aiutare a ridurre i costi a lungo termine, poiché non è necessario mantenere hardware costoso e la gestione dell'infrastruttura diventa più agile.

## 2. DORA e Cloud

Il percorso di adozione del Cloud costituisce per Intesa Sanpaolo un pillar fondamentale per abilitare il processo di trasformazione digitale ed è alla base dell'evoluzione del modello operativo IT. Per definire l'accordo con il principale partner Cloud<sup>5</sup> di Intesa Sanpaolo è stato necessario negoziare molteplici elementi a tutela della nostra continuità operativa e a garanzia della conformità a tutte le normative applicabili. Ciò premesso, ri-

---

<sup>5</sup> Intesa Sanpaolo, TIM e Google a fine 2020 hanno siglato un accordo in base al quale la Banca migrerà una parte rilevante del proprio sistema informativo sui servizi Cloud di Google, che risponderanno ai più elevati standard internazionali di sicurezza e riservatezza delle informazioni e si appoggeranno sui Data Center italiani di TIM a Milano e a Torino. Il progetto prevede l'apertura a Torino di un'innovativa infrastruttura tecnologica per l'erogazione dei servizi Google Cloud e la creazione di un importante centro dedicato all'AI, alla formazione e al sostegno professionale delle start-up attraverso iniziative da definirsi insieme tra Intesa Sanpaolo, Google e TIM.

sulta evidente come Intesa Sanpaolo accolga con estremo favore l'adozione di disposizioni normative che prevedano degli obblighi specifici per i provider tecnologici, in quanto ciò renderebbe la negoziazione per l'adozione di tali tecnologie, e dei relativi livelli di servizio, più rapida e meno onerosa. L'entrata in vigore del Regolamento europeo sulla Resilienza Digitale<sup>6</sup> (DORA) porta una novità dal punto di vista della supervisione dei Cloud provider e delle Terze Parti ritenute critiche per il settore finanziario. Le autorità di vigilanza di settore – segnatamente l'Autorità bancaria europea (EBA), l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) – saranno infatti *overseer* di quei fornitori e provider reputati critici a livello di settore nell'Unione europea (UE) e potranno notificare loro eventuali scoperture dei requisiti di sicurezza. Il tema che resta tuttavia aperto è come in concreto si svilupperà tale supervisione, che sarà oggetto di specifici atti delegati nei diciotto mesi successivi all'entrata in vigore del provvedimento, e in particolare se l'onere della verifica della conformità a seguito dei rilievi dei supervisori spetterà alle singole entità finanziarie o meno.

DORA avrà un impatto importante sulle attività delle imprese che dovranno eseguire un'analisi sugli attuali processi per la gestione del rischio ICT che saranno influenzati dai nuovi requisiti e sviluppare piani d'implementazione. Le imprese dovranno disporre di:

❖ *ICT Risk Management* – capacità di affrontare situazioni critiche in maniera più esaustiva, compresa la necessità di stabilire una strategia *multi-vendor*. Per un'ottimizzazione della gestione, per evitare possibili sovrapposizioni/duplicazioni, sarà di fondamentale importanza l'allineamento con le legislazioni esistenti.

❖ *ICT-related Incident Management* – meccanismi e politiche per la gestione di tutti gli incidenti legati all'ICT e per la segnalazione degli incidenti più gravi. La banca sostiene questo primo tentativo della Commissione europea di armonizzare i requisiti di segnalazione degli incidenti ICT.

---

<sup>6</sup>Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario, dicembre 2022. Il regolamento sulla Digital Operation Resilience per il settore finanziario (DORA-Digital Operational Resilience Act) è molto rilevante in quanto, per la prima volta, si intende accorpate in un unico testo di norme, i requisiti in materia di *digital operation resilience* a livello UE, ad oggi considerati dalla normativa europea in modo indiretto e lasciati alla proliferazione di normative nazionali e approcci di supervisione frammentati, con conseguenti limiti di scalabilità per le aziende multi-country e potenziale creazione di un *uneven playing field*.

DORA, tuttavia, non comporta una completa armonizzazione rispetto agli altri obblighi di segnalazione dell'UE (ad esempio le previsioni della direttiva Network and Information Security 2 – NIS2 per gli incidenti legati al ruolo di Intesa Sanpaolo di fornitore di servizi fiduciari rimangono vincolanti<sup>7</sup>).

❖ *Digital Operational Resilience Testing* – misure per la conduzione dei test di resilienza non solo di sicurezza (ad esempio: non solo *vulnerability assessments and scans*, ma anche *physical security reviews, questionnaires and scanning software solutions, performance testing*) e introduzione di test avanzati e basati su intelligence, i *TLPT – Threat-Led Penetration Testing*.

❖ *ICT Third-Party Risks Management* – i fornitori Terzi ritenuti critici dovranno disporre di regole, procedure, meccanismi e accordi completi, solidi ed efficaci per gestire i rischi ICT a carico delle imprese di servizi finanziari (entro 18 mesi dall'entrata in vigore verranno emanate linee guida sui criteri da adottare per la valutazione). DORA stabilisce nuovi requisiti contrattuali con l'obiettivo di sancire le garanzie minime (alcune sotto forma di raccomandazioni) per consentire alle imprese finanziarie di monitorare meglio i possibili rischi ICT da Terze Parti (la Commissione europea sta lavorando all'elaborazione di clausole contrattuali standard). Le autorità competenti concederanno agli enti finanziari il periodo di tempo necessario per adeguare gli accordi contrattuali con i fornitori Terzi al fine di evitare effetti negativi sulla loro resilienza operativa digitale e per consentire loro di mettere in atto le strategie di uscita più adeguate e i piani di transizione. Le imprese finanziarie non potranno avvalersi di servizi da un fornitore di servizi ICT critico di un Paese Terzo che non stabilisca una filiale nell'UE entro 12 mesi dalla sua designazione come fornitore critico.

❖ *Information Sharing* – con l'obiettivo di incoraggiare lo scambio delle informazioni sulle minacce in ambito finanziario. La banca sostiene l'introduzione di un HUB europeo per la condivisione delle informazioni e per rafforzare la cooperazione tra gli Stati membri anche per la gestione delle crisi; nella norma è richiesto alle autorità di supervisione europee in ambito finanziario di svolgere uno studio di fattibilità entro gennaio 2025.

Alcuni requisiti saranno molto gravosi per un'entità finanziaria e potrebbero aumentare significativamente i costi di conformità, pensiamo ad esempio all'obbligo di adottare una strategia *multi-vendor*, all'obbligo di rescindere il contratto con il *Third Party Provider* (TPP) critico quando ri-

---

<sup>7</sup> Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, dicembre 2022.

chiesto dall'Autorità competente, effettuare su base periodica una valutazione specifica del rischio ICT su tutti i sistemi ICT legacy, oppure all'obbligo di testare tutti i sistemi e le applicazioni critiche.

In aggiunta vale la pena menzionare che il tema del ruolo delle Terze Parti nella garanzia della gestione del rischio cyber sia stato affrontato anche nel documento “*G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*”<sup>8</sup>, pubblicato a ottobre 2022 e alla cui stesura la banca ha partecipato in rappresentanza del settore privato bancario italiano. Questi nuovi principi incoraggiano le terze parti ad essere attive nella gestione dei rischi cyber, in particolare nell'*Element 7* vi è un tentativo di indirizzare anche il tema delle quarte o quinte Parti, che si conclude sostenendo che “*Where applicable, third parties are encouraged to use these Fundamental Elements to address third party risk emanating from their respective third parties in the ICT supply chain*”.

### 3. Dati e Intelligenza Artificiale

Per estrarre il massimo valore dalla relazione con i clienti, offrendo servizi e prodotti che siano in linea con le esigenze e anticipando i loro bisogni, è fondamentale disporre di una strategia sui dati che ne abiliti l'utilizzo in coerenza con i principi a tutela dei diritti fondamentali e delle libertà degli individui.

Come è noto la proposta di Regolamento presentata dalla Commissione europea nell'aprile 2021 – il c.d. Artificial Intelligence Act (AIA)<sup>9</sup> – mira a

---

<sup>8</sup>G7 Fundamental elements for Third Party cyber risk management in the financial sector, October 2022.

<sup>9</sup>Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, aprile 2021. La Commissione europea ha presentato il 21 aprile 2021 una proposta di regolamento che delinea un quadro normativo armonizzato sui sistemi di intelligenza artificiale (c.d. Artificial Intelligence Act – AIA). Oltre alle condotte categoricamente proibite, come ad esempio il social scoring o il riconoscimento facciale eseguito da autorità pubbliche in tempo reale, l'AIA individua alcuni sistemi considerati “ad alto rischio” per la salute, la sicurezza e i diritti fondamentali delle persone. Tra i sistemi ad alto rischio di particolare interesse per la banca segnaliamo quelli di merito creditizio (o creditworthiness) e di punteggio creditizio (o credit scoring) per le persone fisiche, così come quelli legati alla selezione del personale o al lavoro del dipendente. Tra i requisiti da rispettare i più onerosi riguardano i dati utilizzati dal sistema di AI, che devono essere di alta qualità e accuratamente controllati per evitare il rischio di creare o amplificare discriminazioni, anche involontarie. Un altro aspetto fondamentale è quello del controllo umano, per cui si richiede che l'applicazione sia sempre supervisionata da un essere umano, e quindi che l'algoritmo non operi mai in completa autonomia nel prendere decisioni riguardanti gli individui.

creare un ecosistema in UE in cui i sistemi di AI utilizzati siano sicuri, trasparenti, etici, imparziali e sottoposti al controllo umano. Intesa Sanpaolo è favorevole ai principali orientamenti della proposta come l'adozione di un approccio basato sul rischio, già insito nel modello operativo della banca: maggiore è il rischio che il sistema introduce, più restrittiva è la regolamentazione che deve essere rispettata. Per raffigurare questo aspetto le istituzioni europee hanno utilizzato l'immagine della piramide: in cima troviamo i sistemi di AI vietati che non possono essere adottati, perché costituiscono delle condotte categoricamente proibite (come il *social scoring* ampiamente diffuso in Cina); nella parte centrale della piramide troviamo invece i sistemi "ad alto rischio" (e.g. *credit scoring*; gestione e selezione del personale) per i quali dovranno essere rispettati requisiti anche rigorosi e onerosi; e, infine, sono previsti i sistemi che presentano un rischio limitato e un rischio minimo. Un approccio effettivamente *risk-based*, garantendo ampie tutele alle libertà e ai diritti fondamentali degli individui in proporzione al rischio effettivamente introdotto, consentirebbe all'Unione europea di contraddistinguersi come promotrice dell'eccellenza e dell'affidabilità nell'uso dell'AI.

Entrando nel merito della proposta, sono presenti tuttavia alcuni aspetti critici. Tra i più rilevanti per i servizi bancari vi è l'interrelazione tra i requisiti previsti dalla proposta AIA e quelli della Capital Requirements Regulation (CRR<sup>10</sup>), che già si applicano ai modelli di rischio di credito della banca, validati *ex-ante* in ambito "European Central Bank Single Supervisory Mechanism".

Altro aspetto ampiamente dibattuto è quello della supervisione. A dicembre 2021 la Banca Centrale Europea (BCE) ha pubblicato una lettera in cui ha indicato che il testo dell'AIA dovrebbe chiarire in modo inequivocabile che la BCE non è designata come autorità di vigilanza del mercato, né può essere incaricata di tali compiti – come invece era previsto nella proposta dalla Commissione. Come Intesa Sanpaolo supportiamo invece la designazione delle autorità nazionali di vigilanza finanziaria come uniche responsabili della supervisione, così come previsto dal *general approach* del Consiglio<sup>11</sup>.

Da un punto di vista più tecnico invece, se la banca decidesse di adottare un sistema di intelligenza artificiale ad alto rischio, i requisiti da rispettare sarebbero molti. Tra questi i più onerosi riguardano i dati utilizzati dal

<sup>10</sup> Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio relativo ai requisiti prudenziali per gli enti creditizi, giugno 2013.

<sup>11</sup> Council of the EU General Approach.

sistema di intelligenza artificiale, che devono essere di alta qualità e accuratamente controllati per evitare il rischio di creare o amplificare discriminazioni, anche involontarie. Alcuni di questi requisiti risultano però a nostro avviso ancora da approfondire, come ad esempio la richiesta di identificare ogni tipo di “*datagaps or shortcamings*”. A tal proposito auspichiamo che nel corso dell’*iter* legislativo tali requisiti siano maggiormente dettagliati, al fine di delineare *best practice* volte ad aumentare quanto più possibile la qualità dei dati.

Un altro aspetto fondamentale, inoltre, è quello del controllo umano, per cui si richiede che l’applicazione di AI sia sempre supervisionata da un essere umano e quindi che l’algoritmo non operi mai in completa autonomia nell’assumere decisioni riguardanti gli individui. Come Intesa Sanpaolo riteniamo di fondamentale importanza che i processi decisionali automatizzati siano supervisionati da un essere umano, attraverso controlli e strumenti di diversa natura. È, tuttavia, parimenti importante che il legislatore chiarisca maggiormente sia che cosa si intenda per controllo umano, sia quali possano essere le soluzioni – anche tecnologiche – in grado di adempiere tale funzione, che consentano l’intervento di un operatore umano senza pregiudicare significativamente le prestazioni dell’algoritmo di AI.

Non è, inoltre, da sottovalutare il fatto che la proposta incoraggi fortemente l’adozione di codici di condotta volontari anche per i sistemi che presentano un rischio basso o nullo, promuovendo, quindi, il rispetto di requisiti molto onerosi per qualsiasi tipo di sistema di intelligenza artificiale. Come Intesa Sanpaolo siamo promotori di un uso pienamente etico dell’AI e abbiamo iniziato a integrare tali aspetti nella nostra attività bancaria ben prima della pubblicazione del AIA. Riteniamo, tuttavia, che l’adozione dei codici di condotta non dovrebbe comunque comportare un onere eccessivo, in quanto ciò potrebbe scoraggiare l’implementazione di sistemi di AI per sistemi a basso o nessun rischio o in aree in cui non vi sia quasi nessuna minaccia per i diritti fondamentali.

Un ulteriore tema rilevante per le banche riguarda senza dubbio l’uso dell’AI per la concessione del credito. Diversi attori internazionali, come BigTech o FinTech, già da tempo stanno realizzando soluzioni altamente competitive, sfruttando le maggiori libertà di sperimentazione di cui godono, non essendo sottoposte alla stessa regolamentazione degli istituti creditizi. Applicando sempre un approccio *risk-based* è fondamentale che i player di qualsiasi categoria (anche in ottica *level playing field*) possano portare a termine sperimentazioni con un adeguato grado di libertà, pro-

prio al fine di valutare con precisione benefici, opportunità e rischi che verrebbero introdotti con l'uso delle tecnologie in parola.

Nel corso del 2022 è stato costituito a Torino un consorzio per il contrasto dei crimini finanziari digitali attraverso l'impiego delle nuove tecnologie e dell'intelligenza artificiale, che intende diventare un punto di riferimento a livello nazionale e internazionale nella lotta al riciclaggio e al terrorismo; si tratta del c.d. Anti Financial Crime Digital Hub (AFC Digital Hub)<sup>12</sup>.

L'impiego di modelli matematici e dell'AI consentirà all'AFC Digital Hub di sviluppare soluzioni innovative per individuare fenomeni sospetti riconducibili ad attività illecite. L'analisi verterà principalmente su fenomeni legati al riciclaggio e al contrasto del terrorismo e in futuro potrebbe estendersi anche alle situazioni di abuso di mercato e di frodi.

AFC Digital Hub ha come soci Intesa Sanpaolo Innovation Center, l'Università di Torino, il Politecnico di Torino e CENTAI<sup>13</sup>, il nuovo centro di ricerca per l'AI e i sistemi complessi partecipato dalla banca, aperto ad altri istituti di credito e intermediari del sistema.

Da sempre attenta a monitorare i trend di sviluppo per progettare, strutturare e fornire alle proprie risorse e alla clientela servizi sempre più efficaci ed efficienti, Intesa Sanpaolo ha scelto di costituire CENTAI a giugno 2022. CENTAI, avvalendosi di prestigiosi ricercatori e scienziati riconosciuti a livello globale, opererà sia a favore di Intesa Sanpaolo, dove si concentrerà in particolare sulle strategie di sviluppo di Isybank, sia per aziende e società esterne. CENTAI si propone come motore di innovazione nella ricerca sull'intelligenza delle macchine e dei sistemi complessi: una realtà nuova, dotata degli strumenti più avanzati di AI e big data, capace di esplorare le proprietà strutturali di tutti quegli aspetti della società che fanno da collante alle tante variabili di questo pianeta.

All'interno delle strutture di Direzione Centrale della Banca, infine, opera la funzione "Data Science & AI", che costituisce il Centro di Competenza del Gruppo sull'AI: si occupa dello sviluppo e implementazione di soluzioni di Intelligenza Artificiale a supporto di tutte le aree del Gruppo, rappresentando un centro di eccellenza in ambito di ricerca scientifica e applicata sui temi di etica, non-discriminazione e trasparenza degli algoritmi di AI.

---

<sup>12</sup> Intesa Sanpaolo annuncia la costituzione del consorzio Anti Financial Crime Digital Hub.

<sup>13</sup> Intesa Sanpaolo annuncia la costituzione di CENTAI, con sede a Torino, che nasce come Società per Azioni partecipata al 49% da Intesa Sanpaolo e controllata per il 51% dalla compagine scientifica, guidata da un Comitato Scientifico di riferimento di alto profilo internazionale.

## 4. Pagamenti Istantanei

La Commissione europea ha pubblicato una proposta di Regolamento<sup>14</sup> che renderà obbligatorio per gli intermediari finanziari abilitati l'offerta del servizio dei bonifici istantanei (Instant Payment – IP). La proposta, se approvata dal Parlamento e dal Consiglio UE, obbligherà le banche ad effettuare trasferimenti di denaro in euro immediati, a un prezzo non superiore a quello praticato per un bonifico ordinario (SEPA Credit Transfer – SCT).

Recentemente la BCE ha pubblicato la sua Opinione che accoglie con favore la proposta della Commissione<sup>15</sup>.

Le previsioni della proposta maggiormente rilevanti per Intesa Sanpaolo sono riportate di seguito.

❖ i *Payment Service Providers* (PSP) che forniscono il servizio di pagamento SCT dovranno fornire anche l'IP 24 ore su 24, 365 giorni all'anno, senza alcuna possibilità di fissare orari limite o limitare il trattamento solo ai giorni lavorativi;

---

<sup>14</sup> Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) n. 260/2012 e (UE) 2021/1230 per quanto riguarda i bonifici istantanei in euro, ottobre 2022. Aumentare le soluzioni digitali e di instant payment di portata pan-europea è uno dei 4 pilastri della Strategia per l'UE sui pagamenti al dettaglio, che ha l'obiettivo di sviluppare, per i prossimi anni, una visione chiara e un quadro politico unico, coerente e onni-comprendivo per i pagamenti al dettaglio a livello UE. Gli altri pilastri sono: i mercati dei pagamenti al dettaglio innovativi e competitivi; sistemi di pagamenti al dettaglio efficienti ed interoperabili e altre infrastrutture di sostegno ed infine i Pagamenti internazionali efficienti, incluse le rimesse.

<sup>15</sup> I punti principali del Parere BCE sono quelli di seguito riportati.

✓ Definizioni: si raccomanda di allineare alcune definizioni a quelle già previste dalla normativa vigente

✓ Costi per gli IP: si supporta il requisito che gli IP siano offerti alla clientela allo stesso prezzo dei bonifici ordinari.

✓ Discrepanze tra nome e identificativo del conto di pagamento del beneficiario: si ritiene che una "commissione aggiuntiva" potrebbe essere un deterrente per l'adozione degli IP e che dovrebbe essere evitata in quanto il servizio di verifica è cruciale.

✓ Screening per sanzioni UE: si ritiene che la proposta della Commissione non assolve i PSP dall'essere conformi con le sanzioni nazionali rilevanti applicate nei confronti di una persona o entità rilevanti; si suggerisce di introdurre un emendamento per cui l'obbligo di condurre le verifiche rispetto alle misure restrittive avvenga immediatamente dopo la loro pubblicazione in Gazzetta Ufficiale dell'UE; si propone inoltre che venga riconosciuto il ruolo positivo che può avere il LEI (legal entity identifier) non solo in tale processo, ma anche in quello relativo al controllo delle discrepanze.

✓ Procedura d'infrazione: si propone di esentare i PSP dalle procedure d'infrazione nel caso eccezionale in cui lo schema SCT Inst non sia disponibile per un breve periodo di tempo.

❖ i PSP che forniscono il servizio di pagamento SCT dovranno fornire l'IP tramite gli stessi canali disponibili per il primo (ad esempio filiale, internet, app, ATM);

❖ i PSP dovranno fornire al cliente la verifica della corrispondenza tra IBAN e l'intestatario del medesimo indicato dal cliente e quello effettivo prima dell'invio dell'IP e notificare ogni discrepanza. Il cliente dovrà avere la facoltà di confermare o meno l'IP dopo questa verifica;

❖ i PSP dovranno rendere accessibili i pagamenti istantanei in euro, con l'obbligo di garantire che il prezzo applicato per i pagamenti istantanei non superi il prezzo praticato per i bonifici tradizionali non istantanei in euro;

❖ i PSP dovranno verificare almeno quotidianamente i propri clienti rispetto alle liste su sanzioni finanziarie (sulla base della lista consolidata gestita dalla Commissione europea delle persone/gruppi/entità che sono soggetti a sanzioni finanziarie), senza ulteriori controlli al momento dell'esecuzione dell'IP. Sarà in capo al PSP che non svolge correttamente il controllo sul proprio cliente la responsabilità in caso di esecuzione di un IP da/verso ordinante/beneficiario soggetto a sanzioni.

Intesa Sanpaolo, pur supportando pienamente lo sviluppo degli IP, anche in ragione della loro funzione di abilitatore di nuovi servizi innovativi in ambito pagamenti digitali, esprime diverse perplessità su alcune misure dell'attuale proposta in quanto, a nostro avviso, risultano sproporzionate rispetto agli obiettivi che la proposta stessa intende raggiungere e ai benefici indotti. La proposta così come è stata redatta comporterebbe un significativo aumento dei rischi di frode e operativi, con un conseguente prevedibile rilevante incremento delle perdite sia per i clienti, sia per gli intermediari, nonché rilevanti e non giustificati investimenti in capo a questi ultimi. In altre parole, riteniamo che l'attuale proposta sia sproporzionata in termini di oneri richiesti ai PSP e, anche se attuata così com'è, non sarà in grado di raggiungere pienamente gli obiettivi sia di incremento nell'utilizzo dello strumento, sia per lo sviluppo di una soluzione paneuropea basata sugli IP. Gli IP non possono nemmeno essere reputati un'alternativa equipollente ai trasferimenti denominati in cryptovaluta<sup>16</sup>, vista la natura for-

---

<sup>16</sup>Le c.d. valute virtuali (o valute digitali o cripto-attività o criptovalute) sono rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, negoziate o archiviate elettronicamente. Quindi sono un oggetto completamente digitale (nascono, vivono e sono custodite elettronicamente), che non ha un controvalore nell'economia reale, a meno che queste valute non siano accettate come mezzo di scambio. Si stima che siano circa 50 milioni le persone che detengono questo bene, e il loro impatto nel sistema economico è dunque ancora limitato. (L'economia per tutti – Banca d'Italia).

temente diversa, sia nei tempi di esecuzione (a differenza di quanto si credeva, generalmente i pagamenti in crypto sono molto più lenti degli IP), sia perché i trasferimenti in cryptovaluta determinano un rischio di cambio nei confronti delle valute di corso legale da cui gli IP sono esenti *by-design*, essendo denominati in euro.

L'estensione su tutti i canali comporta problematiche operative rilevanti, in quanto non tiene in considerazione le diverse peculiarità dei canali (es. interfaccia utente, tipologia di connessione, ecc.) oltre che investimenti e sforzi enormi per gestire il 24/7/365 e in meno di 10 secondi gli IP, soprattutto per quei canali già ora poco utilizzati per i bonifici ordinari, come gli sportelli automatici. Occorre inoltre sottolineare che l'estensione descritta determinerebbe un aumento sproporzionato delle frodi; gli IP sono molto attraenti per i truffatori, in quanto sono immediati e, soprattutto, irrevocabili, mentre nella maggior parte dei casi i bonifici tradizionali vengono rimborsati grazie al richiamo dei fondi e agli accordi di interoperabilità tra PSP. In tal senso, il rafforzamento dei presidi a tutela della clientela posti in essere dalla banca a partire da fine 2020 che, fra l'altro, subordinano l'utilizzo dell'IP da parte del cliente ad uno specifico iter di valutazione del rischio di tale operatività, hanno consentito la riduzione delle frodi da € 17,9 mln del 2020 ai € 0,3 mln stimati per il 2022; si consideri inoltre che l'IP comporta di per sé l'impossibilità di utilizzo della "recall"<sup>17</sup>, attualmente uno dei mezzi principali di recupero dei fondi; al riguardo si evidenzia che grazie alla "recall" nel primo semestre 2022 la banca ha recuperato circa € 3,5 mln su un totale di € 5 mln di fondi distratti alla clientela.

Con una maggiore diffusione degli IP si potrebbe assistere a nuove frodi, ad esempio, presso gli sportelli automatici, dove potrebbero emergere nuovi scenari di sicurezza che sarebbero ovviamente gestibili, ma con costi e rischi legati ai nuovi canali molto più elevati rispetto ai benefici indotti. Ad esempio, in caso di furto della carta e di accesso al PIN tramite phishing, i truffatori potrebbero trasferire immediatamente e irrevocabilmente i fondi sui loro conti. Oppure i consumatori, minacciati fisicamente, potrebbe-

---

<sup>17</sup> Nel contesto dei sistemi di pagamento, il recall si riferisce alla cancellazione di una transazione di pagamento precedentemente avviata. Ciò può accadere, ad esempio, quando un cliente si rende conto che un pagamento è stato effettuato per errore o quando il pagamento non è stato elaborato correttamente. La funzione di recall è solitamente disponibile per l'originatore del pagamento, che può richiedere la cancellazione del pagamento tramite la propria banca. Tuttavia, il processo di recall può essere soggetto a regole e limiti di tempo specifici e non sempre può essere possibile, a seconda della fase di elaborazione del pagamento.

ro essere obbligati dai criminali a trasferire denaro allo sportello automatico a favore di conti intestati ai truffatori.

L'estensione degli IP è strettamente correlata con la responsabilità delle frodi e con la necessità da un lato di tutelare, ma dall'altro di rendere consapevole la clientela che spesso non ha un'adeguata conoscenza del digitale. Il cliente dovrebbe essere libero di scegliere se affidarsi o meno a questo servizio e messo al corrente, prima di autorizzare il pagamento, delle informazioni richieste (l'importo del pagamento e il beneficiario) per ogni singolo trasferimento. Queste informazioni sono ancora più importanti nel caso di un IP, che è immediatamente esecutivo e irrevocabile.

A mitigazione di tali rischi, la proposta dovrebbe essere modificata prevedendo che l'estensione dell'IP sia facoltativa con riferimento sia alla clientela finale, sia ai canali di offerta. In particolare, l'attivazione dell'IP dovrebbe avvenire su richiesta del cliente ed essere subordinata ad una valutazione di rischio dei profili di cybersecurity che i PSP devono poter svolgere, anche considerata la responsabilità che la direttiva sui Sistemi di Pagamento (PSD2<sup>18</sup>) pone in capo agli stessi in caso di frode. Il testo dovrebbe invece mantenere l'obbligo di raggiungibilità per gli intermediari abilitati, al fine di garantire sempre l'esecuzione degli IP laddove ricorrano le condizioni previste. In caso contrario, i costi sostenuti dai PSP sarebbero sproporzionati rispetto ai benefici per i clienti. In subordine, se l'obbligo di estensione a tutta la clientela fosse confermato, occorrerebbe prevedere la facoltà del cliente di disattivare l'IP anche in considerazione delle sue effettive esigenze finanziarie. Dovrebbe, quindi, essere possibile per il PSP disattivare o sospendere temporaneamente il servizio di IP in maniera selettiva o totale, a fronte di motivate ragioni di sicurezza e per la maggior tutela della clientela. In aggiunta, sarebbe auspicabile che l'attivazione dell'IP fosse resa facoltativa per i PSP sui canali non digitali, quali gli ATM e relativamente ai bonifici multipli. Ciò anche considerato che l'estensione degli IP a tutti i canali richiede investimenti importanti, sia IT sia antifrode, entro le tempistiche stringenti previste dalla normativa. In tal senso, l'equiparazione commissionale tra bonifici SCT ed IP risulta assolutamente ingiustificata e in contrasto con i principi del libero mercato. Questo obbligo non tiene conto del fatto che questi due servizi sono sostanzialmente diversi, con caratteristiche distinte e che il loro utilizzo è concepito per casi d'uso specifici. L'offerta di un bonifico istantaneo richiede enormi investimenti tecnologici, infrastrutturali e di sicurezza.

---

<sup>18</sup> Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno, novembre 2015.

Sempre in tema di responsabilità in caso di frodi riteniamo che l'impegno richiesto per sviluppare il servizio di *name-check* sia sproporzionato rispetto alla sua efficacia e utilità ai fini del contrasto alle frodi. Questo servizio avrebbe effetti limitati ad alcune tipologie di frodi, come *Scam* e *Whaling* (Business email compromesse), lasciando scoperti altri scenari come *Phishing*, *Malware* e *Swap* IBAN. Tali fattispecie, nel corso del primo semestre 2022 sono stati alla base di tentativi di frode ai danni della clientela per € 2,5 mln, intercettati dai sistemi antifrode in uso presso la banca nel 94% dei casi. In ogni caso, tale verifica dovrebbe essere effettuata secondo precisi requisiti funzionali, al fine di delimitare chiaramente la responsabilità del PSP, in particolare al momento della restituzione al cliente dell'esito del controllo di *name-check* e di successiva esecuzione inesatta o fraudolenta dell'IP.

Nei casi di incertezza, ad esempio, i clienti potrebbero sentirsi confusi e non sapere come agire. In secondo luogo, dovrebbe essere stabilita una chiara ripartizione delle responsabilità, come previsto dalla PSD2, tra il PSP del pagatore, il PSP del beneficiario e il cliente in caso di pagamenti negati. Forse varrebbe la pena concentrarsi su altre misure più strutturali per la lotta alle frodi. Un esempio di area da affrontare è il chiarimento dei poteri della banca/PSP quando identifica un truffatore tra i propri clienti, per accelerare i processi relativi al blocco e al recupero del denaro trasferito in modo fraudolento. Questo argomento ha un'importanza maggiore in relazione agli IP, considerando le maggiori difficoltà (spesso impossibilità) nel richiamare le transazioni fraudolente. Inoltre, un'altra area da considerare è quella degli ostacoli sostanziali alla condivisione delle informazioni sulle minacce informatiche, soprattutto quando queste coinvolgono informazioni di identificazione personale, a causa delle diverse interpretazioni dei requisiti comunitari e nazionali. È quindi importante definire i casi di eccezione in cui la condivisione delle informazioni può portare a elevati benefici, ad esempio nella gestione antifrode, nel rispetto delle norme sulla concorrenza, dove le difficoltà legate alla presenza di dati associati a persone fisiche possono essere contrastate. Un primo passo in questa direzione è l'inclusione di una disposizione specifica per la condivisione di informazioni tra entità finanziarie nell'ambito del regolamento DORA. Per combattere le frodi riteniamo necessario anche un maggiore coinvolgimento del settore pubblico, ad esempio mettendo a disposizione strumenti sia per i clienti sia per il settore privato, per agire tempestivamente contro i cybercriminali che cercano di ottenere credenziali o di impersonare la banca/PSP (ad esempio chiudendo o bloccando siti web falsi, imponendo requisiti di verifica più severi per le richieste di apertura di siti web agli Ho-

*sting Provider*, dando la possibilità di recuperare i dati inviati dai clienti su siti fraudolenti, ecc.).

Per quanto attiene, infine, ai profili connessi al *sanction screening*, pur accogliendo con favore questa disposizione che introduce misure armonizzate a livello europeo sullo *screening* delle sanzioni si evidenzia che l'implementazione dello screening giornaliero della propria clientela richiede idonee tempistiche di adeguamento dei sistemi e processi interni; la norma dovrebbe quindi prevedere un *grace period* di almeno 12 mesi prima della sua entrata in vigore. Inoltre, considerando che la proposta non prevede lo screening della transazione, l'art. 5 *quinquies* (1) dovrebbe specificare che l'obbligo di verificare se i propri clienti siano persone o entità designate soggette a sanzioni dell'UE spetta al PSP dell'ordinante, in quanto esegue il bonifico istantaneo, e non al PSP del beneficiario, in quanto quest'ultimo sarà soggetto alle norme sanzionatorie dell'UE esistenti. Di conseguenza, se il PSP dell'ordinante non effettua tali verifiche, sarà ritenuto responsabile ai sensi degli artt. 5d(3) nei confronti del PSP del beneficiario e 5 *quinquies* (3) nei confronti del PSP del beneficiario.

## 5. Mondo Digitale

Considerando che spesso la regolamentazione non ha tempi adeguati allo sviluppo digitale per frenare truffe e *cyberattack*, riteniamo fondamentale rafforzare la protezione degli individui in un'economia sempre più digitale con una risposta operativa più efficace a livello europeo nei confronti del fenomeno delle frodi online.

### ❖ Responsabilità in ambito frodi

Recentemente sono entrate in vigore norme per rafforzare i processi di sostituzione delle SIM da parte degli operatori. Tali interventi sono utili per mitigare i fenomeni di frode basati sulla sostituzione fraudolenta della SIM (*SIM SWAP*).

Diversi fenomeni frodati originano tuttavia da attacchi di inganno sociale (*social engineering*), finalizzati a carpire le credenziali di accesso o i codici dispositivi della clientela.

Tali attacchi vengono realizzati tipicamente tramite i classici attacchi di phishing, con mail dirette alla clientela, ma anche e sempre più spesso tramite chiamate telefoniche o invio di SMS alla clientela.

Al fine di rendere credibili tali attacchi le chiamate vengono effettuate con tecniche di "spoofing telefonico", ovvero tramite chiamate provenienti

da numeri di telefono apparentemente attribuibili alla banca (numeri verdi, numeri intestati alla banca). Nel caso di messaggi via SMS vengono invece utilizzare tecniche basate su utilizzo di “ALIAS SMS fasulli”, ovvero tramite SMS con mittente un numero o un identificativo (ALIAS) riferibili alla banca (es. Gruppo ISP).

Le tecniche di spoofing telefonico e l'utilizzo di ALIAS SMS fasulli sono rese possibili dai meccanismi di funzionamento delle reti telefoniche. Al fine di contrastare tali fenomeni è necessario che siano adottati, a livello normativo, regolamenti atti a: (i) bloccare le chiamate che originano da numeri non reali/alterati (spoofing telefonico); (ii) permettere l'inoltro sulla rete telefonica di SMS tramite identificativi ALIAS o numerazioni solamente a seguito di una verifica della corretta associazione dell' ALIAS o della numerazione al reale mittente (sviluppo registro ALIAS SMS); tali interventi sono stati discussi in sede AGCOM, ma non vedono al momento certezza sulle modalità e i tempi di realizzazione.

#### ❖ **Responsabilità delle banche nel caso di truffe**

L'evoluzione dei sistemi antifrode e gli investimenti effettuati dalla banca hanno portato i frodatori a sviluppare attacchi sempre più basati su tecniche di inganno nei confronti della clientela finale. Tramite tali tecniche la clientela viene convinta ad effettuare o ad approvare transazioni fraudolente.

L'attuale normativa nazionale non prevede specifiche responsabilità in capo agli istituti nel caso di operazioni fraudolente quando le stesse siano state correttamente disposte e autorizzate dai clienti oggetto di truffa.

È opportuno che le evoluzioni normative non introducano modifiche a tale orientamento e che non portino agli operatori finanziari una maggiore responsabilità per eventi che derivano da chiara responsabilità in capo al cliente.

## **6. Prossime sfide e conclusioni preliminari**

Nel contesto appena delineato, Intesa Sanpaolo accoglie favorevolmente una regolamentazione delle nuove tecnologie che sia appropriata e bilanciata, volta a definire un quadro legale sicuro entro cui operare, condizione necessaria affinché un attore di mercato come Intesa Sanpaolo possa offrire i propri servizi.

Allo stesso tempo è tuttavia parimenti importante garantire che le discipline introdotte:

i. siano omogenee all'interno dell'UE e applicabili a tutti gli attori che offrono servizi analoghi, in ottemperanza al principio di parità di condizioni che recita "*same activity, same risk, same regulation*";

ii. siano controbilanciate da un principio di proporzionalità, per cui gli oneri siano adeguati ai rischi correlati all'introduzione della specifica tecnologia e ciò sia valido anche per le sperimentazioni; e

iii. tengano in debita considerazione la concorrenza a livello globale, notoriamente spietata in ambito digitale, anche per previsioni regolamentari sostanzialmente diverse in capo ai diversi attori nelle varie giurisdizioni, in qualche caso a scapito della sicurezza e dei diritti dei consumatori.

Cesare Galli

## **Il futuro delle piattaforme tra *blockchain*, NFT, metaversi e gestione dei dati**

SOMMARIO: 1. La necessità di un approccio sistematico nella disciplina delle nuove tecnologie. – 2. Il rapporto tra metaversi e *blockchain* e le esigenze di corretta contrattualizzazione dei relativi rapporti giuridici. – 3. Token e Non Fungible Token e il loro rapporto con *blockchain* e metaverso. – 4. Metaversi e diritto dei marchi. – 5. Metaversi, nuove tecnologie e gestione dei dati.

### **1. La necessità di un approccio sistematico nella disciplina delle nuove tecnologie**

Il metaverso non è solo un argomento ricorrente nelle cronache giornalistiche di questi ultimi mesi, ma molto di più, perché si trova al crocevia dei vari aspetti di uno dei nodi cruciali per il futuro della nostra economia e delle nostre società, ossia quello della raccolta, gestione e utilizzazione dei dati – e in particolare di quelli raccolti attraverso la rete web – per la fornitura di nuovi servizi, resi possibili dall'uso congiunto di una serie di innovazioni tecniche. Dunque è più che mai necessario che queste nuove tecnologie della rete e le loro applicazioni siano al centro non solo della cronaca, ma anche della discussione giuridica e in particolare di quella che riguarda i diritti della proprietà intellettuale, che in questo campo assumono un ruolo decisivo per governare e indirizzare il cambiamento in atto, dato che non riguardano solo queste tecnologie, ma anche i contenuti digitali realizzati attraverso di essi e le diverse funzioni di mercato che vi sono implicate.

Anche sul piano giuridico il dibattito che si è aperto sul metaverso è tuttavia spesso viziato da una duplice incomprendenza: da un lato si reclamano nuove norme calibrate su singole fattispecie e quindi destinate ad essere rese rapidamente obsolete dall'evoluzione tecnologica e sociale; dall'altro lato si concentra l'attenzione sulle applicazioni più clamorose di queste nuove tec-

nologie, senza coglierne (e valutarne sul piano giuridico) tutte le potenzialità. In entrambi i casi manca una visione del futuro, oggi invece più che mai necessaria, che, sul piano normativo, richiede di valersi di disposizioni astratte e generali ed anzitutto di quelle già esistenti, interpretate in chiave evolutiva, rimuovendo anzi le regole eccezionali che talora ne impediscono o comunque ne limitano l'applicazione estensiva, piuttosto che introdurre eccezioni di eccezioni, come sempre più frequentemente avviene, anche a livello comunitario: si pensi alla direttiva UE 2019/790 in materia di diritti d'autore, assolutamente apprezzabile nei suoi obiettivi, raggiunti però con una tecnica giuridica di tipo casistico, che rende arduo ricavarne principi generali suscettibili di più ampia applicazione e pone anzi, almeno nel nostro ordinamento, problemi di conformità al principio costituzionale di eguaglianza, che impone di trattare in modo equivalente situazioni equivalenti<sup>1</sup>.

Uno sforzo di carattere sistematico, che consenta di inquadrare giuridicamente in modo corretto e coerente le nuove tecnologie, si rende necessario anche sotto due ulteriori profili: il primo è quello legato alla contrattua-

---

<sup>1</sup> A mente del principio della parità di trattamento consacrato nell'art. 3 Cost. la legge non può disciplinare in modo difforme fattispecie del tutto corrispondenti, pena l'introduzione di una ingiustificata discriminazione. L'enunciazione di tale principio è chiarissima da tempo immemorabile nella giurisprudenza costituzionale, che ha affermato che «C'è violazione del principio di uguaglianza quando, di fronte a situazioni obiettivamente omogenee, si ha una disciplina giuridica differenziata determinando discriminazioni arbitrarie ed ingiustificate» (così, fra le altre, Corte cost., 25 giugno 1981, n. 111, in *Giur. cost.*, 1981, I, 974 ss.), in forza dell'insegnamento secondo cui «Il principio di uguaglianza di trattamento, sancito dall'art. 3, comma 1°, della Costituzione, impone al legislatore di assicurare ad ognuno eguaglianza di trattamento, quando eguali siano le condizioni soggettive ed oggettive alle quali le norme giuridiche si riferiscano per la loro applicazione» (si veda già Corte cost., 26 gennaio 1957 n. 3 e n. 38, in *Giur. cost.*, 1957, 5 e 398). Allo stesso modo, la più autorevole dottrina in materia ha chiarito che «Il principio costituzionale dell'uguaglianza nella giustizia sociale, espresso dalla norma in esame (l'art. 3 Cost.: n.d.r.) è violato sia quando senza giustificazione costituzionalmente rilevante situazioni uguali vengono a subire un trattamento diverso, sia quando cittadini in situazione differente e sperequata subiscano un trattamento identico» (così ad esempio P. PERLINGIERI, *Commento alla Costituzione Italiana*, Napoli, 2002, 17) e che «il principio (di cui all'art. 3 Cost.: n.d.r.) può dirsi integralmente applicato quando la legge tratti in modo eguali situazioni eguali ed in modo diverso situazioni diverse» (in tal senso, sempre per limitarsi a noti testi istituzionali, T. MARTINES, *Diritto costituzionale*, Milano, 2005, 525). Per alcune applicazioni di questi principi alla materia della proprietà intellettuale si vedano ad esempio C. GALLI, *Le utilizzazioni libere: ricerca*, in *AIDA*, 2002, 144 ss., ove a questo proposito sottolineavo che anche la prescrizione della direttiva 2001/29/CE che impone che le esenzioni in materia di diritto d'autore si applichino solo a casi speciali, non implica un'assoluta discrezionalità dei singoli legislatori nazionali, ma, tutto all'opposto, esige che l'inclusione o l'esclusione di una determinata attività dall'ambito delle esenzioni che si vogliono prevedere siano giustificate dalle peculiari caratteristiche di questa attività; e C. GALLI, A. CONTINI, *Stampanti 3d e proprietà intellettuale: opportunità e problemi*, in *Riv. dir. ind.*, 2015, I, 115 ss., ove si indica l'esigenza di riportare a coerenza sistematica le eccezioni al diritto dei brevetti e quelle alla legge sul diritto d'autore, appunto per rispettare il principio di eguaglianza.

lizzazione delle relazioni di mercato che esse consentono e richiedono, anche per rendere negoziabili i beni della vita che esse vengono a creare, e qui soccorrono, più che le leggi speciali, gli istituti classici del diritto civile generale; e l'altro riguarda proprio i limiti di validità ed efficacia di queste relazioni e di questa negoziabilità, specialmente sotto il profilo della tutela della concorrenza e quindi della disciplina Antitrust.

## 2. Il rapporto tra metaversi e *blockchain* e le esigenze di corretta contrattualizzazione dei relativi rapporti giuridici

Paradigmatici dell'approccio doppiamente inadeguato che si è segnalato, ma al tempo stesso suscettibili di diventare il banco di prova di una nuova impostazione sistematica, capace di dare risposte non solo ai problemi di oggi, ma anche a quelli di domani, sono proprio gli elementi essenziali del fenomeno in esame, e cioè *blockchain* e token, in particolare Non Fungible Token (in acronimo, NFT)<sup>2</sup>, e lo è in realtà lo stesso metaverso, troppo spesso percepiti come legati soltanto alle criptovalute (la *blockchain*), alle opere d'arte "virtuali" (gli NFT) e a una sorta di versione tecnologicamente aggiornata di "Second Life" o "Roblox"<sup>3</sup> (il metaverso). Essi sono certamente tutto questo, ma sono anche molto di più e molte di più sono correlativamente anche le esigenze di corretto inquadramento legale dei problemi e delle opportunità che suscitano, se si è in grado di "leggerle" proprio in una chiave multidisciplinare e sistematica.

Al riguardo si deve anzitutto notare come queste tecnologie, apparentemente molto diverse, siano in realtà strettamente connesse tra loro: la

---

<sup>2</sup>Per un'indagine fenomenologica degli NFT rinvio a A. TOMASICCHIO, *NFT*, Milano, 2022. Sul piano giuridico, nel contesto del diritto statunitense, ma con indicazioni utili anche nella prospettiva europea si segnala M.E. NOH, S.C. ODENKIRK, Y. SHIONOIRI, *GM! Time to Wake Up and Address Copyright and Other Legal Issues Impacting Visual Art NFTs*, in 45 *The Columbia Journal of Law & the Arts*, 2022, 315 ss., ove gli Autori sottolineano tra l'altro che «existing copyright and contract law that apply to the physical art world apply to the NFT world as well», pur mettendone in luce le peculiarità ed in particolare le maggiori difficoltà che in questo ambiente incontra un efficace *enforcement* dei diritti e, a monte di esso, la stessa corretta attribuzione di essi, ma osservando anche come l'evoluzione tecnica in atto e la concorrenza tra le diverse piattaforme possano contribuire a superarle. Affronta problematiche almeno in parte analoghe, ma muovendosi invece nell'ambito del diritto italiano G. CAVANI, *Non Fungible Tokens (NFT): quali interferenze col diritto d'autore*.

<sup>3</sup>In argomento cfr. S. BROWN, *What Second Life and Roblox can teach us about the Metaverse*, in *MIT Management*, 19 July 2022, reperibile alla pagina web <https://mitsloan.mit.edu/ideas-made-to-matter/what-second-life-and-roblox-can-teach-us-about-metaverse>.

*blockchain* è stata definita “*the heart of the Metaverse*”<sup>4</sup>, più ancora delle tecnologie di interfaccia, dell’intelligenza artificiale e della *cloud computing*, che pure ne sono a loro volta componenti essenziali, perché sta alla base del funzionamento dei token che “circolano” sul metaverso (anzi, come diremo, sui metaversi) e della proprietà digitale sulle creazioni di esso, ma prima ancora perché consente la decentralizzazione e l’interoperabilità che, come vedremo, lo caratterizzano e lo differenziano qualitativamente da esperienze apparentemente consimili che lo hanno preceduto. Ed è sicuramente fonte di preoccupazione che la titolarità dei brevetti sulle tecnologie più innovative della *blockchain* – che in sé è solo relativamente giovane, perché le prime pubblicazioni che la riguardano risalgono agli Anni Novanta del secolo scorso, con i primi studi di scienziati come Stuart Haber e Scott Stornetta –, brevetti cresciuti esponenzialmente a partire dal 2015, sia prevalentemente in capo a società cinesi: 9 su 10 dei maggiori detentori di famiglie di brevetti in questo campo sono cinesi (la decima, che è la sesta nella classifica, è la IBM)<sup>5</sup>.

La *blockchain*, infatti, benché abbia trovato le sue prime e più note applicazioni nel modo della finanza e delle criptovalute (certamente a loro volta importanti anche nel metaverso), si configura come un sistema decentralizzato di “notarizzazione” di singoli dati, che possono riguardare non solo transazioni, ma anche moduli e processi e che, una volta inseriti, risultano sostanzialmente imm modificabili, fornendo anche datazione e geolocalizzazione certe dell’immissione, poiché la modifica richiederebbe il consenso di tutti i partecipanti alla catena (i “nodi”, come vengono abitualmente chiamati), i quali sono potenzialmente infiniti. Della tecnologia *blockchain* si è così avvalsa ad esempio Benetton, nell’ambito del progetto “*Blockchain in a Box*”, elaborato in seno al Gruppo italiano del Council of Supply Chain Management Professionals (CSCMP), per realizzare una lettera di vettura elettronica impiegata nei trasporti internazionali su strada, rendendo più trasparente e controllabile la filiera e riducendo quindi i rischi di abusi e di illegalità, compresa la contraffazione, in particolare sotto la forma dell’immissione illecita in commercio di merci in transito<sup>6</sup>.

---

<sup>4</sup> L’affermazione, proveniente dalla nota società di consulenza Goldman Sachs, ha fatto il giro del web, comparando in numerosi articoli su riviste in ambito tecnologico.

<sup>5</sup> Per questi dati si veda A. YADAV, *The Metaverse: What is the IP Reality of the Virtual World*, in *NFTs, Cryptocurrency & the Metaverse*, 2022, 48 ss., dove tra l’altro analizza le diverse tecnologie che contribuiranno a configurare l’“ecosistema” del metaverso, concentrandosi in particolare su interfacce, *blockchain*, intelligenza artificiale e cloud computing.

<sup>6</sup> Il tema dell’istituzione di una lettera di vettura elettronica, collegata alla tecnologia *blockchain* ha formato oggetto dell’attività del Gruppo di Lavoro sulla *Blockchain* nella *supply*

Una corretta contrattualizzazione – anche sul piano dei rimedi e della gestione efficace (ed *enforceable*) delle controversie -, che tenga conto insieme degli aspetti tecnici e delle implicazioni giuridiche del ricorso a questa tecnologia, può infatti consentire l’adozione su larga scala della *blockchain* come tecnologia garante dei flussi documentali digitalizzati scambiati tra le parti di un rapporto, cosa di estrema importanza sia nel sempre più diffuso Internet of Things<sup>7</sup>, sia nella gestione delle filiere produttive (che con l’utilizzo di questa tecnologia possono essere più facilmente garantite da marchi collettivi e di certificazione, i quali rappresentano oggi valori aggiunti sempre più importanti per le imprese che se ne avvalgono, comunicando per il tramite di essi il proprio impegno su temi come l’etica e la sostenibilità), sia nel controllo dello *smartworking* e nella sua integrazione nell’organizzazione del lavoro<sup>8</sup>, sia nella circolazione delle tecnologie segrete, oggi più che mai necessaria, a fronte delle criticità che emergono nelle *supply chain* e che rendono quindi spesso consigliabile completare i processi produttivi nei Paesi di destinazione delle merci, facendo “viaggiare” materialmente solo i semilavorati: dunque integrando virtuosamente (e in modo sicuro) mondo reale e mondo virtuale.

Ed è importante notare quanto ciò sia suscettibile di sviluppi virtuosi sul piano concorrenziale, perché non esiste “una” *blockchain*, ma vi sono plurime catene, con diversi livelli di affidabilità e di complessità e anche di costo e di sostenibilità, economica e ambientale, anche in considerazione dei consumi energetici che questa tecnologia comporta e che oggi costituisce un tema più che mai critico.

---

*chain* costituito all’interno del Gruppo italiano del Council of Supply Chain Management Professionals (CSCMP), costituito allo scopo di approfondire i processi di gestione delle spedizioni internazionali di merci, assumendo un approccio interamente digitale basato sui c.d. registri distribuiti (DLT), per superare le criticità delle filiere, e in particolare i problemi di controllo (anche contro la contraffazione) e di affidabilità. A tal fine è stato già realizzato con Benetton un progetto pilota, che ha previsto l’introduzione di una lettera di vettura elettronica (che trasforma in una sua mera stampa la lettera di vettura cartacea, in attesa di poterla integralmente sostituire) nell’ambito del trasporto su strada disciplinato dalla CMR (*Convention relative au contrat de transport international de Marchandises par Route*), che rimane il più diffuso negli scambi in ambito europeo. A tal fine è stata predisposta una clausola contrattuale-modello da inserire in ciascun contratto di trasporto (se la vendita non avviene con resa *ex works*), ovvero da sviluppare in autonomo contratto collegato a quello di trasporto (se, invece, la resa sarà *ex works*, come frequentemente avviene), che vincoli tutte le parti – acquirente, venditore, vettore, eventuale spedizioniere ed eventuali *sub-contractors* del vettore – ad impiegare una lettera di vettura elettronica e-CMR e che abbia alla base l’utilizzazione delle tecnologie *blockchain*.

<sup>7</sup>Sul tema, si veda F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, spec. 281 ss.

<sup>8</sup>Per uno spunto in tal senso si veda *Software di controllo degli smart worker all’esame di privacy*, in *Privacy News*, 2021, 11, 41 ss.

### 3. Token e Non Fungible Token e il loro rapporto con *blockchain* e metaverso

Questa integrazione è ancora più evidente negli NFT, a loro volta garantiti proprio attraverso il ricorso alla tecnologia *blockchain*<sup>9</sup>, che non sono soltanto utilizzati per rendere riconoscibili (e negoziabili) come tali gli “originali” delle opere d’arte digitali, distinguendoli dalle copie, ma possono diventare – sempre attraverso un’adeguata contrattualizzazione (che frequentemente prevede anche il pagamento di una *royalty* al titolare dei diritti in caso di cessione del *token*, secondo un modello che ricorda il diritto di seguito sulle vendite successive delle opere dell’arte figurativa<sup>10</sup>) – veri e propri titoli di credito *sui generis*, a loro volta negoziabili, rappresentativi (*token*, appunto) di beni e servizi del mondo reale, magari non ancora prodotti (e che verranno prodotti sulla base della domanda, riducendo gli sprechi, domanda magari raccolta attraverso processi di *crowd-funding*<sup>11</sup>, dunque anche qui facilitando l’accesso al mercato anche di start-up con poche disponibilità finanziarie, tanto più se poi la prima produzione può avvenire attraverso tecnologie additive, ossia di stampa 3D, che non comporta economie di scala<sup>12</sup>), e che gli utilizzatori della rete possono scegliere in negozi virtuali – e quindi sono a loro volta essenziali per il funzionamento del metaverso – e poi ritirare o farsi consegnare nel mondo reale.

Ad essi, quindi, sono pienamente applicabili le disposizioni in materia di proprietà intellettuale, a cominciare dalla norma recentemente introdotta

---

<sup>9</sup>Sul fondamentale ruolo che la tecnologia *Blockchain* svolge nella creazione e nella circolazione degli NFT e sul rilievo che essi assumono nel contesto del nascente Web3 e quindi anche nello sviluppo del Metaverso, in particolare sotto il profilo della decentralizzazione si veda GARON, *Legal Implications of an Ubiquitous Metaverse and a Web3 Future*, in 106 *Marquette Law Review* (2022), 163 ss., spec. 180-185.

<sup>10</sup>Strategie di questo tipo sono molto frequenti sui c.d. registri distribuiti: si veda il recente caso Trib. Roma, ord., 19 luglio 2022, in *Diritto ind.*, 2022, con nota di A. RAINONE, *Sul rapporto tra diritto di seguito e arte contemporanea*. In argomento si veda altresì S. STABILE, E. DEL SASSO, *Il “diritto di seguito” nel mercato primario dell’arte contemporanea*, sempre in questa *Rivista*, 2012, 507 ss.

<sup>11</sup>Nel nostro Paese un esempio di crowdsourcing diretto a selezionare e presentare al pubblico prodotti di design innovativi, producendo però solo il numero di pezzi che le persone realmente desiderano avere e solo quando si fosse raggiunto un punto di breakeven che rendesse conveniente e profittevole iniziarne l’effettiva produzione è stato il progetto Natevo. In argomento rinvio alla pagina web <https://www.domusweb.it/it/design/2013/03/28/natevo-crowdsourcing-design.html>.

<sup>12</sup>Per la sottolineatura di questi aspetti cfr. A. MINGARDI, *Distruzione creativa? Stampanti 3D, nuovi metodi di produzione e vecchie paure* e M. SOBRERO, *L’avvento della manifattura additiva: sviluppi tecnologici e modelli di business*, entrambi in C. GALLI, A. ZAMA, *Stampa 3D – Azienda, economia, finanza, IT, brevetti, lavoro, sicurezza, ambiente. Profili giuridici e opportunità di business*<sup>2</sup>, Bologna, 2015, rispettivamente 27 ss. e 49 ss.

ta nell'art. 20 del Codice della Proprietà Industriale (e nell'art. 10, regolamento UE 2017/1001 sul marchio dell'Unione europea), che attribuisce al titolare anche il diritto di vietare, salvo proprio consenso, di apporre il segno su “*altri mezzi su cui il marchio può essere apposto ovvero di offrire, immettere in commercio, detenere a tali fini, importare o esportare tali mezzi recanti il marchio, quando vi sia il rischio che gli stessi possano essere usati in attività costituenti violazione del diritto del titolare*”<sup>13</sup>.

Sempre tra i token rientrano altresì i *fan token*, attraverso i quali il titolare dei diritti sui segni distintivi o sulle immagini o su altri materiali coperti dal diritto d'autore può instaurare un rapporto più stretto e coinvolgente con il pubblico, facendolo sentire parte di una *community* che si costituisce proprio intorno al valore comunicazionale ed esperienziale di questi oggetti virtuali, tutelati appunto attraverso i diritti della proprietà intellettuale, anzitutto marchi e diritto d'autore, ma, almeno in prospettiva, anche i disegni e modelli, specialmente se verrà approvata la proposta di riforma del regolamento n. 6/2002/CE e della direttiva 1998/71/CE nel testo attualmente in discussione, che sembra annoverare in modo espresso l'aspetto esteriore delle opere digitali tra le creazioni tutelabili con questo diritto di esclusiva<sup>14</sup>, ovviamente quando sussistano i requisiti previsti in generale per l'applicazione di esso.

#### 4. Metaversi e diritto dei marchi

Questa prospettiva consente di comprendere che anche il metaverso non è solo un mondo virtuale parallelo a quello reale, bensì può diventare una componente importante della comunicazione d'impresa e della fidelizzazione dei consumatori, riproducendo e integrando le esperienze di *shopping* del mondo reale ed estendendole a servizi che per il consumatore hanno un valore proprio perché sono in rapporto con questo mondo reale e non perché rappresentano un'alternativa economicamente più accessibile

---

<sup>13</sup> In argomento cfr. il mio *L'ambito di protezione del marchio: problemi risolti, problemi ancora aperti e nuovi problemi*, in questa *Rivista*, 2017, 125 ss.

<sup>14</sup> Cfr. la *Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (CE) n. 6/2002 del Consiglio su disegni e modelli comunitarie abroga il regolamento (CE) n. 2246/2002 della Commissione*, documento COM(2022) 666, reperibile alla pagina web [https://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/com/2022/0666/COM\\_COM\(2022\)0666\\_IT.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2022/0666/COM_COM(2022)0666_IT.pdf) e *Proposta di Direttiva del Parlamento Europeo e del Consiglio sulla disciplina giuridica dei disegni e modelli (rifusione)*, documento COM(2022) 667, reperibile alla pagina web <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0667&from=EN>. La proposta di riforma del regolamento riguarda gli artt. 3, 18 *bis*, 19, 20, 20 *bis*, 26 *bis*, 36, 36 *bis*, 37, 96, mentre la proposta di riforma della direttiva riguarda gli artt. 1-20.

ad esso<sup>15</sup>, aprendo quindi una nuova frontiera alla concorrenza tra imprese, sempre fondata sulla capacità di internalizzare e valorizzare le esternalità positive che si costituiscono intorno ai segni distintivi<sup>16</sup> e dunque allo sfruttamento della funzione pubblicitaria, di comunicazione e di investimento che ai marchi viene oggi riconosciuta, secondo l'insegnamento della Corte di Giustizia europea<sup>17</sup>, e che giustificano sempre di più la felice metafora di Stefano Sandri, che già molti anni fa parlava di "marchi personificati"<sup>18</sup>, ossia percepiti dai consumatori come amici, più o meno fidati, che li consigliano e li orientano nelle loro scelte commerciali, culturali e sociali.

Anche il metaverso, in realtà, è nuovo solo in senso relativo: il suo nome nasce da un romanzo del 1992 dello scrittore americano Neal Stephenson, *Snow Crash*<sup>19</sup>, che chiamava con questo nome un universo virtuale creato da un computer, nel quale un personaggio del romanzo passava gran parte del suo tempo, estraniandosi dalla vita di ogni giorno. Al di fuori della finzione romanzesca, la tecnologia del metaverso ha come base la creazione di una forma di realtà aumentata accessibile via web, nella quale si può agire anche attraverso i propri alter ego (gli avatar)<sup>20</sup>.

---

<sup>15</sup>I diversi *business models* suscettibili di creare valore attraverso le varie forme del metaverso e il relativo impatto economico e finanziario sono indagati da R. MORO VISCONTI, *From physical reality to the Metaverse: a Multilayer Network Valuation*, in 2 *Journal of Metaverse* (2022), 16 ss. In una prospettiva analoga, ma dedicandosi principalmente alla ricognizione delle esperienze già in atto di uso commerciale del metaverso, si veda anche C. BUSHHELL, *The Impact of Metaverse on Branding and Marketing – A Study of How Individuals and Celebrities Use Metaverse as a Brand Extension, and the Implications for Marketing*, disponibile in rete alla pagina web <http://dx.doi.org/10.2139/ssrn.4144688>.

<sup>16</sup>Rinvio in argomento al notissimo studio di W.M. LANDES, R.A. POSNER, *The Economics of Trademark Law*, in 78 *TMR*, 1988, 267 ss. [versione rielaborata di *Trademark Law: an Economic Perspective*, in 30 *Journ of Law and Econ.*, 1987, 265 ss.] e a quello parimenti importante di N. ECONOMIDES, *The Economics of Trademarks*, in 78 *TMR*, 1988, 523 ss., dei quali ho cercato di sviluppare alcuni spunti in C. GALLI, *Protezione del marchio e interessi del mercato*, in AA.VV., *Studi di diritto industriale in onore di Adriano Vanzetti*, Milano, 2004, 661 ss.

<sup>17</sup>Corte giust. U.E., 22 settembre 2011, nel procedimento C-323/09, *Interflora*, su cui mi soffermo nel mio articolo.

<sup>18</sup>S. SANDRI, *Il marchio personificato*, in *Riv. dir. ind.*, 2006, I, 68 ss. L'Autore costruiva questa categoria a partire dall'osservazione, mutuata da studi di psicologia dei consumi, secondo cui il pubblico «tende ad antropomorfizzare il marchio, ricercandone i valori personali di cui si carica e recuperandoli secondo le proprie esigenze valoriali». In questa prospettiva, oggi più che mai attuale, i marchi «divengono vere e proprie icone culturali, che i consumatori conoscono e riconoscono appunto come portatori di messaggi specifici, dai quali non è possibile prescindere nel giudicare della possibile interferenza tra segni simili»: così, commentando l'articolo di Sandri, C. GALLI, *Segni distintivi e industria culturale*, in *AIDA*, 2006, 339 ss., a p. 351.

<sup>19</sup>N. STEPHENSON, *Snow Crash*, New York, 1992 (edizione italiana: Milano, 2007).

<sup>20</sup>La caratteristica per cui gli utenti potranno avere sul metaverso «un nuovo corpo digitale»

Come ha spiegato in un recente *webinar* organizzato da *The Economist*<sup>21</sup> il Global Affairs President di Meta, Nick Glegg, la tecnologia del metaverso non consiste solamente in un hardware o in un software, ma è una nuova *computing platform*, che può essere vista come la costruzione di un Internet “nuovo”, che però rappresenta solo un’evoluzione della esistente tecnologia che, dalla nascita del computer all’approdo sul mercato di *smartphone* e *social*, si sta orientando verso una direzione ben chiara, cioè fornire servizi che consentono alle persone di avvicinarsi e interagire al di là della distanza fisica. Questa, in fondo – ha sottolineato ancora Glegg nel corso del Webinar – è sempre stata la promessa di Internet, fin dai suoi albori: consentire una comunicazione al di là della distanza e dei limiti geografici, per cui – coerentemente con le radici da cui proviene – connettere le persone è anche la promessa del metaverso.

Lo *step forward* rispetto al passato consisterebbe nella possibilità per le persone di ritrovarsi virtualmente nello stesso spazio digitale, man mano che la tecnologia si affinerà e diventerà sempre più avanzata, beneficiando di servizi sempre nuovi: i problemi che Meta sta incontrando ad imporsi – e che l’anno scorso avevano fatto diminuire drasticamente (–60%) il valore delle sue azioni – nascono proprio dall’inadeguatezza tecnologica, dalla presenza di bug nel software che stanno rallentando il lancio di nuovi servizi e quindi dalla sua scarsa attrattività sugli utenti<sup>22</sup>. Ciò non toglie però che non solo Meta, ma anche altri soggetti qualificati come Microsoft ed Apple stiano investendo significativamente nella realtà aumentata, il che

---

è tra quelle su cui maggiormente insiste Meta ed ha in effetti colpito la fantasia di chi si è occupato del fenomeno: si veda ad esempio l’articolo di B. RUFFILLI, *L’annuncio di Zuckerberg: «Nel metaverso avremo anche le gambe»*, in *la Repubblica – Italian Tech*, 11 ottobre 2022.

<sup>21</sup> Economic Opportunities in Virtual Worlds, 27 settembre 2022, ai cui contenuti si farà riferimento a seguire nel testo. Una sintesi dei contenuti di questo seminario e degli altri inclusi nello stesso ciclo si trova alla pagina web [https://images.go.economist.com/Web/Economist-Conferences/%7Bbc86d19b-b7d9-4192-ab65-34479ccb9e18%7D\\_Meta2022\\_Summary.pdf?RefID=EM8295-Meta2022\\_Webinar3-PR](https://images.go.economist.com/Web/Economist-Conferences/%7Bbc86d19b-b7d9-4192-ab65-34479ccb9e18%7D_Meta2022_Summary.pdf?RefID=EM8295-Meta2022_Webinar3-PR).

<sup>22</sup> Cfr. per tutti, l’articolo di A.R. CHOW, *A Year Ago, Facebook Pivoted to the Metaverse. Was It Worth It?*, in *Time*, 27 ottobre 2022. Anche i recenti recuperi del titolo sul mercato azionario appaiono legati non solo al contenimento delle perdite nell’ultimo trimestre del 2022, ma anche allo sviluppo di nuove tecnologie in grado di superare alcuni limiti del sistema, in particolare l’accentuata dipendenza dalle capacità del sistema operativo mobile di Apple nel tracciamento e nella misurazione degli annunci pubblicitari: in argomento si veda *Thing are looking up for Meta*, in *The Economist*, 2 febbraio 2023, dove si riferisce tra l’altro che «Meta has come up with ways to work around Apple’s privacy settings. Its artificial-intelligence capabilities are improving, both in the lab and in the real world – specifically, in the world of Reels, where algorithms for serving up short videos on Facebook and Instagram, Meta’s two profit motors. These are reportedly getting cleverer at creating engagement».

lascia supporre – anche queste previsioni sono state fatte nel webinar citato – che nel giro di due anni il metaverso possa perfezionarsi a sufficienza per diventare realmente attrattivo, in cinque anni la sua realtà virtuale diventerà un luogo abituale per trascorrere il tempo, fare acquisti, organizzare meeting e che in dieci anni potrà raggiungere la sua maturità. Tuttavia – e questo è probabilmente il punto decisivo – il *plus* di questa tecnologia dovrebbe consistere proprio nel fatto che, se funzionerà secondo le intenzioni, esso non sarà composto né da un metaverso unico, né da un fascio di metaversi tra loro paralleli (il metaverso di Google, il metaverso di Microsoft, il metaverso di Meta), ma, come Internet, sarà composto da una rosa di servizi e di luoghi virtuali con caratteristiche diverse, ma tutti connessi, grazie all'interoperabilità tra le tecnologie che al suo interno confluiranno, seppur sviluppate da operatori economici differenti<sup>23</sup>.

In questo senso il tema giuridico che il metaverso pone al diritto dei marchi non è tanto quello della classificazione dei prodotti o dei servizi che vi si troveranno. L'EU IPO ha già chiarito che, ai fini della registrazione, i beni virtuali (naturalmente una volta specificati) saranno inseriti nella classe 9, gli NFT saranno definiti come *file* digitali scaricabili garantiti tramite la tecnologia *blockchain*, i marchi per i servizi di commercio elettronico nel metaverso potranno beneficiare della registrazione nella classe 35 dove si collocano i servizi di vendita (anche qui specificando le tipologie di beni che saranno venduti) e i servizi di trattenimento che costituiranno certamente una componente importante del metaverso si collocheranno nella classe 41, mentre i servizi di *information technology* diretti alla creazione di questi ambienti virtuali saranno inseriti nella classe 42<sup>24</sup>. Ma se questo aspetto è certamente molto rilevante per i nuovi marchi che, non avendo ancora avuto il “batte-simo” del mercato, non comunicano ancora alcun messaggio al pubblico di riferimento, cosicché l'ampiezza della loro tutela dipende esclusivamente dalle rivendicazioni merceologiche effettuate all'atto della registrazione (con la sola estensione ai prodotti e servizi astrattamente “affini” a quelli rivendi-

---

<sup>23</sup> Per un'ampia analisi delle ragioni tecniche, giuridiche ed economiche che inducono a ritenere che ciò che emergerà dall'evoluzione in atto sarà «a multiverse, a loose confederation of distinct virtual worlds and metaverse environments», ossia «an international, partially interoperable array of metaverses, each subject to a different mix of state authority, corporate oversight and participatory governance» si veda ancora J. GARON, *Legal Implications of an Ubiquitous Metaverse and a Web3 Future*, cit., 171 ss., tra le quali l'Autore dà ampio spazio al «movement towards Web3, the next phase in the development of the digital economy».

<sup>24</sup> Si soffermano soprattutto su questi aspetti T. VERBORGH, B. DE JAN, *EU Trademarks related to the metaverse*, in *ILO*, 10 October 2022. Cfr. anche S. DI VIRGILIO, *Il Metaverso per aziende e brand*, in *Sprint*, 21 December 2022, dove cita l'esempio di Nike, che ha registrato il suo marchio “Nike-land” nelle classi 9, 35 e 41, appunto nella prospettiva di meglio tutelarsi nel metaverso.

cati), per quelli già usati ipotizzare che essi non possano essere fatti valere nel metaverso, ove non siano stati registrati specificamente nelle classi sopra indicate, è ingenuo quanto lo è stato a suo tempo pensare che Internet fosse uno spazio senza legge, essendo vero esattamente l'opposto, perché i luoghi virtuali raggiungibili dagli utenti di tutto il mondo sono soggetti contemporaneamente alle leggi di tutti i Paesi ai cui utenti si rivolgono<sup>25</sup>; e la protezione dei marchi più famosi per definizione si estende anche ai prodotti e servizi per i quali non sono registrati, quando viene usato nell'attività economica in relazione ad essi un segno eguale o simile, in relazione al quale gli utenti possono istituire un collegamento, da cui derivi alternativamente un vantaggio per l'utilizzatore non autorizzato o un pregiudizio per il titolare concernenti il messaggio di cui il marchio è portatore<sup>26</sup>.

Almeno nel nostro ordinamento, dopo la riforma del 2010 (ma già prima, se si pensa ad esempio al caso Bulgari<sup>27</sup> o, a livello comunitario, al caso Adidas/Fitnessworld<sup>28</sup>), non vi è anzi dubbio sul fatto che anche usi non

---

<sup>25</sup> In argomento, a proposito di questo problema per Internet, cfr. S. MAGNI, M.S. SPOLIDORO, *La responsabilità degli operatori in Internet: profili interni e internazionali*, *Dir. inf e inf.*, 1997, 63 ss., spec. 79 ss., che parlano al riguardo di «frazionamento delle competenze giurisdizionali». Dei problemi di giurisdizione e di legge applicabile che si pongono in relazione al web ed ai criteri da seguire per affrontarli, rimando al mio *I domain names nella giurisprudenza*, Milano, 2001, spec. 81 ss. e 88-89.

<sup>26</sup> In argomento, ampiamente C. GALLI, *L'ambito di protezione del marchio*, in C. GALLI, A.M. GAMBINO, *Codice commentato della Proprietà Industriale e Intellettuale*, Torino, 2011, 245 ss., spec. 312 ss. Di questi principi ha fatto una piana applicazione anche Trib. Roma, 20 luglio 2022, in questa *Rivista*, 2022 con nota di A. RAINONE, salutata come la prima applicazione del diritto dei marchi ad un NFT, che ha ritenuto violati i marchi della Juventus utilizzati senza autorizzazione in un prodotto "virtuale" (*cards*) consistente nell'elaborazione dell'immagine di un suo ex-calciatore, appunto in relazione all'aggiungimento a tali marchi e al loro valore comunicazionale derivante da quest'uso, che il Tribunale ha correttamente ritenuto effettuato nell'attività economica, avendo rilevato che «l'operazione della creazione e vendita di dette *cards* ha esclusivi fini commerciali». Si veda anche M.D. MURRAY, *Trademarks, NFTs, and the Law of the Metaverse*, destinato a 6 *Arizona Law Journal of Emerging Technologies* (2023), ma già disponibile online, che discute vari casi statunitensi in cui vengono in considerazione ipotesi di uso non autorizzato di marchi famosi altrui nel contesto di NFTs, prendendo in considerazione anche il limitato spazio che può avere la *artistic fair use defense*.

<sup>27</sup> Cfr. Trib. Milano, decr. 28 ottobre 2005, poi confermato da Trib. Milano, ord. 14 novembre 2005 e seguito da un secondo provvedimento cautelare (ord. 1° settembre 2006, reperibile in forma anonimizzata alla pagina web [https://www.iplawgalli.it/wp-content/uploads/2014/05/NEWSLETTER\\_2\\_2006.pdf](https://www.iplawgalli.it/wp-content/uploads/2014/05/NEWSLETTER_2_2006.pdf)) e dalla sentenza di merito del 16 gennaio 2009, che hanno tutti tutelato il marchio Bulgari contro l'uso nell'attività economica del nome Bulgari come pseudonimo di un'attrice pornografica.

<sup>28</sup> Corte giust. U.E., 23 ottobre 2003, nel procedimento C-408/01, *Adidas/Fitnessworld*, in *Riv. dir. ind.*, 2004, II, 141 ss., con nota di C. GALLI, *I limiti di protezione dei marchi rinomati nella giurisprudenza della Corte di Giustizia C.E.*

distintivi di segni eguali o simili al marchio altrui vadano sanzionati, purché ciò che ne forma oggetto sia percepito anche come portatore di un messaggio che richiama il marchio: ciò è infatti oggi espressamente previsto dall'art. 20, comma 1, lett. c), c.p.i. In questa prospettiva diventerà invece importante soprattutto stabilire dove si colloca il limite del giusto motivo e dove finiscono gli usi nell'attività economica e quelli che rientrano invece nella libertà di espressione garantita dall'art. 21, e non dall'art. 41 Cost.<sup>29</sup>: ed è difficile, io credo, sostenere che la "MetaBirkin" sia un'opera d'arte e non un prodotto, per quanto virtuale, che deriva la sua attrattività proprio dal richiamo a Hermes<sup>30</sup>.

Questo strumento creerà perciò (e sta già creando) anche nuove opportunità per lo svolgimento di attività di *licensing* e soprattutto di *co-branding*, dato che consente di creare più facilmente circoli virtuosi di utilizzazioni coordinate di segni distintivi imprenditoriali, ma anche di marchi territoriali e di DOP e IGP, per valersi scambievolmente e in modo reciprocamente profittevole dei rispettivi valori comunicazionali positivi<sup>31</sup>, specialmente per competere su un mercato che resta globale anzitutto perché globale è la rete web<sup>32</sup> (almeno dove la libertà economica si accompagna alla libertà politica, senza la quale del resto anche la prima è inevitabilmente limitata, come in Cina o nella Russia neosovietica di Putin).

---

<sup>29</sup> Su questo necessario coordinamento e più in generale sulla nozione di giusto motivo e della contraffazione realizzata mediante usi non distintivi del marchio rinvio al mio *L'ambito di protezione del marchio*, in C. GALLI, A.M. GAMBINO, *Codice commentato della Proprietà Industriale e Intellettuale*, Torino, 2011, 254 ss., spec. 325-332; e M. RICOLFI, *Trattato dei marchi*, Torino, 2015, vol. II 758 ss.

<sup>30</sup> Il tema si sarebbe potuto porre nel caso deciso da Trib. Roma, ord., 20 luglio 2022, cit., che, pur non affrontandolo *ex professo*, ha correttamente attribuito rilievo, ai fini del riconoscimento della contraffazione dei marchi della Juventus, alla circostanza per cui «anche la fama delle diverse squadre in cui il calciatore ha giocato contribuisc(e) a dare valore all'immagine digitale da acquistare».

<sup>31</sup> Sulle opportunità che il *co-branding* offre si veda già G. IASEVOLI, *Le alleanze di marketing. Sviluppare, gestire e valutare il co-branding e il co-marketing*, Milano, 2004. Con specifico riferimento all'uso in *co-branding* dei segni distintivi degli enti territoriali e culturali e di consorzi di tutela di DOP e IGP insieme a quelli di prodotti industriali, nella prospettiva di valorizzazione reciproca si veda in particolare il capitolo *Nomi geografici, protezione contro l'aggancio parassitario e opportunità di licensing globale*, in C. GALLI, D. MAININI, D. ZANI, *Competere con il brand sul mercato globale*, Bologna, 2017, 190 ss.; e CONTINI, *La tutela specifica di Indicazioni geografiche e Denominazioni di origine*, in C. GALLI, A.M. GAMBINO, *Codice commentato della Proprietà Industriale e Intellettuale*, Torino, 2011, 442 ss., spec. 455-457. dove si sofferma sulle possibilità di sfruttamento attivo della reputazione delle denominazioni tutelate.

<sup>32</sup> In una prospettiva più ampia si veda su questo stesso tema anche F. ALBERONI, C. CATANELO, 1989-2019. *Il rinnovamento del mondo*, Milano, 2021.

## 5. Metaversi, nuove tecnologie e gestione dei dati

Nel campo del diritto (e della concorrenza, che vive sempre in rapporto dialettico con le esclusive<sup>33</sup>) rientrano del resto anche le tecnologie attraverso le quali queste nuove applicazioni informatiche funzionano, che possono essere coperte da diritti d'autore (come nel caso del *software* e quindi anche degli algoritmi che le governano) o anche da brevetti (anche sulle *computer implemented inventions* e sugli stessi *software* che producano un effetto tecnico ulteriore alla necessaria interazione di essi col computer)<sup>34</sup>: anzi, è proprio l'esistenza di questi diritti che consente ai titolari di scegliere se consentirne o meno usi liberi da parte di terzi, subordinando questi usi al rispetto di regole che si estendono anche alle elaborazioni realizzate da questi terzi, come nel caso delle licenze *creative commons*<sup>35</sup> ormai largamente tipizzate dalla pratica e riconducibili all'ambito delle regole oggettive del commercio internazionale<sup>36</sup>. E certamente è da prevedere che con lo sviluppo di questi fenomeni si creeranno anche degli standard, con la correlativa presenza di Standard Essential Patents (SEP)<sup>37</sup>, proprio per-

---

<sup>33</sup> Per la sottolineatura di questo aspetto e delle implicazioni che esso comporta nell'interpretazione delle norme che delimitano il contenuto delle esclusive industrialistiche, cfr. C. GALLI, *La nozione di diritti di proprietà industriale e l'inquadramento generale del Codice della proprietà industriale tra diritto internazionale e comunitario e diritti naturali*, in C. GALLI, A.M. GAMBINO, *Codice commentato della Proprietà Industriale e Intellettuale*, Torino, 2011, 3 ss., spec. 27-28.

<sup>34</sup> Per un quadro d'insieme si vedano G. MUSCOLO, *Innovazione nella rete e diritti non titolati: il ruolo di know how, copyright, banche dati e pratiche commerciali sleali*, in questa Rivista, 2015, 114 ss.; L. BOSOTTI, *I limiti di brevettabilità nelle innovazioni della rete*, *ibidem*, 137 ss.; M. BOTTI, *La tutela del software*, *ibidem*, 146 ss.; e C. GALLI, *L'innovazione nel web: opportunità e problematiche giuridiche*, *ibidem*, 105 ss. (tutti nel fascicolo che raccoglie i saggi che sviluppano le Relazioni tenute al Convegno "Fare e brevettare: le innovazioni del nuovo web", tenutosi a Parma il 31 ottobre 2014).

<sup>35</sup> Per un inquadramento giuridico del fenomeno rinvio a L. CHIMIENTI, *Come cambia il diritto d'autore in Internet*, in B. CASSANO, B. TASSONE, *Diritto industriale e diritto d'autore nell'era digitale*, Milano, 2022, 107 ss., spec. 124-133, che richiama tra l'altro opportunamente le *Conclusioni* presentate il 10 settembre 2020 dall'Avvocato Generale Szpunar nel procedimento C-392/19 (poi deciso dalla sentenza di Corte giust. UE, 9 marzo 2021), nelle quali esse sono presentate come un modello da seguire anche per altre problematiche della rete, in particolare per offrire «la flessibilità necessaria nei casi in cui i titolari dei diritti d'autore intendessero autorizzare collegamenti automatici alle loro opere» (punto 107).

<sup>36</sup> Per quest'ultima nozione si veda già M.J. BONELL, *Le regole oggettive del commercio internazionale*, Milano, 1973; e, per un inquadramento generale di esse nel contesto attuale della varietà delle fonti del diritto, A. MAZZONI, M.C. MALAGUTI, *Diritto del commercio internazionale. Fondamenti e prospettive*, Torino, 2019, spec. 143 ss., dove gli Autori si soffermano sul rilievo di contratti tipo e clausole standard come fonti di un diritto transnazionale non statale.

<sup>37</sup> Un'articolata riflessione a più voci sugli Standard Essential Patents, tra ruolo economico e

ché, come si diceva, le caratteristiche essenziali dei metaversi sono proprio l'interoperabilità e la decentralizzazione.

Ed ancora è disciplinata dal diritto la sorte dei dati generati da questi strumenti e dalle interazioni degli utenti con essi, che devono rispettare anzitutto le regole in materia di *privacy* (compresi i diritti alla cancellazione), ma che possono a loro volta costituire oggetto di diritti, sotto forma di *database* e di *trade secret*<sup>38</sup>, come tali negoziabili e idonei ad essere trattati in modo da generare metadati, parimenti negoziabili e utilizzabili nell'ambito del *data learning* che sta alla base dell'altra grande tecnologia del futuro, l'intelligenza artificiale, anch'essa spesso "volgarizzata" e fraintesa, mentre va apprezzata (e valutata giuridicamente) per quello che è, uno strumento idoneo a facilitare e a rendere molto più rapida la ricerca, la creazione e soprattutto l'innovazione<sup>39</sup>.

Anche in questo caso non abbiamo dunque bisogno di nuove norme *ad hoc*, bensì di un'interpretazione evolutiva delle norme già esistenti, in materia di esclusive e di concorrenza, le une e le altre applicabili senza sostanziali differenze anche al web e ai soggetti che vi operano, anche non imprenditori, in quanto vi svolgano comunque un'attività economica, come nel caso degli *influencer* della rete (o aspiranti tali, che promuovono comunque se stessi in questo ruolo e quindi non possono sottrarsi alla disciplina delle pratiche commerciali, nel cui perimetro la loro attività incontestabilmente si colloca<sup>40</sup>), attraverso il necessario dialogo e la condivisione delle diverse competenze ed esperienze degli operatori del mercato, dei tecnici, degli esperti di comunicazione, degli economisti e dei giuristi.

---

disciplina giuridica in Europa dopo la sentenza nel caso *Huawei* (Corte giust. CE, 16 luglio 2015, nel procedimento C-170/13), si rinvia nel fascicolo 1 del 2017 della rivista *Orizzonti del diritto commerciale*, con i saggi di E. Arezzo, F. Denozza, G. Ghidini e G. Trabucco, M. Libertini, V. Meli, G. Muscolo e C. Osti. In una prospettiva principalmente economica (ma anche con un'analisi giuridica comparatistica dei principali ordinamenti) si veda anche J. PADILLA, D.H. GINSBURG, K.W. WONG-ERVIN, *Antitrust Analysis Involving Intellectual Property and Standards: Implications from Economics*, in 33 *Harvard Journal of Law & Technology*, 2019, 1 ss.

<sup>38</sup> Cfr. i saggi raccolti in V. FALCE, G. GHIDINI, G. OLIVIERI, *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, tra cui in particolare, sul profilo segnalato nel testo, C. GALLI, M. BOGNI, *I requisiti per la tutela IP dei Big Data*, 93 ss.

<sup>39</sup> Sul ruolo dell'intelligenza artificiale nell'innovazione esaminato specialmente dal punto di vista del diritto dei brevetti si vedano L. BOSOTTI, *Nuove creazioni del web, intelligenza artificiale e rapporto tra invenzioni e diritto d'autore*, in *Diritto ind.*, 2021, 180 ss.; e C. GALLI, M. BOGNI, *Intelligenza artificiale, nuove dinamiche della ricerca e problem and solution approach*, *ivi*, 2020, 127 ss.

<sup>40</sup> In tal senso mi sono espresso in *Social media, segni distintivi e lealtà della concorrenza, tra influencers, trend setters, fake news e pubblicità*, in *Diritto ind.*, 2019, 122 ss.

**Pasquale Stanzione**

**Verso la società della simulazione?  
Il metaverso e le sue sfide**

Le nuove tecnologie hanno mutato in maniera incisiva le coordinate fondamentali su cui si articola il rapporto tra l'uomo e il mondo, innovando gli stessi concetti di spazio e tempo, forme e contenuti delle relazioni sociali e, con esse, delle categorie giuridiche come del rapporto tra poteri. È mutata profondamente la stessa antropologia, con implicazioni ancora da sviluppare e comprendere fino in fondo.

Una delle più rilevanti di esse è, verosimilmente, destinata ad essere il metaverso: l'evoluzione di internet più prossima e, verosimilmente, più direttamente negli effetti sulla persona e sulla società. Il termine è ripreso dal romanzo cyberpunk *Snow Crash* con cui Neal Stephenson, nel 1992, raccontava di una realtà distopica dominata da un meta-capitalismo con esiti anarchici, in cui l'esercizio del potere fosse delegato alle multinazionali, giunte quasi a soverchiare la funzione sociale e pubblica degli ordinamenti statuali. Il ruolo sociale di ciascuno è, nel romanzo, definito dal proprio avatar, cui affidare il privilegio del riscatto da una vita stretta tra difficoltà e insoddisfazioni (il protagonista è un fattorino di *CosaNostraPizza*), con un'esistenza immaginifica proiettata nel virtuale. La dimensione in cui si muove il "gemello digitale" di ciascuno è dunque, in *Snow Crash*, tanto più utopica quanto più è distopica la realtà che lo circonda, con un tessuto sociale lacerato, uno Stato latitante e poteri privati selvaggi. Come anche nel film *Ready player one*, emerge la suggestione dell'altrove virtuale concepito come dai contorni utopici, in cui proiettare, sublimandola, l'esigenza di riscatto da un quotidiano quasi distopico. Come ne *La vita è altrove* di Milan Kundera, il mondo sostitutivo – lì fatto di versi – offre la possibilità di una seconda vita che sublimi le miserie di quella reale, tra le quali il fatto "*che la gente abbia disimparato la libertà*".

E pur nella sua iperbolicità, la narrazione visionaria di Stephenson anti-

cipava molti degli aspetti (e dei rischi) del capitalismo delle piattaforme che si sarebbero delineati negli anni a venire: la *gig economy* con il pericolo di un caporalato dell'algoritmo, la progressiva affermazione dei poteri privati, la traslazione della vita nella dimensione digitale.

È significativo che il neologismo con cui Stephenson indica la realtà virtuale in cui, tra le Second Life degli avatar, dilaga un virus informatico capace di penetrare anche il cervello degli hacker, sia stato ripreso da Mark Zuckerberg per individuare, già nel 2021, la "*prossima frontiera nel connettere le persone*", in cui l'utente non si limita a "*vedere*" ma finisce con l'*essere* il contenuto e non soltanto un cursore sullo schermo.

Si tratterà di una dimensione (articolata anche su plurime piattaforme) caratterizzata da un'interattività persistente, tridimensionale e dunque ancor più credibile, ubiqua e trasversale, in cui è possibile agire e interagire mediante ologrammi che costituiscono veri e propri tramiti digitali del sé. La definizione di virtuale, per questo nuovo spazio, accentuerà ancor più il suo significato etimologico di potenziale, di possibilità suscettibile di realizzazione. Così come il prefisso Meta, non a caso ripreso da Menlo Park nel suo rebranding (simboleggiato dall'emblema dell'infinito), indica l'oltre, la dimensione cui tendere nel superamento di un limite, identificabile e spesso identificato nella fisicità del reale. Nella misura in cui apparirà come sempre più verosimile, capace di simulare la realtà fin quasi a sostituirla, questa nuova dimensione (non solo spazio-temporale, ma addirittura esperienziale e, quindi, esistenziale) potrà finire per rappresentare, almeno per molti, il luogo delle infinite possibilità, in cui affrancarsi anche, forse, dall'immane concretezza del reale. E forse non se ne percepirà fino in fondo la natura atopica, di vero e proprio non luogo, nell'accezione di Marc Augè: spazio destinato al transito effimero e non all'appartenenza, avulso da strutture sociali e quindi da relazioni intorno a cui costruire un radicamento.

Certamente, quest'universo multisensoriale a confini mobili, con ambiti suscettibili di coprire ogni settore della vita, spaziando dal lavoro al commercio all'intrattenimento, riproporrà, ma con valenza esponenziale, opportunità ma anche rischi e problematiche emersi con l'internet "tradizionale". Quest'esperienza immersiva e potenzialmente totalizzante, iperreale nell'accezione di Baudrillard, rappresenterà il crocevia tra alcune delle neotecnologie più rilevanti del contesto in cui viviamo: a.i., dispositivi indossabili, realtà aumentata, big data, robotica avanzata, cloud computing. E se l'esito sarà un netto cambio di prospettiva non è soltanto per il principio hegeliano secondo cui mutamenti anche solo quantitativi possano risolversi persino, se particolarmente rilevanti, in distinzioni qualitative.

Non sono chiari i contorni che assumerà il metaverso né quali di queste caratteristiche possiederà. Non sappiamo se la sua struttura sarà centralizzata o policentrica, unitaria o multipolare (un pluriverso?), né quale modello di *governance* la ispirerà. Il futuro è ancora tutto da scrivere. Ma sappiamo che, pur nella varietà delle forme che dovesse assumere, il metaverso avrà alcune implicazioni importanti su almeno tre aspetti.

Anzitutto, la trasversalità e molteplicità delle esperienze suscettibili di realizzazione e il volume delle informazioni che potranno generarsi nel metaverso determineranno una raccolta di dati personali non comparabile con quella del web, per quantità ma anche per qualità. Vi saranno, infatti, compresi anche dati biometrici veicolati, tra gli altri, da dispositivi indossabili, di cui va impedito ogni utilizzo abusivo. La rilevanza qualitativa e quantitativa dei flussi di dati indurrà a ripensare *by design* il sistema di raccolta del consenso e le garanzie di trasparenza negli obblighi informativi. Anche in ragione del notevole tasso d'interazione tra gli utenti e della conseguente esigenza di proteggere i minori da esperienze pregiudizievoli, sarà determinante la garanzia *dell'age verification*. Dirimente sarà anche la tenuta delle garanzie (previste ora dal Gdpr, a breve dall'Artificial Intelligence Act) rispetto alle decisioni algoritmiche e alle interazioni tra uomo e macchine che simulino il comportamento umano (si pensi agli assistenti virtuali), di cui si dovrà assicurare la trasparenza e la consapevole gestione.

L'impostazione tecnologicamente neutra (e per ciò *future-proof*) del Gdpr potrà fornire una regolazione tendenzialmente completa sui principali aspetti di questo mondo nuovo, soprattutto grazie all'approccio basato sul rischio, determinante per modulare le tutele sulle caratteristiche di una realtà in continua evoluzione. Ma la personalizzazione dei contenuti propria del metaverso lascerà emergere, verosimilmente, nuove istanze di tutela, a fronte di nuove vulnerabilità e persino nuove soggettività, come quella del gemello digitale in cui si proietterà il nostro io.

E si pensi a categorie di dati del tutto peculiari, come quelli "relazionali", inferiti dalle interazioni on-line, suscettibili di esprimere stati emotivi, cui dovrà accordarsi una tutela proporzionata al grado di intimità rivelabile. La creatività digitale mostrerà l'urgenza di delineare un confine tra *data-economy* (fondata sempre più sulla deduzione dei dati nel sinallagma negoziale) e monetizzazione della privacy, con tutti i rischi, in termini di libertà ed eguaglianza, suscettibili di derivarne.

Quanto più l'esperienza, immersiva e totalizzante, di questa vita "altra" sia mediata dai contenuti proposti dagli algoritmi, tanto più si dovrà garantire la libertà del singolo dal condizionamento esercitato dal pedinamento

digitale. Il metaverso potrebbe amplificare esponenzialmente il *nudging* su cui si fonda il sistema delle bolle di filtri, che induce omologazione e intolleranza verso le minoranze ed ogni soggettività espressiva di differenza, con conseguente polarizzazione sociale.

Il rischio è che la libertà di dare forma al proprio mondo, promessa dal metaverso, sia solo apparente e nasconda, invece, un'eterodirezione delle scelte indotta dal microtargeting, i cui effetti distorsivi sulla formazione dell'opinione individuale e pubblica sono ben espressi dal caso Cambridge Analytica. In assenza di correttivi adeguati, la capacità di orientamento propria della selezione dei contenuti proposta dagli algoritmi rischia infatti di divenire, in un'esperienza virtuale così pervasiva, una vera e propria egemonia culturale in senso gramsciano.

L'accrescimento del potere– informativo e persino performativo– delle piattaforme, che accompagnerà lo sviluppo del metaverso imporrà scelte lungimiranti sotto il profilo della *governance*. E quale che sia il modello cui si orienterà lo sviluppo del metaverso, è indispensabile l'adozione di alcune garanzie essenziali, volte a impedire che questa dimensione altra, da spazio utopico del possibile, degeneri in un luogo anomico dove impunemente violare diritti. Lo suggerisce lo stesso esordio di Horizon World, caratterizzato per una vera e propria violenza sessuale di gruppo in danno di una ricercatrice, tramite il suo avatar. La smaterializzazione dello spazio e delle relazioni, la trasfigurazione della persona in un ologramma, la verosimile diffusione dei *deep fake* possono, infatti, ridurre la percezione del disvalore (reale!) degli illeciti commessi nella dimensione virtuale.

Ma le garanzie da accordare nel metaverso dovranno estendersi anche agli effetti più profondi e a lungo termine suscettibili di derivare da quella che può divenire una vera e propria società della simulazione, fondata su interazioni senza contatto, con una sua specifica antropologia,. Significativo, in questo senso, l'impatto psicologico, anche in termini di akrasia e alienazione sociale che può avere, soprattutto sui giovani, l'esperienza immersiva della vita in una dimensione altra, costruita, con una sorta di autoinganno, secondo i nostri desideri e modulata sulle nostre percezioni. Non è azzardato ipotizzare una tendenza al disimpegno dal reale in favore di questo altrove dai contorni onirici. Rilevanti sono inoltre le implicazioni, in termini identitari, della relazione quasi osmotica con il gemello digitale di sé, con un rischio di dipendenza certamente maggiore di quello proprio dei social tradizionali.

Va inoltre considerato l'impatto che potrà avere la (già progettata) sostituzione dei visori con un'interfaccia neurale, capace di proiettare questo

mondo virtuale direttamente nel cervello, ovvero nella regione del corpo più delicata perché irriducibile a mera biologia, quale correlato neurale della coscienza. E questo, in contesto in cui le neurotecnologie potrebbero, in un futuro non lontano, leggere i pensieri, decodificando i dati neurali con sistemi di *brain reading*. L'ingresso della tecnica in *quell'inner world* in cui neppure il più coercitivo dei poteri si era spinto, non può che suscitare, dunque, nuove istanze di tutela. Anzitutto di quel foro interno (l'Io sovrano, per dirla con Musil) dalla cui libera formazione dipende ogni altra libertà, se non si vuole che innovazioni potenzialmente utili divengano lo strumento per fare dell'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere.

La protezione dei dati ha oggi anche il compito di impedire questa deriva riduzionista, per promuovere un'innovazione sostenibile e non democraticamente regressiva, tanto più a fronte di uno scenario così inesplorato, ma non per questo necessariamente da temere, come quello dischiuso dal metaverso.



## Gustavo Ghidini

### Di diverso avviso

La dimensione globale del fenomeno del potere delle grandi piattaforme digitali impone al giurista che si occupa di concorrenza, di allargare la visione comparatista oltre l'abituale confronto USA-Europa. Oggi c'è la Cina, la prima concorrente degli USA, che sta sviluppando una normativa e una giurisprudenza di estremo interesse comparatistico sia per quanto riguarda il controllo delle sue big tech (da ultimo, anche a proposito di oneri di trasparenza degli algoritmi) sia per quanto riguarda la promozione del digitale e in particolare della AI, rispetto alla cui tutela di PI ha superato realisticamente lo pseudo problema della 'mano umana' come inventore o autore. Che è quella (v. la sentenza *Tencent* del novembre 2019) degli ingegneri di software che hanno creato l'algoritmo in vista di un fine utilitaristico e hanno immesso i dati su cui lavorare ed elaborare.

La prospettiva di interventi normativi vede le convergenze parallele di due linee: promozione dello sviluppo tecnologico, e disciplina delle sue espressioni ed effetti sull'individui e la comunità.

In particolare, l'Europa (modello di capacità di regolare, meno di investire) esprime un complesso disegno regolatorio, iniziato con il GDPR e proseguito con il Digital package su cui ci siamo intrattenuti. Un disegno non certo penalizzante delle imprese bensì volto ad assicurare uno sviluppo ben temperato: e come tale anche più solido e duraturo, in quanto capace di attirare la fiducia di cittadini che si sentano protetti nei loro supremi interessi alla libertà, dignità, sicurezza. Valori non "europei": universali.

Il disegno europeo affronta il tema del contenimento del potere dei web titans in una chiave soprattutto di interventi di tipo comportamentale. Una chiave che affianca la regolazione-per tutti: gli obblighi dei *gatekeepers* – all'antitrust – per tutti: gli abusi self preferencing.

Tutto ciò per affermare, in breve, che rispetto a questi nuovi scenari l'At deve allearsi con una regolazione che può dirsi di sostegno, come quella che l'Europa si è data e si sta dando con DMA, e a breve DSA e regolamento AI, ecc.

Al contempo, l'AT potrebbe osare di più, ad esempio frenando su futuri allargamenti polipoidi dei giganti- che errore clamoroso autorizzare l'ingestione di Instagram e Whatsapp! e l'ingresso di Amazon nel mercato della salute. E forse si potrebbe prendere in considerazione la proposta di Gal e Petit di attuare dei temporanei shut down, forme cioè di sospensione di attività, come qualche volta avviene per discoteche in cui circola troppa polvere bianca. Questa prospettiva potrebbe affiancarsi, sul piano della sanzione di abusi, alle prescrizioni di doveri di condotta. Ma certo non si incide in profondo sul potere dei big tech.

Qui, il nodo riguarda possibili rimedi c.d. strutturali. Prima di evocarli nell'attualità, lasciatemi ricordare un precedente normativo, 'legge Maccanico', istitutiva dell'AGCOM, legge alla cui stesura ebbi il privilegio di collaborare come uno dei consiglieri giuridici del compianto Ministro delle PPTT.

Venendo all'oggi, i rimedi di stampo 'strutturale' (separazioni societarie di gruppi) sono evocati come *extrema ratio* – il che è condivisibile – in modo ambiguo dall'UE (v considerando 64 DMA con la bertoldesca condizione che ripetute violazioni di obblighi siano ascrivibili alla struttura stessa dell'impresa: sic)

Roberto Sommella ha fatto da confessore a Margaret Vestager in una brillante recente intervista a MF. La Commissaria ha liquidato in sostanza la prospettiva di break up come farraginoso e controproducente.

Qui si apre un interessante spunto di confronto con USA, ove gli iniziali bollenti spiriti e giovanili ardori della nuova Chair della FTC, Lina Kahn, nominata dal presidente Biden, e che agita esplicitamente lo spauracchio di divestitures dei big tech sono stati raffreddati dal silenzio eloquente dello stesso Presidente il quale nell'emanare nel luglio del 21 un Executive Act su *Competition in America*, pur col riconoscimento – labiale – di rischi per la democrazia del potere dei big tech, si guarda bene dal citare, sia pure per allusione evocativa, ai rimedi strutturali.

Queste notazioni ci introducono alla nuova frontiera, che sinora è rimasta fuori – e comunque ai margini, con segnali debolissimi – dal radar eu-

ropeo che ancora interpella insieme AT e regolazione.

Quella del grande potere delle piattaforme è questione che specie in USA vede voci autorevoli e plurali-politiche, accademiche, scientifiche, affermare che rispetto al potere delle grandi piattaforme gatekeepers dei flussi di informazione e dati-potere accresciuto dall'assetto spiccatamente oligopolistico del relativo 'mercato' – gli strumenti dell'AT da soli non bastano. Non bastano né ad evitare distorsioni dei mercati bensì anche di distorsioni della democrazia – come ha scritto recentemente F. Fukujama su *Foreign Affairs*, e come un quarto di secolo fa Giuliano Amato (*Il potere e l'antitrust*) ricordava quando distingueva, rispetto al potere concentrato, fra efficienza economica ed efficienza democratica.

La comprensione in profondità di questi atteggiamenti deve spingersi al di là di tecnicismi e categorie tradizionali. L'Europa, stretta tra USA e Cina, non vuole intralciare la crescita di campioni nazionali europei: come fece negli anni '60-'70 – penso al memorandum Colonna – rimandando, per due decenni il controllo delle concentrazioni.

Per gli USA, probabilmente la ragione è quella di non ostacolare la ulteriore crescita dei propri campioni nazionali, impegnati a confrontarsi con i colossi cinesi. E così, con questi chiari di luna europei ed USA, mi vien da pensare, da vecchio socialista, che il sol dell'avvenire lo vedranno sorgere i nipoti. Io ne ho tre: in bocca al lupo.



## Gli Autori

**Valeria Falce**, Jean Monnet Professor in Digital Transformation and AI Policy e Ordinario di Diritto dell'Economia nell'Università Europea di Roma

\* \* \*

**Emanuela Arezzo**, Associato di Diritto Commerciale nell'Università degli studi di Teramo

**Maria Letizia Bixio**, Ricercatore (a tempo determinato) di Diritto dell'Economia nell'Università Europea di Roma

**Roberto Bocchini**, Ordinario di Istituzioni di Diritto Privato nell'Università degli Studi "Parthenope" di Napoli

**Francesco Di Ciommo**, Ordinario di Diritto Privato nell'Università LUISS Guido Carli

**Filippo Donati**, Ordinario di Diritto Costituzionale nell'Università di Firenze

**Nicola N.M. Faraone**, Assegnista di ricerca in Diritto dell'Economia nell'Università Europea di Roma

**Tommaso Edoardo Frosini**, Ordinario di Diritto Pubblico Comparato nell'Università "Suor Orsola Benincasa" di Napoli

**Cesare Galli**, Ordinario di Diritto Commerciale nell'Università di Parma

**Alberto Maria Gambino**, Ordinario di Diritto Privato e Prorettore Vicario nell'Università degli Studi Europea di Roma

**Anna Genovese**, Ordinario di Diritto Commerciale nell'Università di Verona

**Gustavo Ghidini**, Emerito di Diritto Industriale nell'Università degli Studi di Milano e Senior Professor nell'Università LUISS Guido Carli

**Silvia Giudici**, Associato di Diritto Commerciale nell'Università degli Studi di Milano

**Marco Macchia**, Professore Associato di Diritto Amministrativo presso l'Università degli studi di Roma "Tor Vergata"

**Massimo Proverbio**, Chief IT, Digital and Innovation Officer, Intesa Sanpaolo

**Cristina Schepisi**, Ordinario di Diritto dell'Unione Europea nell'Università degli Studi "Parthenope" di Napoli

**Maria Antonietta Scopelliti**, Segretario Generale e Responsabile della Protezione dati Privacy della Commissione Nazionale per le Società e la Borsa (CONSOB)

**Pasquale Stanzone**, Presidente del Garante per la protezione dei dati personali

**Guido Stazi**, Segretario Generale dell'Autorità Garante della Concorrenza e del Mercato



Finito di stampare nel mese di aprile 2023  
nella Stampatre s.r.l. di Torino – Via Bologna 220



UNIVERSITÀ EUROPEA DI ROMA

---

*Volumi pubblicati*

Sezione Giuridica – MANUALI

1. A.M. GAMBINO-A. STAZI-D. MULA, *Diritto dell'informatica e della comunicazione. Terza edizione*, 2019, pp. XVI-288.

Sezione Giuridica – SAGGI

1. A. MERONE, *Il tribunale arbitrale dello sport*, 2009, pp. X-266.
2. F. TESTA, *La funzione negoziale nell'azione sindacale. Seconda edizione. Contributo per una teoria unificante del riconoscimento giuridico dell'azione sindacale*, 2010, pp. XVI-228.
3. P. RIVELLO, *Il processo penale di fronte alle problematiche dell'età contemporanea. Logiche processuali e paradigmi scientifici*, 2010, pp. VIII-188.
4. V. FALCE, *La modernizzazione del diritto d'autore. Seconda edizione*, 2012, pp. VI-274.
5. T. SCANDROGLIO, *La Teoria Neoclassica sulla legge naturale di Germain Grisez e John Finnis*, 2012, pp. XII-516.
6. F. TESTA, *Il diritto alle ferie del lavoratore subordinato*, 2012, pp. XVIII-142.
7. E. BILOTTI, *Separazione dei beni del defunto e tutela dei creditori*, 2012, pp. X-222.
8. F. SANTAGADA, *La mediazione*, 2012, pp. X-190.
9. M. PALMARO, *Eutanasia: diritto o delitto? Il conflitto tra i principi di autonomia e di indisponibilità della vita umana*, 2012, pp. XII-116.
10. A. STAZI, *Innovazioni biotecnologiche e brevettabilità del vivente. Questioni giuridiche e profili bioetici nei modelli statunitense ed europeo*, 2012, pp. X-302.
11. I. GARACI, *Nuovi beni e tutela della persona. Lo sfruttamento commerciale della notorietà*, 2012, pp. XIV-106.
12. C. LONGARI, *Le cause di estinzione del reato*, 2012, pp. XIV-218.

13. G. NAVA, *Regolamentazione e contenzioso tra operatori nelle comunicazioni elettroniche*, 2012, pp. VIII-224.
14. E. PROSPERETTI, *L'opera digitale tra regole e mercato*, 2013, pp. VIII-280.
15. F. TOZZI, *La circolazione dei diritti della persona*, 2013, pp. X-214.
16. F. VARI, *L'affermazione del principio d'eguaglianza nei rapporti tra privati. Profili costituzionali*. Seconda edizione, 2016, pp. X-142.
17. W. WALDSTEIN, *Scritto nel cuore. Il diritto naturale come fondamento di una società umana*, traduzione italiana a cura di Filippo Vari, 2014, pp. XIV-146.
18. V. OCCORSIO, *La clientela professionale come bene giuridico*, 2016, pp. VIII-240.
19. A. MERONE, *Il disconoscimento delle prove documentali*, 2018, pp. XXIV-328.
20. A. STAZI, *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto comparato*, 2019, pp. XII-196.
21. M.L. BIXIO, *Modelli di gestione collettiva a tutela dei diritti d'autore. Itinerari tra dinamiche concorrenziali ed interferenze di diritto sovranazionale*, 2020, pp. XX-260.

#### Sezione Giuridica – MATERIALI

1. *Codice civile applicato. Casi scelti a cura di A.M. GAMBINO-E. BILOTTI-E. SQUINTANI*, 2011, pp. VIII-284.
2. F. DONATO-SEMINARA, *La speciale disciplina delle banche popolari cooperative*, 2011, pp. VIII-224.
3. *Rimedi e tecniche di protezione del consumatore a cura di A.M. GAMBINO*, 2011, pp. X-450.
4. F. VARI, *La fecondazione eterologa tra costituzione italiana e convenzione europea dei diritti dell'uomo*, 2012, pp. VIII-194.
5. V. FALCE, *Fairness e innovazione nel mercato digitale*, 2020, pp. XIV-210.
6. V. FALCE (a cura di), *Financial Innovation tra disintermediazione e mercato*, 2021, pp. XXVIII-212.
7. V. FALCE (a cura di), *Digital Markets and Competition Law*, 2021, pp. XVIII-334.

8. V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, 2023, pp. XIV-322.

Sezione Economica – SAGGI

1. M. PEDRANA, *Le dimensioni del capitale sociale. Un'analisi a livello regionale*, 2012, pp. XIV-178.

Sezione Economica – MATERIALI

1. A. NUZZI, *Towards year 2010. Issues in European Transport Policy - Railways and Motorways*, 2009, pp. XVI-224.

Sezione Umanistica – SAGGI

1. P. SCARAFONI, *Il Dio presente*, 2013, pp. XII-300.

