DECA
12
COLLANA DEL DIPARTIMENTO DI ECONOMIA AZIENDALE

A cura di
FABIO BASSAN

L'APPLICAZIONE DELL'AI ACT IN ITALIA E LA TUTELA DEL CONSUMATORE

Il ruolo delle autorità indipendenti

RomaTrE-Press
2026

Roma Tre
Università degli Studi Roma Tre
Dipartimento di Economia aziendale

DECA Collana del Dipartimento di Economia Aziendale

1 *Analisi di bilancio. Un percorso di sintesi*
Marco Tutino

2 *Sindacati in un mondo globale*
Giampiero Bianchi

3 *Ideazione, sviluppo e marketing dei nuovi prodotti*
Carlo A. Pratesi, Andrea Geremicca

4 *Studi e ricerche del Dipartimento di Economia Aziendale 2023*
a cura di Alberto Pezzi

5 *Il consumatore: responsabile, attivo, partecipativo*
a cura di Fabio Bassan, Maddalena Rabitti

6 *Profili ragionieristici della contabilità nazionale*
Claudio Columbano

7 *Investment advice and sustainability. A survey on professional-client interactions*
Paola Soccorso, Massimo Caratelli

8 *Studi e ricerche del Dipartimento di Economia Aziendale 2024*
a cura di Alberto Pezzi

9 *Qualità, Innovazione e Sostenibilità nella filiera agro-alimentare*
a cura di Maria Claudia Lucchetti, Maria Francesca Renzi

10 *L'applicazione dell'AI Act in Italia e la tutela del consumatore*
a cura di Maddalena Rabitti, Fabio Bassan

11 *Marketing e innovazione*
Carlo Alberto Pratesi

Università degli Studi Roma Tre
Dipartimento di Economia Aziendale

12

COLLANA DEL DIPARTIMENTO
DI ECONOMIA AZIENDALE

L'APPLICAZIONE DELL'AI ACT IN ITALIA E LA TUTELA DEL CONSUMATORE

Il ruolo delle autorità indipendenti

A cura di
FABIO BASSAN

RomaTrE-Press
2026

Collana del Dipartimento di Economia Aziendale
Direttore
Alberto Pezzi

Coordinamento editoriale
Gruppo di Lavoro Roma TrE-Press

Impaginazione e cura editoriale
teseo editore Roma teseoeditore.it

Elaborazione grafica della copertina
MOSQUITO. mosquitoroma.it

Edizioni Roma TrE-Press ©
Roma, giugno 2026
ISBN: 979-12-5977-640-2

http://romatrepress.uniroma3.it

L'attività della Roma TrE-Press è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma.

IL PROGETTO ROMA TRE-PRESS

Il progetto della Roma TrE-Press nasce nel 2013 ed inizia la sua attività all'interno del Sistema Bibliotecario di Ateneo.

Vengono avviate le prime Collane e Riviste di Ateneo. Fin dall'inizio il progetto ha scelto la strada dell'open access: opere scientifiche realizzate in formato digitale ed accessibili a chiunque, dovunque, sempre.

Le ragioni sono le stesse che spingono altre università europee: la ricerca accademica è finanziata da risorse pubbliche; occorre che i suoi risultati siano accessibili a tutti, senza onerose intermediazioni; ciò è reso possibile dalle tecnologie digitali; rientra nella "terza missione" delle università diffondere al pubblico più largo i suoi prodotti sia didattici che scientifici; ma è anche un'esigenza di contenimento dei costi dettata dalle crescenti ristrettezze di bilancio.

Nel primo quinquennio (2013/2017) la Roma TrE-Press pubblica quasi 100 volumi. La crescente richiesta dei ricercatori dell'Ateneo e il successo dell'iniziativa (oltre 150.000 downloads) suggeriscono agli organi di Ateneo di affidare, a partire dall'autunno 2018, l'attività di e-press alla Fondazione Roma Tre Education.

Le linee guida della Roma TrE-Press sono:

• La piena autonomia scientifica dei Dipartimenti e dei Centri di Ateneo nella scelta di che cosa pubblicare, con un forte incoraggiamento verso procedure di assicurazione della qualità secondo le migliori prassi recepite dalle comunità scientifiche di riferimento.

• L'apertura verso autori e istituzioni non appartenenti all'Università Roma Tre, secondo logiche di aggregazione e di promozione della ricerca di qualità.

• Il plurilinguismo, non solo come esigenza culturale ma anche come strumento di coesione e collaborazione internazionale.

• La cura – affidata alla responsabilità della Roma TrE-Press – della linea grafica (copertine e impaginazione), secondo la secolare tradizione del libro come prodotto anche estetico ed artistico.

• La promozione del movimento verso una generale politica di open access che coinvolga anche altre istituzioni accademiche italiane e straniere in coerenza con il dettato dell'art. 9 della nostra Costituzione: "*La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica*".

La squadra della Roma Tre-Press è così composta

prof. Vincenzo Zeno-Zencovich (*Delegato di Ateneo per l'e-press*)

prof.ssa Nazarena Patrizi (*Responsabile editoriale*)

prof. Sirio Zolea (*Delegato per i rapporti internazionali*)

dott. Ivan Guiducci (*Webmaster*)

Alessandro Riboldi (*Collaboratore informatico*)

Università degli Studi Roma Tre
Dipartimento di Economia Aziendale
Codice etico delle Colane edite da Roma Tre Press

Il Dipartimento di Economia Aziendale per le collane edite da Roma TrE-Press si impegna a garantire standard di comportamento etico in ogni fase del processo editoriale, ispirandosi alle linee guida del **Committee on Publication Ethics (COPE)**.

1. Doveri degli Autori

- **Originalità e Proprietà Intellettuale:** gli autori garantiscono che l'opera sia originale e non violi i diritti di proprietà intellettuale di terzi. Devono citare correttamente ogni fonte per evitare il plagio e ottenere i permessi per riprodurre contenuti protetti da copyright.
- **Paternità dell'opera:** L'elenco degli autori deve riflettere accuratamente chi ha svolto la ricerca. In caso di paternità multipla, l'ordine dei nomi è determinato congiuntamente dai coautori.
- **Uso dell'Intelligenza Artificiale (IA):** gli strumenti di IA non possono essere indicati come autori o co-autori.
  - È consentito l'uso di IA esclusivamente per finalità di supporto tecnico (es. traduzione, miglioramento della fluidità linguistica, correzione grammaticale e rielaborazione stilistica).
  - È vietato l'uso di IA per la generazione di contenuti scientifici originali, interpretazione di dati o formulazione di conclusioni.
  - Gli autori devono dichiarare esplicitamente nel manoscritto (es. in una nota o nei ringraziamenti) l'impiego di tali strumenti, specificandone il modello e le finalità. L'autore umano resta l'unico responsabile dell'accuratezza e dell'integrità del lavoro.
- **Esclusività:** I manoscritti non devono essere inviati contemporaneamente ad altri editori.
- **Finanziamenti e Conflitti di Interesse:** Eventuali fonti di finanziamento della ricerca e conflitti di interesse devono essere chiaramente identificati nel manoscritto.

2. Doveri del Direttore e dei Comitati (Scientifico ed Editoriale)

- **Imparzialità ed Equità:** Le decisioni si basano esclusivamente sulla qualità scientifica e l'idoneità del lavoro per la Collana, senza discriminazioni di alcun tipo.
- **Trasparenza del Processo:** Il Comitato Editoriale supervisiona il referaggio garantendo l'anonimato tra autori e revisori.
- **Gestione dei Conflitti d'Interesse:** In caso di contributi proposti da membri del Comitato Editoriale, la gestione della pratica è affidata esclusivamente al Direttore per garantire l'assoluta terzietà.
- **Riservatezza:** Tutto il materiale ricevuto deve essere trattato come riservato fino alla pubblicazione.

3. Doveri dei Revisori (Referee)

- **Oggettività e Qualità:** I revisori devono valutare il materiale con cura e obiettività, fornendo feedback costruttivi in modo tempestivo.
- **Conflitto di Interessi e Riservatezza:** I revisori devono segnalare immediatamente qualsiasi conflitto di interessi. Non possono utilizzare per fini personali le informazioni contenute nei manoscritti né generare il report caricando i lavori su piattaforme di IA generativa.
- **Segnalazione di Irregolarità:** I revisori sono tenuti a informare il Direttore in caso di sospetto plagio o somiglianze eccessive con opere già edite. Il Direttore e il Comitato Editoriale avviano un'indagine interna. Qualora l'indagine confermi comportamenti scorretti, la Collana provvederà al ritiro dell'opera dalla piattaforma Roma TrE-Press o alla pubblicazione di una errata corrige ufficiale.

Collana del Dipartimento di Economia Aziendale

Editorial Policy e descrizione dello scopo della Collana

La collana nasce con lo scopo di contribuire allo sviluppo e alla diffusione delle tematiche di gestione d'impresa: economico-aziendali, finanziarie, giuridiche e matematiche, valorizzando il pluralismo culturale e l'interdisciplinarietà presenti nel Dipartimento.

La collana è aperta a contributi che supportino il miglioramento della didattica dei corsi di studio universitari e post-universitari e favoriscano il dibattito tra il modo delle imprese e il mondo accademico.

La collana accoglie contributi monografici e collettanee.

I volumi pubblicati nella collana sono sottoposti a referaggio affidato al Comitato editoriale.

I volumi pubblicati dalla collana sono liberamente accessibili in formato elettronico sul sito dell'editore Roma TrE-Press. La versione a stampa è acquistabile in modalità "Print on demand".

Le pubblicazioni hanno una numerazione progressiva ed eventuali richiami o citazioni ad essi devono riportare la denominazione estesa del contributo a cui si fa riferimento.

AUTORI

Fabio BASSAN
Professore ordinario di Diritto internazionale e componente del Collegio dei docenti del dottorato di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre.

Marco CAPPAI
Dottore di ricerca in «Mercati, impresa e consumatori» e assegnista di ricerca in Diritto amministrativo presso l'Università degli Studi Roma Tre. Abilitato alle funzioni di professore universitario di seconda fascia nel settore concorsuale di Diritto amministrativo.

Armando DI CELLO
Dottorando di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre.

Matteo GHEZZI
Dottorando di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre.

Cristiana LAURI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Ricercatrice presso l'Università di Macerata, abilitata alle funzioni di professore universitario di seconda fascia nel settore concorsuale di Diritto amministrativo.

Michela MASTRANTONIO
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Avvocato. Funzionario presso l'Autorità per le garanzie nelle comunicazioni.

Federico NESPEGA
Dottorando di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Avvocato del Foro di Roma.

Paolo OCCHIUZZI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionario dell'Autorità garante della concorrenza e del mercato.

Vincenzo ORSINI
Dottore di ricerca in «Economia e politiche dei mercati e delle imprese». Docente a contratto in Diritto dell'economia presso l'Università degli Studi di Salerno.

Francesca PELLICANÓ
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionario di ruolo dell'Autorità per le garanzie nelle comunicazioni.

Sara PERUGINI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionario dell'Autorità garante della concorrenza e del mercato.

Rosaria PETTI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionario di ruolo presso l'Autorità per le garanzie nelle comunicazioni e avvocato.

Serafina PIANTEDOSI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionario presso l'Autorità nazionale anticorruzione e avvocato.

Aurora SAIJA
Dirigente presso Assonime, Area Diritto societario e impresa.

Piattaforme digitali e consumatori.
Il ruolo delle autorità indipendenti

Indice

Piattaforme digitali e consumatori. Il ruolo delle autorità indipendenti

Fabio Bassan

Il fenomeno delle piattaforme digitali ha modificato in modo dirompente e ormai definitivo la realtà in cui gli individui vivono, le aziende producono, gli stati si relazionano tra loro. Le piattaforme caratterizzano la nostra epoca, che possiamo classificare come un'era ibrida, poiché l'esperienza umana è integrata – a volta aumentata ma comunque influenzata - dalla macchina, che produce spesso, via intelligenza artificiale, un'esperienza autonoma, con la quale quella umana si confronta, si arricchisce o soccombe.

Le piattaforme digitali dominano il Web2, ovvero l'evoluzione di internet, passata da un ambiente iniziale punto-multipunto (le notizie di informazione, i blog individuali: il Web1) a un ambiente caratterizzato da 'orchestratori' che ne condizionano l'accesso (i social networks, tipicamen-te) o ne orientano i flussi (le piattaforme di commercio, quando 'aperte', non soggette a iscrizione): il Web2. I modelli di business delle piattaforme, diversi in ragione delle caratteristiche di ciascuna, si fondano tutti sulla gestione di una gran mole di dati, non sempre anonimizzati, che consentono procedure di profilazione individuale che incidono sulle scelte degli individui, siano questi elettori o consumatori. Gli strumenti ormai sofisticati di rilevazione hanno condotto a risultati sorprendenti, quali l'annullamento di elezioni politiche nazionali (in Romania) in ragione dell'indebita influenza sugli elettori, o a sanzioni economiche molto rilevanti, imposte dalle autorità di vigilanza in ragione dell'uso distorto o illecito dei dati raccolti dalle piattaforme.

Queste evidenze producono modelli di vigilanza e regolazione divergenti nelle varie aree di influenza, e dunque, limitandoci alle tre principali, nell'Unione europea, negli Stati Uniti e in Cina. Mentre gli Stati Uniti proseguono decisi nella tradizione consolidata di un intervento minimo sui mercati e di utilizzo delle imprese private per finalità pubbliche (ad esempio, consolidare la primazia del dollaro sui mercati internazionali), l'Unione europea e la Cina seguono un percorso di regolazione, con modelli diversi ma coerenti tra loro, a dimostrazione del fatto da un lato, che il 'Brussels' effect' teorizzato da Anu Bradford opera in modo efficace, e dall'altro, che il modello europeo funziona indipendentemente dal coefficiente democra-

tico del paese che lo applica, e può servire sia per garantire lo stato di diritto, secondo una rule of law fondata non più sulla separazione dei poteri ma sulla garanzia dell'*enforcement*, sia per offrire – sempre via *enforcement* – un controllo ancora più sistematico e infallibile da parte di chi esercita un monopolio politico. Si tratta di un precipitato inquietante ma non imprevisto, se si considera che il driver delle piattaforme digitali è la tecnologia, neutra per definizione, mentre non è mai neutro l'uso che se ne fa.

Le stesse impostazioni nelle tre aree di influenza si riproducono nel Web3, termine che semplifica l'evoluzione della blockchain, sovrastruttura di internet con caratteristiche idonee a consentire un ulteriore sviluppo, soprattutto in tema di sicurezza e certificazione dei pagamenti, potenzialmente idoneo a disintermediare l'inefficienza, mantenendo nella catena solo gli intermediari che creano valore. I temi che pongono le evoluzioni Web3 rilevano anche ai fini delle politiche internazionali, in quanto mettono in discussione i presupposti fondamentali dell'effettività della sovranità statale, dal controllo del territorio all'emissione della moneta.

E dunque, l'evoluzione nel Web3 delle piattaforme digitali le trasforma, da destinatari delle regole degli stati, a soggetti in grado di negoziare le regole, 'tra pari'. Le piattaforme, infatti, da un lato sono ordinamenti giuridici anch'esse (esercitano il potere normativo, esecutivo e para-giurisdizionale nei confronti dei propri clienti se piattaforme aperte, o dei propri iscritti, se piattaforme chiuse), e dall'altro sono 'potenze' in grado di confrontarsi e competere con gli Stati a parità di strumenti (la valuta, da ultimo). La novità, dirompente, è che questi soggetti non sono Stati, ma imprese private. Di nuovo: l'ibridazione è il fenomeno che caratterizza anche questa evoluzione, sul piano internazionale e transnazionale.

Precipitato di questo è l'evoluzione del ruolo che ci si aspetta che eserciti il consumatore: mutano rapidamente il grado di conoscenza dei fenomeni, il livello delle tutele preventive sul piano tecnologico ma anche della consapevolezza, nonché delle sanzioni ex post per le violazioni; il tema dell'*enforcement* torna quindi decisivo, quanto alla capacità di monitorare, prevenire e sanzionare gli illeciti.

Web2 e Web3, con l'intelligenza artificiale a cerniera, sono gli ambienti indagati in questo Rapporto Consumerism 2025 che celebra i vent'anni di collaborazione tra il Dipartimento di Economia aziendale di Roma Tre e Consumersforum, dedicati allo studio dell'impatto dell'innova-zione sui consumatori. La metodologia utilizzata resta quella elaborata nel corso di questi anni di ricerca, che guarda alla regolazione con gli strumenti della matrice regolatoria, tra silos verticali (settoriali) e orizzontali (regole generali applicate a tutti i settori), e ne segue l'applicazione secondo il percorso del

circolo regolatorio, in base al quale le regole nascono dal mercato e al mercato tornano, via soft law o hard law secondo necessità.

In questa metodologia il ruolo crescente e l'attività delle autorità indipendenti sono fondamentali, per riempire di contenuti applicativi lo spazio lasciato dalle norme europee, direttive vent'anni fa, sempre più regolamenti oggi, questi ultimi direttamente applicabili ma non sempre self-executing: da qui, la rilevanza della vigilanza e della regolazione di secondo livello, a colmare il vuoto, prima che lo faccia il mercato.

Le autorità nazionali di origine unionale, costituite a partire dagli anni '90 del secolo scorso da direttive e regolamenti con cui il legislatore europeo disintermediava gli stati sui mercati, e sviluppate poi in reti europee di coordinamento, sono divenute oggi il braccio esecutivo della Commissione o delle autorità europee, nelle quali si sta accentrando il potere normativo (di secondo livello) ed esecutivo (delle norme). La narrazione dominante che giustifica questo percorso di accentramento di poteri è stata per molti anni la necessità di rispondere alla globalizzazione con la stessa velocità con cui questa si sviluppava; oggi, che la globalizzazione è regionalizzata di fatto, l'accentramento europeo si giustifica con la necessità di una reazione comune alle piattaforme digitali e agli interessi interni ed esterni che queste rappresentano e perseguono. In alcuni settori (da quello bancario, alle comunicazioni elettroniche quanto ai 'silos verticali', o alla concorrenza, tra i 'silos orizzontali' della matrice) il fenomeno è stato istituzionalizzato; in altri è conseguenza di una prassi applicativa consolidata.

Decisivo diventa allora il coordinamento tra le autorità, e se quello verticale (tra autorità di settore nazionali ed europee) è definito dalle norme europee, quello orizzontale (tra autorità nazionali dei diversi settori) è in parte affidato alla regolazione di secondo livello, che crea spesso lacune e sovrapposizioni. Questo tema è ricorrente nelle nostre ricerche 'Consumerism', e oggi è dirimente, considerato che lo schema a matrice con cui ci siamo orientati negli ultimi vent'anni (con silos verticali e orizzontali) tende di fatto a venire meno. Quando le banche vendono prodotti assicurativi o finanziari la regolazione per soggetti non serve più; dalla regolazione per attività siamo passati a quella per singolo prodotto e poi oggi, alla cross-regulation (V. Colaert e M. Rabitti), che però funziona solo se il coordinamento orizzontale opera in modo sistematico e strutturale. Si rinvia sul punto in questo Rapporto all'intervento di Marco Cappai e Paolo Occhiuzzi.

Il Rapporto Consumerism di quest'anno non è dunque solo la celebrazione di una collaborazione e di un metodo, ma continua ad essere un avamposto di frontiera dello studio delle tutele dei consumatori sui mercati. Le piattaforme sono gli strumenti-veicolo della tecnologia, che non è più

solo abilitatore ma anche strumento, e sono quindi i principali destinatari ma anche i più determinati negoziatori delle norme, europee e nazionali.

Le piattaforme sono destinatarie di regolamenti europei quanto ai comportamenti sui mercati (DMA), perché tenute al rispetto di obblighi crescenti in proporzione alla loro rilevanza, ma anche quanto alle relazioni con i propri clienti/utenti (DSA). Mentre però il DMA accentra sulla Commissione europea i poteri di controllo e intervento a tutela della concorrenza, il DSA affida alle autorità nazionali – non della concorrenza, ma delle comunicazioni – il compito di vigilare sul rispetto delle tutele degli utenti. Compito fondamentale questo, perché trasporta gli strumenti di tutela dei consumatori dall'ordinamento privato, interno, delle piattaforme, che si fonda sul contratto, a quello pubblico, esterno, degli ordinamenti nazionali, che consente alle autorità nazionali interventi di integrazione e modifica dei contratti. Le prime applicazioni di questa disciplina sono oggetto di studio in questo Rapporto, negli interventi di Francesca Pellicanò e Rosaria Petti, e di Sara Perugini.

Le protezioni da forme invasive della tecnologia sul piano dei cyberattacchi, previste dalla disciplina unionale e da quella nazionale, costituiscono una forma ulteriore e complementare di tutela, per i consumatori, le imprese, la pubblica amministrazione. Norme e regole tecniche europee, specificate sul piano nazionale, stabiliscono un perimetro di tutele efficace in funzione della partecipazione delle imprese, chiamate ad approntare strumenti di protezione adeguati, e dei consumatori, chiamati a esercitare un controllo frutto di una consapevolezza crescente stimolata da attività continue e generali di educazione a fini preventivi, delle autorità e delle imprese. I poteri attribuiti all'autorità nazionale, ulteriormente integrati a seguito dell'applicazione del regolamento sull'intelligenza artificiale, cui abbiamo dedicato il Rapporto Consumerism 2024, sono sintetizzati in questo Rapporto da Michela Mastrantonio e misurati in relazione al potere esercitato dalle piattaforme.

Azioni preventive sono lo strumento principale delle tutele anche sui temi degli strumenti e dei mezzi di pagamento, su cui si sta concentrando uno scontro di valori e di impostazioni. Al modello europeo di un 'euro digitale', valuta sottratta al controllo statunitense dei pagamenti digitali (con il circuito delle carte di credito), si contrappone il modello trumpiano – ma ormai, statunitense – delle *stablecoins*, monete ancorate al dollaro. Dietro al divieto (!) di adottare un dollaro digitale imposto alla FED dal 'Genius Act' del luglio di quest'anno, si può leggere l'intenzione dell'amministrazione USA di avere una massa valutaria sui mercati internazionali che: (a) rafforza il dollaro come moneta degli scambi internazionali, (b) non crea

inflazione e (c) sostiene il debito pubblico statunitense, poiché la garanzia della parità con il dollaro viene garantita, dagli emittenti privati, mediante l'acquisto dei titoli di stato statunitensi. Il rischio di instabilità monetaria che consegue a masse rilevanti di valute non controllate dalle banche centrali è per gli Stati Uniti secondario e comunque non assoluto ma relativo, in quanto condiviso con tutti gli altri paesi, ivi inclusi gli stati membri dell'Unione europea. Il percorso seguito dall'UE e dalla Cina è differente e fondato sulla moneta di banca centrale, che si evolve sul piano digitale. Il modo in cui questi due opposti percorsi tenderanno a integrarsi inizia ora ad essere oggetto di studi; l'intervento di Armando Di Cello in questo Rapporto ne illustra il precipitato sul sistema dei pagamenti, mentre quello di Matteo Ghezzi si concentra sulle prospettive dei mercati finanziari, e dunque sulle conseguenze della rivoluzione tecnologica per i consumatori-investitori.

Un indizio sulla 'giusta distanza' tra le impostazioni divergenti degli USA rispetto a UE e Cina sulla politica monetaria digitale può venire dalla protezione dei dati personali, che ha visto svilupparsi un percorso analogo, poiché la Cina ha applicato una disciplina GDPR-like. L'intervento di Aurora Saija in questo Rapporto illustra i punti critici e le soluzioni adottate sinora, con riferimento all'ampiezza dei dati raccolti, alla trasparenza, alla base giuridica del trattamento, ai dark pattern, alle decisioni interamente automatizzate, al potenziale effetto manipolativo dell'uso dell'IA e alle sfide del coordinamento.

Nei trasporti, Federico Nespega indaga la trasformazione dei mercati determinata dalle piattaforme digitali, che in questo settore più che in altri hanno rapidamente conquistato il mercato (facilitando l'evoluzione multimodale di architetture di *Mobility as a Service*) e i consumatori, e in cui è dunque più urgente estendere le forme di tutela. In quest'ottica diventa sempre più decisivo il coordinamento tra ART e altre autorità, a partire da AGCM, AGCom, ARERA e GPDP, poiché è nell'intersezione della matrice che il mercato si sviluppa sfruttando l'implosione della matrice regolatoria. I trasporti sono, insieme ai mercati bancari, finanziari e assicurativi, il migliore esempio di settore ibrido, che si sviluppa in ragione dell'intermobilità, e richiede una *cross-regulation*, e dunque un'applicazione delle norme di ciascun settore in ragione del segmento del viaggio offerto da operatori del settore.

Peculiare è anche l'operare delle piattaforme nei settori dell'energia, gas, acqua, igiene ambientale, settori regolati da ARERA, ciascuno con discipline autonome, europee e nazionali, e reazioni diverse del mercato di fronte all'erompere della tecnologia. L'ARERA è stata tra le prime autorità

a dotarsi di strumenti tecnologici e metterli a disposizione dei consumatori, con piattaforme che sono diventate standard europei. Ciononostante, l'evoluzione normativa europea, che tenta di inseguire i mercati, mette alla prova gli strumenti e impone continue modifiche, che l'ARERA adotta secondo le dinamiche ormai consolidate del circolo regolatorio.

Mentre nei settori verticali, o nelle regole generali, orizzontali, della matrice regolatoria, registriamo un inseguimento delle autorità di vigilanza agli operatori sul mercato, con strumenti *ex post* o, per le autorità anche di regolazione, *ex ante*, che scontano però asimmetrie informative e rischi di cattura, superati solo dalla nuova metodologia della 'regolazione partecipata', l'Autorità nazionale anti-corruzione rappresenta un caso a sé stante, illustrato da Serafina Piantedosi. Le norme di primo livello (il nuovo Codice dei contratti pubblici), le norme di secondo livello, di *hard* (regole tecniche, adottate dall'AgiD) e *soft law* (linee guida), unitamente a un'organizzazione virata sulla tecnologia e a un coordinamento efficace delle diverse forme dell'amministrazione pubblica, garantiscono all'ANAC un'esecuzione delle norme coerente con il dato legislativo ed efficace sul mercato. Del mercato, peraltro, l'ANAC si propone come interlocutore pubblico tecnologico; in sostanza, una rivoluzione copernicana.

Ad esempio, la Banca Dati Nazionale dei Contratti Pubblici costituisce, nei fatti, una piattaforma logica che opera nel Web2 e costruisce un ponte verso il Web3. Questa piattaforma logica è coordinata con altre piattaforme, da cui estrae e deriva i dati, ed è quindi con queste interoperabile; garantisce però un accesso controllato e condizionato, che legittima poi la trasparenza interna alla piattaforma. Si tratta dunque di un modello più che centralizzato, distribuito.

Nella prospettiva Web3 il modello distribuito autorizza a immaginare un'interoperabilità tra piattaforme logiche, più che tra banche dati. Si pensi alla correlazione tra le polizze assicurative di una gara pubblica e la piattaforma IVASS sulle polizze, incluse quelle transfrontaliere, e in particolare si pensi all'evoluzione di una certificazione delle polizze su blockchain, che già le norme consentono per le gare pubbliche. Questi passaggi, unitamente a un'evoluzione della semplificazione anche normativa, possono aumentare in maniera significativa l'efficacia e l'efficienza del sistema.

In questo ambito è chiara e netta anche la separazione delle competenze tra autorità, nella fattispecie, tra ANAC e AGID, competente quest'ultima per l'adozione delle regole tecniche, tra cui la descrizione dei flussi, degli schemi di dati e degli standard europei di interoperabilità tra i sistemi telematici, della certificazione delle piattaforme di *procurement* che gestiscono l'intero ciclo di vita dei contratti pubblici, in ambito nazionale

e per gli appalti transfrontalieri (via e-Certis, che consente di individuare le corrispondenze tra certificati e attestati nei paesi UE). La connessione tra l'AgiD e il mercato diretta e via ANAC consente un'applicazione piena e coerente del circolo regolatorio, avendo sia l'autorità sia l'agenzia un contatto diretto con il mercato e l'indipendenza (sul piano informativo) e l'autonomia (sul piano informatico e tecnologico) per orientare il mercato verso le garanzie del welfare europeo, ormai continentale.

Il dovere di leale collaborazione istituzionale nei rapporti tra autorità indipendenti e agenzie: dal coordinamento occasionale alla strutturale interdipendenza

Marco Cappai, Paolo Occhiuzzi[1]

Il contributo esamina la crescente complessità del quadro regolatorio europeo in materia di mercati digitali, mettendo in luce come l'intensificazione dell'attività normativa dell'Unione – espressione del cosiddetto Brussels Effect regolatorio – abbia condotto alla formazione di un sistema caratterizzato da una fitta sovrapposizione di discipline settoriali (tra cui DSA, DMA, AI Act, GDPR e Codice del Consumo), privo tuttavia di adeguati strumenti di raccordo e compensazione. La molteplicità degli interessi pubblici coinvolti e la disomogeneità nella designazione delle autorità nazionali competenti hanno prodotto un mosaico istituzionale frammentato, nel quale più amministrazioni risultano contemporaneamente legittimate a intervenire, in assenza di criteri certi di riparto e di risoluzione dei conflitti di competenza.

In tale contesto, la giurisprudenza e la prassi amministrativa hanno progressivamente delineato un principio di leale cooperazione inter-autorità, volto a colmare, praeter legem, le lacune di coordinamento emerse nelle fasi di public enforcement. *Tuttavia, la proliferazione di comitati, gruppi di lavoro e tavoli di coordinamento rivela una duplice natura: da un lato, rappresenta una risposta fisiologica alla crescente complessità del sistema; dall'altro, evidenzia la crisi di un modello di* law-making *ancora improntato a una logica quantitativa di produzione normativa, piuttosto che qualitativa.*

*In chiave prospettica, il lavoro si interroga sugli effetti che una più piena attuazione del principio di cooperazione potrà esercitare sull'evoluzione del diritto regolatorio europeo, prospettando l'avvio di una Better Regulation Agenda 2.0. Tale agenda dovrebbe includere, già nella fase di valutazione d'impatto (*impact assessment*), non solo i costi dell'*enforcement*, ma anche quelli del coordinamento inter-amministrativo, così da calibrare le architetture regolatorie sulla reale capacità delle autorità di cooperare in modo efficace.*

[1] I paragrafi 1, 3 e 3.1 sono a cura di Marco Cappai, mentre i paragrafi 2, 3.2 e 4 sono a cura di Paolo Occhiuzzi. Le considerazioni e le opinioni espresse nel presente contributo riflettono esclusivamente il pensiero degli autori e non impegnano in alcun modo le Autorità di appartenenza.

Il coordinamento delle istruttorie tende, infatti, ad assumere i tratti di una prassi strutturale e non meramente eventuale. Ciò comporta il rischio che la moltiplicazione delle sedi di confronto generi costi di coordinamento crescenti, destinati a gravare sull'efficienza complessiva del sistema. Per questa ragione, la valutazione preventiva di tali costi appare imprescindibile ai fini di una regolazione sostenibile.
In definitiva, il coordinamento inter-autorità si configura non solo come attuazione concreta del principio di leale collaborazione, ma anche come banco di prova per il futuro assetto della governance regolatoria europea: un assetto che, per essere equilibrato e funzionale, dovrà saper coniugare la pluralità delle competenze con l'esigenza di un'azione amministrativa coerente, proporzionata e realmente integrata.

SOMMARIO. 1. Il piano normativo: molte sovrapposizioni, poche stanze di compensazione – 2. Il piano applicativo: l'elaborazione, ad opera della giurisprudenza, di un dovere di coordinare gli interventi di *public enforcement* – 3. Verso una strutturale interdipendenza. Le vie del coordinamento – 3.1. Il coordinamento (e la semplificazione) delle normative: una *better regulation agenda* 2.0? – 3.2. Il coordinamento delle istruttorie in via di prassi – 4. Verso una governance cooperativa delle istruttorie

1 Il piano normativo: molte sovrapposizioni, poche stanze di compensazione

È opinione diffusa che, soprattutto nell'ultimo decennio, l'energico impegno dell'Unione a governare la complessità dei mercati digitali attraverso un c.d. *Brussels effect* regolatorio abbia prodotto, accanto a molti effetti positivi, alcuni eccessi, con una rapida stratificazione di interventi normativi in parte ridondanti, in quanto diretti a conseguire obiettivi di *policy* tra loro spesso affini o contigui.

A tale moltiplicazione delle fonti di produzione si deve aggiungere la non sempre irreprensibile tecnica normativa impiegata dal legislatore europeo.

Sempre più atti di legislazione secondaria dell'Unione – pur optando per la forma-tipo del regolamento – si caratterizzano per formule ampie, dettando regole direttamente applicabili, ma non auto-applicative. In aggiunta, molte di queste normative, siano esse dettate con regolamento o direttiva, si caratterizzano per un contenuto multi-valoriale, dando ingresso a una pluralità di interessi pubblici eterogenei. Paradigmatici, in tal senso, sono il Regolamento sui servizi digitali (*Digital Services Act* – DSA)[2] e sull'intelligenza artificiale (*Artificial Intelligence Act* - AI Act)[3].

[2] Cfr cons. 9 e art. 1 Reg. (UE) n. 2065/2022, secondo cui "*l'obiettivo del* […] *regolamento è contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo*". Per una panoramica, A. TURILLAZZI,M. TADDEO, L. FLORIDI, F. CASOLARI, *The digital services act: an analysis of its ethical, legal, and social implications*, in *Law, Innovation and Technology*, n. 15(1)/2023, 83 ss.

[3] Reg. (UE) n. 1689/2024. L'*AI Act* pone dei requisiti minimi che, ancorché scalari, sono uniformi su tutto il territorio dell'Unione e ineriscono, essenzialmente, all'affidabilità (*trustworthiness*) della tecnologia. Tale anima del regolamento riflette un *product safety approach*

In molti di questi casi, la designazione delle Autorità nazionali competenti è rimessa, in ossequio al principio di autonomia procedurale, agli Stati membri, che volta per volta optano per l'istituzione di nuovi soggetti, la designazione di Autorità esistenti o modelli misti.

Coesistono, dunque, più normative di principio, presidiate, sul piano del *public enforcement*, da più soggetti amministrativi. Ciascuna di queste discipline può rilevare, incidentalmente, in sede di applicazione di un'altra.

Muovendo da questa premessa di contesto, il contributo si divide tra presente e futuro.

In parte, esso si sforza di fotografare le principali difficoltà sin qui affiorate nella giurisprudenza e nella prassi; in parte, esso prova a immaginare possibili percorsi – a livello sia normativo che di prassi – per completare la transizione, già in corso, da un modello di autonomia funzionale delle *Authorities* (e *Agencies*) di regolazione e vigilanza del mercato a un modello di inevitabile (e, dunque, permanente e strutturale) interdipendenza tra queste.

L'osservatorio privilegiato dei processi trasformativi in atto sono tutte quelle numerose situazioni in cui si verificano, cumulativamente, le seguenti condizioni:

(i) si registra una sovrapposizione normativa intersettoriale (es. privacy-antitrust/DMA/DSA/tutela del consumatore; tutela del consumatore/DSA; IA/GDPR-normative settoriali[4]; ecc.), nel senso che la medesima vicenda può essere sussunta in diverse norme di legge, affidate all'*enforcement* di amministrazioni non riconducibili al medesimo sistema di vigilanza[5];

---

e, non a caso, si intreccia, in larga parte, con la disciplina europea in materia di sicurezza dei prodotti. Al contempo, la protezione dei "valori europei" rappresenta una dichiarata finalità del regolamento, che intende coniugare il carattere dell'affidabilità con quello dell'"antropocentrismo" della tecnologia al fine di assicurare che l'IA sia rispettosa dei diritti fondamentali (*rights based approach*). Cfr. cons. 1 e art. 1 del Regolamento, nonché M. Almada, N. Petit, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in CML Rev., n. 62(1)/2025, 85 ss.

[4] Per una panoramica, P. Hacker, *The AI Act between Digital and Sectoral Regulations*, Bertelsmann Stiftung. Gütersloh, 2024.

[5] Le sovrapposizioni tra normative nazionali che ineriscono, nei vari Stati membri, allo stesso ambito materiale (concorrenza; privacy; tutela del consumatore; ecc.) sono meno problematiche, potendo e dovendo trovare una composizione interna al sistema comune di vigilanza. Il che talvolta avviene attraverso meccanismi di *case-allocation* predeterminati dal legislatore (si pensi al GDPR o al DSA), talaltra attraverso strumenti di *soft law* (si pensi

(ii) le Autorità amministrative di più ambiti ordinamentali possono ritenersi, per i profili di competenza, titolate a intervenire e manca un criterio di risoluzione del concorso tra le norme sostanziali in concorso (la formula tipo è: "… [Il/La] *presente* [regolamento/direttiva] *non pregiudica l'applicazione di* …")[6];
(iii) il legislatore non prevede (o non disciplina compiutamente) meccanismi di coordinamento inter-amministrativo: talvolta nulla dice sul punto; talaltra si limita a evocare genericamente il principio di leale collaborazione; altre volte ancora crea delle apposite sedi istituzionali di confronto ("comitati", "gruppi", e via discorrendo), senza però regolarne, in concreto, l'operatività.

Con riferimento alla terza e ultima condizione, possono portarsi alcuni esempi.

Per quanto concerne le possibili sovrapposizioni del *Digital Markets Act* (DMA)[7] con altre discipline europee applicabili ai mercati digitali, è stata istituita un'apposita struttura, il Gruppo ad alto livello (*High Level Group*), con funzioni di alto coordinamento, limitato a questioni di interesse generale[8]. Il fatto stesso che il legislatore europeo abbia avvertito l'esigenza di creare un simile luogo di confronto denota un rischio di interferenze tra i vari corpi normativi considerati. Tuttavia, il Regolamento non stabilisce meccanismi concreti di cooperazione intersettoriale tra Autorità, né detta criteri sostanziali di raccordo delle varie discipline riguardate[9].

---

alla Comunicazione della Commissione relativa alla cooperazione tra la Commissione e le giurisdizioni degli Stati membri dell'UE ai fini dell'applicazione degli articoli 81 e 82 del trattato CE (2004/C 101/04), adottata nel quadro del Reg. (CE) n. 1/2003).

[6] La questione si pone in termini meno pronunciati in presenza di previsioni di legge che, pur senza delimitare nettamente le competenze, si fanno comunque carico di regolare il concorso tra le norme sostanziali di riferimento. Può al riguardo richiamarsi la saga sull'*actio finium regundorum* tra Autorità Garante della Concorrenza e del mercato (AGCM) e le Autorità di settore in materia di tutela del consumatore, sorta intorno all'interpretazione del criterio di specialità di cui all'art. 3(4) Direttiva 2005/29/CE. Tale previsione, ancorché foriera di incertezze interpretative, si preoccupa, infatti, di disciplinare il concorso tra norme.

[7] Reg. (UE) n. 1925/2022.

[8] Art. 40 DMA.

[9] Il Gruppo ad alto livello svolge funzioni che potrebbero definirsi di *advocacy* sul coordinamento. Esso è composto dall'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC); il Garante europeo della protezione dei dati (EDPS) e il Comitato europeo per la protezione dei dati (EDPB); la Rete europea della concorrenza (ECN); la

Viene poi in rilievo il Comitato europeo per i servizi digitali istituito nel quadro del DSA[10]. Esso è composto da un rappresentante per ciascun Coordinatore dei servizi digitali designato a livello nazionale. A prima lettura, il Comitato potrebbe essere considerato come un foro di confronto privo di interesse intersettoriale, essendo proiettato, verso l'interno, alla "sola" attuazione della disciplina sui servizi digitali. In realtà, però, così non è, perché l'interdisciplinarietà è, in qualche modo, un attributo insito all'intero DSA, esempio tipico, come visto, di normativa multi-*mission*. Non a caso, il Regolamento prevede che ogni Stato membro può designare una o più "Autorità competenti"[11] e che, una di queste, debba assumere il ruolo di "Coordinatore dei servizi digitali"[12]. Ogni coordinatore deve dunque farsi carico – oltre che di dialogare assiduamente, in seno al Comitato, con i coordinatori di altri Stati membri e con la Commissione europea – di garantire, all'interno del territorio nazionale, l'uniforme e ordinato svolgimento delle misure di *enforcement* fondate sul Regolamento. Il legislatore nazionale ha designato l'AGCom come coordinatore dei servizi digitali[13], prevedendo altresì che "l'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione"[14]. Come si vede, né il Regolamento, né la disciplina nazionale di esecuzione ripartiscono nettamente le competenze e/o dettano criteri sostanziali di risoluzione di eventuali conflitti tra norme.

Rete di cooperazione per la tutela dei consumatori (CPC-Net); il Gruppo dei regolatori europei per i servizi di media audiovisivi (ERGA). Il Gruppo può individuare e valutare le interazioni attuali e potenziali tra il DMA e le norme settoriali applicate dalle autorità nazionali che compongono le reti e gli organismi europei in questione, e presentare una relazione annuale alla Commissione in cui illustra tale valutazione e individua potenziali questioni di carattere transdisciplinare. Tale relazione può essere accompagnata da raccomandazioni volte a convergere verso approcci coerenti e sinergie tra l'attuazione del DMA e quella di altre fonti settoriali (art. 40(7) DMA).

[10] Art. 61.

[11] Art. 49(1) DSA.

[12] Art. 49(2) DSA.

[13] Art. 15, comma 1 D.L. n. 123/2023, conv., con modificazioni, dalla L. n. 159/2023.

[14] Ivi, art. 15, comma 2.

Identico discorso può esser fatto per il "Comitato di coordinamento" che la legge nazionale in materia di intelligenza artificiale ha istituito presso la Presidenza del Consiglio. Il Comitato è composto dai direttori generali dell'AgID e dell'ACN – designate, rispettivamente, come Autorità di notifica e Autorità di vigilanza del mercato ai sensi dell'AI Act[15] – e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Attraverso il Comitato – alle cui riunioni possono partecipare, quando si trattano questioni di rispettiva competenza, rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS – l'AgID e l'ACN "*assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti*"[16].

Talvolta, infine, è lo stesso legislatore nazionale, con iniziative unilaterali, a creare le condizioni che rendono necessario il coordinamento.

Recentemente, l'AGCM è stata investita del potere di condurre indagini conoscitive suscettibili di concludersi con l'imposizione di misure di regolazione asimmetrica, quando vengano riscontrati "*problemi concorrenziali che ostacolano o distorcono il corretto funzionamento del mercato con conseguente pregiudizio per i consumatori*" (c.d. *new competition tool* – NCT)[17]. Trattandosi di misure, comportamentali e/o strutturali, imposte *ex ante* e che non presuppongono l'accertamento di un illecito, sussistono rilevanti profili di intersezione con i poteri di regolazione pro-concorrenziale di altre Autorità, soprattutto quelle investite del compito di vigilare sulle *public utilities*[18]. Dopo il parere con cui il Consiglio di Stato ha ritenuto il NCT esteso a tutti i settori economici[19], e non solo a quello aereo, come una prima lettura del testo suggeriva[20], sia l'ARERA che l'AGCom hanno assunto un posizionamento critico sul nuovo potere[21]. Ad oggi, l'unica (timida) forma di procedimen-

[15] Art. 70(1) Reg. (UE) n. 2024/1689.

[16] Art. 20, comma 3 legge n. 132 del 2025, recante "*Disposizioni e delega al Governo in materia di intelligenza artificiale*".

[17] Art. 1, commi 5 e 6 D.L. n. 104/2023, convertito, con modificazioni, con L. n. 136/2023 (c.d. D.L. Asset).

[18] A titolo esemplificativo cfr., per quanto concerne l'AGCom, l'art. 51 d. lgs. n. 201/2021 (TUSMA), nonché, per quanto concerne l'ARERA, l'art. 43, comma 5 d. lgs. n. 93/2011.

[19] Cons. Stato, Sez. I cons., 29 gennaio 2024, n. 61.

[20] Questa la posizione di S. Pagliantini, R. Pardolesi, *Da Twining ad Austin: come far cose con regole o con parole? Sui nuovi poteri dell'Autorità garante della concorrenza e del mercato*, in *Foro it.*, n. 2/2024, 76 ss.

[21] La prima ha auspicato, con un atto di *advocacy*, una modifica normativa volta a limitarne

talizzazione del coordinamento intersettoriale ai fini del nuovo potere si rinviene nella Comunicazione AGCM "*relativa all'applicazione dell'articolo 1, comma 5, decreto legge 10 agosto 2023, n. 104, convertito con modificazioni dalla legge 9 ottobre 2023, n. 136*"[22], dunque un atto di *soft law* non cogente. Ivi si prevede, in particolare, l'acquisizione del parere del competente Regolatore ad opera dell'AGCM.

2. Il piano applicativo: l'elaborazione, ad opera della giurisprudenza, di un dovere di coordinare gli interventi di *public enforcement*

Nel solco delle considerazioni che precedono, l'attenzione può ora concentrarsi su una delle aree in cui le criticità legate alla sovrapposizione normativa si sono manifestate con maggiore evidenza: quella in cui vengono in rilievo, simultaneamente, la disciplina della protezione dei dati personali e quella della tutela del consumatore o della concorrenza. Si tratta, in particolare, dei casi in cui le pratiche di trattamento dei dati personali costituiscono parte integrante di modelli di business digitali fondati sull'apparente gratuità dei servizi, nei quali l'utente, in cambio dell'accesso alla piattaforma, offre i propri dati come forma implicita di controprestazione.

In tali contesti, le competenze delle diverse Autorità – segnata-

la portata applicativa a settori non regolati (Segnalazione AGCom al Governo del 6 settembre 2024, ai sensi dell'articolo 1, comma 6, lettera c), n. 1 della legge istitutiva, con la quale si evidenziano le criticità derivanti dall'applicazione del cd. Decreto Asset sulle competenze regolamentari dell'Autorità); la seconda ha impugnato l'atto di *soft law* con cui l'AGCM ha disciplinato l'esercizio del nuovo potere (cfr. «*Comunicazione relativa all'applicazione dell'articolo 1, comma 5, decreto-legge 10 agosto 2023, n. 104, convertito con modificazioni dalla legge 9 ottobre 2023, n. 136*», approvata con provv. AGCM n. 31190 del 7 maggio 2024, e Deliberazione 8 luglio 2024 276/2024/C, recante «*RICORSO AVVERSO LA COMUNICAZIONE DELL'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO ADOTTATA DALLA MEDESIMA CON PROVVEDIMENTO N. 31190 DEL 2024*»), su cui v. TAR Lazio, Sez. I, ord. 13 febbraio 2026, n. 2796. Nella presentazione alla Relazione annuale 2024, il Pres. Besseghini ha poi chiarito che "[i]n un mondo in cui la regolazione è chiamata ad intervenire con profili crescenti nei settori regolati, con obiettivi che sono la sintesi di sollecitazioni comunitarie, con evidenti e oggettive necessità di miglioramento dei servizi è del tutto chiaro che la 'leale collaborazione istituzionale' debba essere il quadro di riferimento entro il quale svolgere una comune azione".

[22] Adottata con Del. n. 31190 del 2024.

mente il Garante per la protezione dei dati personali e l'Autorità Garante della Concorrenza e del Mercato (AGCM) – tendono a intersecarsi, dando luogo a un duplice piano di tutela: da un lato, quello della privacy, incentrato sul diritto fondamentale all'autodeterminazione informativa; dall'altro, quello del consumatore e della concorrenza, volto a garantire la correttezza delle pratiche commerciali e l'equilibrio competitivo dei mercati digitali.

La giurisprudenza più recente – sia nazionale che dell'Unione europea – ha progressivamente elaborato, proprio a partire da tali ipotesi di interferenza, un principio di coordinamento tra *enforcement* settoriali, volto a evitare sovrapposizioni sanzionatorie e a garantire un'applicazione coerente delle diverse discipline. Tale principio è stato in particolare affermato in relazione ai rapporti tra GDPR e Codice del Consumo, da un lato, e tra GDPR e diritto antitrust, dall'altro.

Ma procediamo con ordine.

Nel contesto dell'economia digitale europea, la costruzione di un mercato unico non può più essere intesa esclusivamente come il perseguimento della libera circolazione di beni e servizi, ma deve oggi necessariamente estendersi alla regolazione dei mercati digitali e delle piattaforme online, nei quali i dati personali costituiscono una risorsa economica di primaria importanza.

In questa prospettiva, l'Unione europea ha progressivamente delineato un quadro regolatorio volto a conciliare, tra gli altri, due obiettivi fondamentali: da un lato, la promozione di un ecosistema digitale competitivo e innovativo; dall'altro, la tutela dei diritti fondamentali degli individui, *in primis* il diritto alla protezione dei dati personali.

Il Regolamento (UE) 2016/679 (GDPR) si colloca come uno degli strumenti centrali di questa architettura normativa, ponendosi l'obiettivo di garantire la tutela del soggetto iperconnesso che opera in ambienti digitali complessi, spesso caratterizzati da asimmetrie informative e da relazioni contrattuali implicite o non formalizzate[23]. La disciplina della protezione dei

[23] L'architrave della protezione dei dati personali si fonda su contrappesi complessi, che non si limitano ai rimedi sanzionatori o risarcitori: è stato osservato (G.M. Riccio, La Nuova Giurisprudenza Civile Commentata, n. 5/2023, p. 1125. Nota a sentenza) che l'evoluzione legislativa sia stata guidata proprio dalla necessità di rafforzare la posizione dei singoli (o, utilizzando la terminologia propria del Regolamento GDPR, dei soggetti interessati), cui sono riconosciuti una serie di diritti, nell'ottica di bilanciare le asimmetrie informative spesso sussistenti tra chi tratta i dati e i soggetti cui tali dati si riferiscono.
Su questo percorso, la dottrina (L. Ammanati, *Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?*. in RIVISTA TRIMESTRALE DI DI-

dati personali, qualificando il dato come espressione di un diritto fondamentale, prescinde dall'esistenza di un rapporto sinallagmatico tradizionale, imponendo al titolare del trattamento obblighi di trasparenza, correttezza e proporzionalità nella raccolta e nell'utilizzo delle informazioni personali.

L'art. 6, par. 1, del GDPR individua i presupposti di liceità del trattamento, tra i quali il consenso dell'interessato e l'adempimento di obblighi legali. In tal modo, la disciplina si configura come un sistema di garanzie autonome, ma suscettibile di interagire con altri ambiti normativi — in particolare con il diritto dei consumatori e con il diritto della concorrenza — ogniqualvolta il trattamento dei dati costituisca la controprestazione economica implicita di un servizio apparentemente "gratuito"[24].

RITTO DELL'ECONOMIA, *2019:1(2019), pp. 8-30*.) ha sostenuto che, nel caso dell'asimmetria informativa, di norma, l'attenzione è indirizzata sul deficit dal lato del consumatore ritenuto, di conseguenza, incapace di decisioni informate. Perciò sarebbe necessario considerare più attentamente la "circolazione delle informazioni" in quanto la lacuna che separa le due parti è di natura più cognitiva che conoscitiva.

[24] A ben vedere, la qualificazione dei dati personali degli utenti dei social media come controprestazione non pecuniaria trova il suo primo riconoscimento espresso nell'ambito dell'attività della Commissione europea (di seguito, "Commissione"), la quale già nel 2014 ne aveva individuato la rilevanza economica in sede di valutazione di una concentrazione tra imprese digitali. In particolare, nel caso *No. COMP/M.7217 – Facebook/WhatsApp*, relativo all'acquisizione di WhatsApp da parte di Facebook, la Commissione ha sottolineato come i servizi di social networking siano normalmente offerti agli utenti in maniera gratuita, ma siano in realtà monetizzati attraverso meccanismi indiretti, quali la pubblicità mirata e i servizi a pagamento (*premium services*).
Come evidenziato nel paragrafo 47 della decisione, "*The vast majority of social networking services are provided free of monetary charges. They can however be monetized through other means, such as advertising or charges for premium services*". Nel medesimo provvedimento, la Commissione ha altresì valorizzato il ruolo del "network effect" quale elemento determinante nella creazione di valore economico per le *consumer communication apps*, considerando specificamente gli effetti derivanti dall'integrazione tra WhatsApp e Facebook in termini di interoperabilità e comunicazione cross-platform. Tale prospettiva ha consentito di riconoscere nei dati personali degli utenti un asset di rilevanza economica strategica, capace di incidere sulle dinamiche concorrenziali del mercato digitale (cfr. §137 della decisione).
La medesima impostazione è stata successivamente confermata dalla Commissione nella decisione del 21 ottobre 2016, nel caso *No. COMP/M.8124 – Microsoft/LinkedIn*, ove si ribadisce la natura economica dei dati e la loro funzione quale leva competitiva nelle concentrazioni tra imprese operanti nei mercati digitali.
Analoga consapevolezza è stata manifestata anche a livello sovranazionale da parte dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), che, nella co-

In questo senso, la sovrapposizione tra GDPR e Codice del Consumo (d.lgs. n. 206/2005) emerge in modo evidente nelle pratiche commerciali digitali, ove la cessione dei dati personali rappresenta il corrispettivo per l'accesso a servizi online. Tale convergenza, pur potenzialmente utile a rafforzare la tutela del consumatore, genera complesse questioni di coordinamento in sede di *public enforcement*.

Non ogni violazione della normativa sulla protezione dei dati comporta, infatti, la configurabilità di una pratica commerciale scorretta ai sensi della direttiva 2005/29/CE. Solo laddove la violazione delle regole di trasparenza e consenso sia tale da alterare il comportamento economico del consumatore medio, può configurarsi un illecito concorrenziale o consumeristico. Tuttavia, l'inosservanza degli obblighi informativi previsti dal GDPR può costituire un indice sintomatico della scorrettezza della pratica, incidendo sull'effettiva libertà di autodeterminazione del consumatore e sul suo consenso "economicamente consapevole"[25].

---

municazione del 2016 intitolata *Big Data: Bringing Competition Policy to the Digital Era*, ha riconosciuto esplicitamente il valore economico del patrimonio informativo costituito dai dati degli utenti delle piattaforme digitali, tra cui Facebook. L'OCSE ha poi approfondito il tema dei servizi a costo zero nei mercati digitali nel documento *Quality Considerations in Digital Zero-Price Markets* del 28 novembre 2018, nel quale ha posto l'accento sulla necessità di ripensare i parametri di qualità e trasparenza dei servizi in cui il prezzo monetario è sostituito dal conferimento di dati personali.

Da ultimo, nel Policy Paper "*Good Practice Guide on Consumer Data*" del settembre 2019, l'OCSE ha fornito alle imprese una serie di linee guida di condotta responsabile nei confronti dei consumatori attivi nei mercati digitali, raccomandando di garantire la massima trasparenza circa le modalità di raccolta, utilizzo e monetizzazione dei dati personali. In particolare, nel documento si prescrive di: "*Tell consumers the full story about how their data will be collected and handled. Inform consumers of privacy and data security practices, before asking them to make a material decision. If your business derives revenue from the use of consumer data, do not conceal that from consumers when offering free services*" (p. 9 ss.).

In altri termini, l'OCSE invita le imprese a "raccontare ai consumatori la storia completa" del trattamento dei propri dati, informandoli in modo chiaro e preventivo sulle politiche di privacy e sicurezza, nonché sulle eventuali forme di remunerazione indiretta derivanti dall'utilizzo dei dati personali, anche nei casi in cui il servizio sia apparentemente gratuito.

[25] Non sussiste, secondo l'orientamento ormai granitico della giurisprudenza amministrativa (TAR Lazio, sez. I, sentenza n. 260/20, confermata da Cons. Stato, Sez. VI, n. 2631/2021) "… *alcuna incompatibilità o antinomia tra le previsioni del "Regolamento privacy" e quelle in materia di protezione del consumatore, in quanto le stesse si pongono in termini di complementarietà, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell'altro alla corretta*

In tale prospettiva, la giurisprudenza e l'attività dell'Autorità Garante della Concorrenza e del Mercato (AGCM) hanno progressivamente ampliato la portata applicativa della normativa consumeristica[26], estendendola a condotte relative al trattamento dei dati personali qualora esse si inseriscano in un rapporto di consumo. Emblematico, in tal senso, è il caso Telepass, in cui l'AGCM ha sanzionato la società per modalità ingannevoli di acquisizione del consenso al trattamento dei dati, evidenziando la connessione tra violazione della privacy e lesione della libertà di scelta del consumatore.

La stessa Corte di Giustizia dell'Unione europea, nella sentenza *Meta Platforms Inc.* (C-252/21, 4 luglio 2023), ha confermato la crescente integrazione tra diritto della concorrenza e tutela dei dati personali, affermando che un'autorità antitrust nazionale può accertare la violazione del GDPR qualora tale valutazione sia necessaria per determinare un abuso di posizione dominante. La Corte ha precisato che l'accesso e l'uso dei dati personali rappresentano elementi costitutivi del potere di mercato nei settori digitali, e che il loro sfruttamento improprio può compromettere non solo la privacy degli utenti, ma anche la contendibilità del mercato stesso.

Tale pronuncia, in linea con l'orientamento espresso dalla Commissione europea e recepito nel *Digital Markets Act*, sancisce il principio secondo cui il trattamento dei dati personali non è più materia estranea alla logica concorrenziale, bensì fattore economico suscettibile di integrare una condotta abusiva.

---

informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole".

[26] Cfr., *ex multis*, PS10207-Samsung; PS10601-WhatsApp; *PS11112 - Uso dei dati degli utenti a fini commerciali*. Quest'ultimo caso, in effetti, rappresenta il punto di svolta nell'approccio a questa applicazione congiunta delle discipline. Nel 2018, infatti, l'AGCM condannava Facebook al pagamento di due sanzioni amministrative pecuniarie, di importo pari a 5 milioni di euro ciascuna, e alla pubblicazione di una dichiarazione rettificativa a causa delle pratiche commerciali scorrette (l'una ingannevole e l'altra aggressiva) poste in essere dal *social network*. Facebook presentava ricorso avverso tale decisione al TAR Lazio, che lo accoglieva soltanto in parte: il tribunale confermava l'esistenza della pratica commerciale ingannevole ma non anche di quella aggressiva. Pertanto, la sentenza veniva impugnata dinanzi al Consiglio di Stato sia da parte di Facebook affinché venisse dichiarata l'insussistenza *in toto* di pratiche commerciali scorrette, sia da parte dell'AGCM affinché venisse riconosciuta, in capo al *social network*, anche la realizzazione di una pratica commerciale aggressiva. Il Consiglio di Stato, tuttavia, confermava la sentenza del Tar, condividendo l'annullamento della pratica aggressiva e confermando la sussistenza della pratica commerciale ingannevole (Cons. Stato, sez. VI, n. 2631/2021).

In questa cornice, il diritto nazionale mostra una progressiva tendenza al coordinamento tra i due plessi normativi.

L'art. 67-*sexdecies*, comma 3-*bis*, del Codice del Consumo, che rinvia all'art. 130, comma 3-*bis*, del Codice della Privacy (d.lgs. n. 196/2003), conferma la contiguità tra le due discipline, delineando una relazione di complementarità più che di alternatività[27]. Tuttavia, permane l'esigenza di assicurare un effettivo coordinamento in sede di *enforcement*, al fine di evitare sovrapposizioni sanzionatorie e incoerenze interpretative.

Sotto il profilo procedimentale, non esiste, allo stato, un obbligo legale di consultazione tra AGCM e Garante per la protezione dei dati personali. L'art. 27 del Codice del Consumo prevede un obbligo di parere soltanto nei confronti dell'AGCOM, mentre il Garante Privacy, non essendo autorità regolatoria di settore, non rientra in tali previsioni[28]. Questa lacuna istituzionale ha indotto la giurisprudenza amministrativa a elaborare un principio pretorio di leale cooperazione, in base al quale le autorità indipendenti devono coordinare le proprie attività quando le rispettive competenze si intersecano.

In tale direzione si colloca la sentenza del Consiglio di Stato n. 497

[27] Va sottolineato, sotto il profilo della contaminazione normativa tra il settore consumeristico e quello della tutela dei dati personali, che anche alcune disposizioni nazionali depongono per una non generale insensibilità di rapporti tra la disciplina delle pratiche commerciali scorrette e quella della privacy laddove le condotte anticonsumeristiche contestate a 'professionisti' intercettino – o addirittura consistano – in una illecita modalità di trattamento dei dati. Rileva significativamente, nella specifica materia che qui ci occupa, la previsione recata dall'art. 67-*sexdecies* d.lgs. 206/2005 (Codice del consumo), nella versione modificata dall'art. 6, comma 2, lettera a-*bis*) d.l. 13 maggio 2011, n. 70 convertito con modificazioni dalla l. 12 luglio 2011, n. 106 e che ha introdotto il comma 3-*bis* nel ridetto articolo, che ora così recita: "*1. L'utilizzazione da parte di un fornitore delle seguenti tecniche di comunicazione a distanza richiede il previo consenso del consumatore: a) sistemi di chiamata senza intervento di un operatore mediante dispositivo automatico; b) telefax. 2. Le tecniche di comunicazione a distanza diverse da quelle indicate al comma 1, quando consentono una comunicazione individuale, non sono autorizzate se non è stato ottenuto il consenso del consumatore interessato. 3. Le misure di cui ai commi 1 e 2 non comportano costi per i consumatori. 3-bis. È fatta salva la disciplina prevista dall'articolo 130, comma 3-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, per i trattamenti dei dati inclusi negli elenchi di abbonati a disposizione del pubblico*".

[28] Per una lettura parzialmente differente, v. M. Cappai, *Dalla legalità procedurale alla legalità cooperativa*, in M. Cappai, A. Davola, U. Malvagna, S. Vaccari (a cura di), *Nuove frontiere della regolazione conformativa dei mercati: esperienze a confronto*, *Rivista di diritto bancario*, fascicolo monografico Suppl. n. IV/2025, 254-256.

del 15 gennaio 2024, che ha annullato un provvedimento dell'AGCM per mancata interlocuzione con il Garante Privacy. La sentenza del Consiglio di Stato n. 497 del 15 gennaio 2024, riformando la decisione del TAR Lazio, ha completamente annullato il provvedimento sanzionatorio adottato dall'AGCM nei confronti di Telepass S.p.A., relativa a presunte pratiche commerciali ingannevoli nella promozione di polizze assicurative RC Auto, fondate – tra l'altro – sulla mancata informazione ai consumatori circa la raccolta e il trattamento dei dati personali per finalità di *marketing* diretto.

Il Consiglio di Stato ha ritenuto che l'AGCM, pur avendo acquisito i pareri dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) e dell'IVASS, avrebbe dovuto coinvolgere anche il Garante per la protezione dei dati personali nel corso dell'istruttoria, poiché la condotta oggetto di indagine implicava aspetti rilevanti di trattamento dei dati personali. In assenza di tale interlocuzione, l'attività istruttoria è stata ritenuta viziata da un difetto di collaborazione inter-amministrativa, in violazione del principio di leale cooperazione tra autorità indipendenti.

Il giudice amministrativo ha evidenziato come le tutele offerte dai due ordinamenti – privacy e concorrenza/consumo – non costituiscano compartimenti stagni, ma elementi di un sistema unitario di garanzie multilivello volto a proteggere la persona anche nella sua dimensione economico-patrimoniale[29].

[29] In questi termini si è già espresso il Consiglio di Stato, Sez. VI, 497/2024: "… *con il termine "trattamento" l'art. 4, n. 2), del Regolamento europeo n. 679/2016 ha inteso riferirsi (con una declinazione dell'espressione, peraltro, già accolta dall'art. 4, comma 1, lett. a), d.lgs. 196/2003, oggi formalmente abrogato per effetto dall'art. 27, comma 1, lett. a), n. 1), d.lgs. 10 agosto 2018, n. 101, c.d. decreto innesto, a far data dal 19 settembre 2018, ma il cui contenuto sostanzialmente sopravvive nella su indicata previsione regolamentare europea) a "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*". *Da ciò ne deriva, lo spettro amplissimo di ipotesi riconducibili all'attività di trattamento e dunque rilevanti in materia di dati personali delle persone fisiche e quindi ricadenti nella sfera di applicazione del GDPR, esclude, già da solo, che la sostenuta (dall'Autorità appellata) esistenza di compartimenti "stagni", non permeabili tra di loro, tra l'ambito di competenza e dei poteri di AGCM rispetto a quelli di altre Autorità, in particolare del Garante privacy, possa validamente militare nel senso di escludere "a priori" qualsiasi forma di collaborazione tra le due Autorità nel corso di una indagine che, seppure fondamentalmente indirizzata all'esame circa la compatibilità o meno con la disciplina consumeristica di condotte sviluppate da professionisti, abbia indubitabilmente addentellati forti e robuste caratterizzazioni osmotiche con la tutela dei dati personali, potendosi, in thesi, sostenere addirittura una*

Tale orientamento, pur coerente con la logica del coordinamento istituzionale, ha tuttavia generato un vuoto di tutela sostanziale, poiché l'annullamento dei provvedimenti dell'AGCM per difetto di collaborazione con il Garante Privacy ha di fatto impedito l'attivazione tempestiva delle misure repressive previste dal Codice del Consumo. La giurisprudenza amministrativa, per tale via, configura la cooperazione amministrativa come condizione di legittimità procedimentale, necessaria e doverosa ai fini dell'applicazione della tutela.

L'insegnamento della Corte di Giustizia nel caso *Meta* rafforza tale orientamento, affermando un principio di integrazione funzionale tra enforcement antitrust e tutela dei dati. In virtù di tale impostazione, le autorità nazionali devono garantire un'applicazione coerente e coordinata delle rispettive normative, nel rispetto del principio di proporzionalità e del divieto di doppia sanzione (*ne bis in idem*).

Sebbene l'approccio giurisprudenziale risponda a un'esigenza di tutela effettiva, esso pone non pochi interrogativi operativi, in quanto suscettibile di appesantire i procedimenti amministrativi e di generare incertezza sui confini delle competenze.

In conclusione, la progressiva contaminazione tra diritto della concorrenza e protezione dei dati personali impone una riflessione sistematica sulla natura e sui limiti del coordinamento tra autorità indipendenti. Al riguardo, tanto la giurisprudenza nazionale quanto quella dell'Unione europea hanno progressivamente riconosciuto l'esistenza di un principio generale di leale collaborazione tra autorità indipendenti, principio che si configura non già come eccezione, bensì come corollario necessario di un sistema di tutele intrinsecamente interconnesso e reciprocamente permeabile. In particolare, con riferimento alle piattaforme digitali, la costante interrelazione tra profili di privacy, tutela del consumatore e concorrenza impone un modello di enforcement cooperativo e coordinato, nel quale la protezione dei dati personali, la trasparenza del mercato e la correttezza delle pratiche commerciali si integrano in un'unica rete di garanzie funzionali alla salvaguardia della persona digitale e al buon funzionamento del mercato unico europeo.

funzionalizzazione tra i comportamenti contestati e la violazione, contemporanea, di discipline normative differenti perché riferite a settori specialistici e quindi la doverosità della cooperazione tra Autorità".

3. Verso una strutturale interdipendenza. Le vie del coordinamento

Se le premesse che precedono sono corrette, allora le vie per realizzare il coordinamento inter-amministrativo tra Autorità indipendenti/Agenzie dovrebbero essere, essenzialmente, due: a monte, occorre limitare, quanto più possibile, che la legislazione (*in primis*, europea) sostanzi le condizioni che rendono inevitabile l'interdipendenza del *public enforcement*, così attivando, come si è visto, il dovere di coordinamento fondato sulla leale collaborazione istituzionale (*infra* § 3.1); a valle – e in mancanza di congegni normativi volti a predeterminare, nell'operatività, le modalità del coordinamento – le stesse Amministrazioni coinvolte devono attivarsi per trovare le migliori formule di coesistenza (*infra* § 3.2).

3.1. Il coordinamento (e la semplificazione) delle normative. Una better regulation agenda 2.0?

Nel corrente momento storico, caratterizzato da una forte instabilità geopolitica, il modello di "*Regulatory State*" europeo sta vivendo una stagione di profondi ripensamenti. Nel dibattito pubblico sembra infatti prevalere, secondo una narrativa schiacciata dalla logica della "competitività", la *de-regulatory agenda*[30]. I diversi pacchetti "*omnibus*" varati dalla Commissione Von der Leyen 2, del resto, puntano chiaramente la direzione della semplificazione.

Non è nelle intenzioni di questo contributo prendere posizione sulla questione, altamente politica, di quale sia la ricetta regolatoria più adeguata a sostenere il ciclo economico nel rispetto dei diritti della cittadinanza.

Il punto di attenzione, più stretto, che ci si sforzerà qui di privilegiare attiene agli effetti che la giurisprudenza sulla leale collaborazione istituzionale tra Autorità/Agenzie, sopra illustrata (§ 2), potrebbe spiegare sul processo di *law-making*, specie ove ripetuta su larga scala.

In particolare, nella misura in cui i princìpi espressi nella sentenza *Meta* fossero portati al loro massimo livello di astrazione, traendone un criterio guida valido non solo per quei casi in cui venga in gioco la tutela della

[30] L. Avril, *The EU post-regulatory state and its deregulation agenda*, in *European Law Open*, n. 4/2025, 158: "The convergence of several long-term or medium-term dynamics (new political alliances, rise of the competitiveness narrative and redefinition of public/private relations) is creating the conditions for political and institutional success for critics challenging the European regulatory State".

privacy, ma per tutti i campi del diritto europeo, si potrebbe ben sostenere che l'introduzione di livelli eccessivi di regolazione rappresenti un "costo" non solo per le piccole e medie imprese – come evidenziano i Report di Mario Draghi[31] e, sotto il profilo della perdita di sovranità, della Commissione affari europei del Senato francese[32] – ma anche (e soprattutto) per le Amministrazioni, chiamate a farsi carico, alla luce della cennata giurisprudenza, di un sempre più significativo "costo" di coordinamento.

Da questo punto di vista, il proliferare di "Gruppi" e "Comitati", comunque denominati, deputati al coordinamento è un fenomeno ambivalente (*φάρμακο*): da un lato, esso costituisce la risposta più razionale e immediata a un crescente bisogno di coordinamento (antidoto); dall'altro lato, rappresenta la spia di allarme di un problema più serio, che disvela un modo di legiferare in cui l'approccio quantitativo prevale su quello qualitativo (veleno).

Dal che l'interrogativo se qualcosa debba cambiare nel modo di legiferare in Europa e, se sì, cosa.

È stato notato che – ancorché il principio "*one in, one out*" sia oggi preso in considerazione, nel contesto della *Better Regulation Agenda*, solo in riferimento agli oneri imposti dal legislatore ai consociati, e non anche a quelli che la legge europea pone a carico delle P.A.[33] – è indubbio che a

[31] M. Draghi, *The future of European competitiveness*, Part B - *In-depth analysis and recommendations*, 321: "SMEs tend to perceive the cost of complying with EU law as greater, also because they are less likely to survive long enough to reap the full benefits of regulation. In 2023, 55% of SMEs flagged regulatory obstacles and administrative burden as their greatest challenge. This was also the second most quoted challenge for start-ups (52%, after access to finance) and the third most frequently cited for mid-caps (36%, after difficulties in finding employees and supply chain disruptions […])".

[32] Sénat, Sessione ordinaria 2024-2025, n. 190 del 4 dicembre 2024, Rapport d'information fait au nom de la Commission des affaires européennes "*sur la dérive normative de l'Union européenne*", <https://www.senat.fr/rap/r24-190/r24-190.pdf>.

[33] Comunicazione della Commissione "*Legiferare meglio: unire le forze per produrre leggi migliori*" (COM(2021) 219 final), §§ 5 e 5.1: "[L']*approccio «*one in, one out*»* […] *garantisce che gli eventuali nuovi oneri introdotti da una nuova legge siano controbilanciati dalla riduzione di oneri precedenti nello stesso settore di attività.* […] L]*'introduzione di approcci del tipo «*one in, one out*» incoraggia i responsabili politici a guardare oltre gli obiettivi strategici e a focalizzarsi sugli aspetti pratici dell'attuazione delle politiche. Con l'introduzione dell'approccio «*one in, one out*», intendiamo rafforzare una cultura di elaborazione delle politiche che non solo garantisca il conseguimento dei nostri obiettivi politici, ma presti anche maggiore attenzione a come ciò viene realizzato. In tale ottica cercheremo di semplificare i processi che permettono di conseguire i risultati previsti prendendo in considerazione l'uso di soluzioni di-*

ogni unità marginale di *enforcement* richiesta dalla nuova legislazione corrisponda, inevitabilmente, una (almeno parziale) diminuzione delle risorse destinate al *public enforcement* delle normative (europee e nazionali) previgenti[34]. E non è isolata l'opinione che, proprio per tali ragioni, i costi dell'*enforcement* debbano avere ingresso nella fase pre-legisativa[35].

Nei medesimi contributi si è poi notato che l'attività di analisi di impatto della regolazione (*Impact Assessment*) condotta dalla Commissione europea in sede di esercizio del potere di iniziativa legislativa ha efficacia limitata quando si tratti di misurare, prospetticamente, i costi dell'*enforcement*.

Per un verso, infatti, la Commissione potrebbe non essere in possesso delle informazioni necessarie a condurre simili analisi, o potrebbe non avere particolari incentivi a reperirle, atteso che – come noto – il diritto amministrativo europeo si regge, in larghissima parte, sulla capacità esecutiva degli Stati membri ("*fait faire*", per dirla con Jean Monnet).

Per altro verso, l'analisi di impatto viene svolta sulla proposta legislativa e non viene ripetuta a seguito degli emendamenti intervenuti nel corso dell'*iter* legislativo (di regola: di co-decisione), per mano del Parlamento e/o del Consiglio.

Cosa potrebbe cambiare, allora?

Per esempio, è stato proposto di sottoporre a consultazione pubblica il *draft impact assessment* predisposto dalla Commissione prima di sottoporlo all'esame del *Regulatory Scrutiny Board* (RSB), nonché di onerare le strutture interne del Parlamento e del Consiglio di stimare l'impatto degli emendamenti proposti[36].

Seguendo questa logica, anche le singole Amministrazioni impattate – ove già individuabili *ex ante* o, perché no, sulla base di una "candidatura spontanea" (l'esperienza dell'*AI Act* insegna) – potrebbero stimare il

gitali ai fini di un'attuazione delle politiche più facile e meno costosa. Così facendo, dovremmo riuscire non solo a ridurre gli oneri imposti dalla legislazione, ma in generale a migliorare la qualità della legislazione specifica e quindi dell'intero corpus *legislativo. Ciò si tradurrà in una maggiore attenzione all'efficienza legislativa, evitando oneri che non sono strettamente necessari per il conseguimento degli obiettivi strategici*".

[34] J. Blockx, *One In, One Out: The Increase of EU Legislation Will Lead to a Crisis of Enforcement*, in *EconPol Forum*, n. 25(6)/2024, 10 ss.

[35] In questo senso, v. anche M. Scholten, *Let us wait and see first how the law does not work? 'Better Regulation' can do it better!*, Jean Monnet Network on EU Law Enforcement Working Paper Series, 2025.

[36] M. Bassini, M. Maggiolino, A. de Streel (CERRE), *Better law-making and evaluation for the EU digital rulebook*, 2025, 44-45.

"costo amministrativo specifico" della proposta legislativa, sotto il profilo dell'*enforcement*. Questo esercizio avrebbe la doppia valenza di accrescere il grado di consapevolezza della Commissione in ordine alle ricadute pratiche della proposta e di consentire, un domani, al legislatore nazionale di designare l'Autorità o Agenzia che abbia prospettato l'impiego maggiormente efficiente delle risorse a disposizione, se del caso indicando, con realistica chiarezza, il fabbisogno supplementare stimato.

Non solo.

Posto che – come si è tentato di illustrare – sembrerebbe di assistere a una fase di transizione, da una stagione di coordinamenti inter-settoriali solo sporadici e occasionali a un futuro segnato, in potenza, da una strutturale interdipendenza tra *Authorities/Agencies*, il naturale completamento di questa proposta sarebbe quello di considerare, nell'*impact assessment*, non solo i costi dell'*enforcement*, ma anche quelli del coordinamento inter-amministrativo.

Maggiore il suddetto costo, minore l'opportunità di dar seguito alla proposta legislativa.

3.2. Il coordinamento delle istruttorie in via di prassi

In assenza di meccanismi normativi idonei a predeterminare, in concreto, le modalità operative del coordinamento, a valle si sviluppano forme di cooperazione in via di prassi tra le Autorità indipendenti e le Agenzie europee e nazionali.

Il riferimento è qui, in particolare, a quelle esperienze che, pur in mancanza di un fondamento legislativo espresso, hanno dato vita a formule di dialogo istituzionale nelle fasi istruttorie dei procedimenti di regolazione e vigilanza dei mercati digitali.

Le Autorità e le Agenzie indipendenti, a livello sia europeo sia nazionale, mostrano ormai una piena consapevolezza di tale esigenza, avendo progressivamente elaborato meccanismi di coordinamento funzionale volti non solo a prevenire sovrapposizioni di competenze o conflitti di attribuzione, ma anche a favorire una lettura comune e condivisa delle dinamiche dei mercati digitali.

Ai fini dell'analisi, tali esperienze possono essere ricondotte a tre principali modelli di cooperazione: i forum allargati, che coinvolgono più Autorità in sedi stabili di confronto; le iniziative unilaterali di livello sovra-europeo, promosse da istituzioni o organismi centrali come la Commissione o l'EDPB; e, infine, le iniziative bilaterali, espressione di una collaborazione diretta tra singole Autorità accomunate da ambiti di competenza intersecanti.

3.2.1. La prassi di coordinamento "organizzato": i forum allargati

Un primo modello di coordinamento è rappresentato dai *forum* istituzionalizzati, nati con la funzione di assicurare un confronto sistematico e stabile tra autorità competenti in settori regolatori contigui.

Si pensi, in ambito europeo, al Digital Markets Act High Level Group, previsto dall'art. 40 del Regolamento (UE) 2022/1925 (DMA)[37], che riunisce la Commissione europea, l'European Data Protection Board (EDPB), il Comitato europeo per la sicurezza informatica (ENISA), il Board per il Digital Services Act (DSA) e il Body of European Regulators for Electronic Communications (BEREC).

Tale meccanismo, formalmente ancorato al DMA, costituisce un laboratorio di cooperazione intersettoriale volto a prevenire conflitti di competenza e a favorire una lettura integrata delle ulteriori discipline settoriali che vengono in rilievo nel momento applicativo del DMA.

L'applicazione di tale modello tuttavia non appare semplice per il coordinamento multilivello che è tenuto ad effettuare e il più delle volte si sostanzia, nella pratica, nell'elaborazione di migliori pratiche di livello "alto".

Accanto a tali esperienze formalizzate, si collocano i forum spontanei, sorti per iniziativa delle stesse autorità. Particolarmente rilevante, sotto questo profilo, è l'esperienza britannica del Digital Regulation Cooperation Forum (DRCF), che riunisce la Competition and Markets Authority (CMA), l'Information Commissioner's Office (ICO), l'Ofcom e la Financial Conduct Authority (FCA)[38]. Il DRCF si è affermato come best practice di cooperazione regolatoria, capace di coniugare flessibilità operativa e chiarezza strategica. Esso rappresenta una forma di coordinamento "orizzontale" che consente alle autorità di affrontare in modo unitario i temi emergenti – come l'uso dell'intelligenza artificiale, la profilazione algoritmica e l'interoperabilità delle piattaforme – mediante documenti di indirizzo e *joint workplans* annuali.

Tuttavia, secondo quanto riconosciuto dagli stessi membri fondatori[39] (Ofcom, ICO e CMA, 2021), l'approccio puramente volontario pre-

[37] Il Considerando 39 del Regolamento DMA chiarisce le finalità del Gruppo che è quella di "*di garantire un'applicazione coerente, efficace e complementare del presente regolamento e di altri regolamenti settoriali applicabili ai gatekeeper*".

[38] Per un approfondimento Vanberg, A.D. (2023). Coordinating digital regulation in the UK: is the digital regulation cooperation forum (DRCF) up to the task? *International Review of Law, Computers & Technology*, *37*(2), 128-146; *(2025) The Digital Regulation Cooperation Forum: a Research Note on Work in Progress. Working Paper. CREATe.*

[39] Competition and Markets Authority. 2022a. DRCF Terms of reference. <https://www.

senta criticità intrinseche, in quanto privo di strumenti giuridicamente vincolanti per garantire la cooperazione effettiva. Il DRCF, infatti, non può emanare direttive o decisioni nei confronti dei propri membri, limitandosi a favorire il dialogo informale e lo scambio di informazioni su questioni di comune interesse. Ciò si traduce, nei fatti, in una debolezza funzionale, poiché in caso di conflitti di competenza o divergenze interpretative – ad esempio tra l'ICO e la CMA nel caso "Google Privacy Sandbox"[40] – il Forum non dispone di poteri per risolvere i dissensi o per stabilire quale autorità debba prevalere.

Questa assenza di poteri decisionali è stata criticata dalla House of Lords Communications and Digital Committee[41], che pur accogliendo positivamente la creazione del DRCF, ha sollecitato l'introduzione di strumenti normativi vincolanti, come obblighi di consultazione reciproca e meccanismi statutari di condivisione delle informazioni tra le quattro autorità. In mancanza di tali strumenti, il rischio è che il DRCF rimanga un organismo incapace di assicurare coerenza e collaborazione effettiva nei casi di sovrapposizione regolatoria[42].

Un ulteriore elemento negativo riguarda la composizione del DRCF, che non include tutti i soggetti coinvolti nell'analisi dei comportamenti degli attori digitali (ad esempio, è stata esclusa la National Cyber Security Centre (NCSC)).

---

gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference> (open in a new window).

[40] Competition and Markets Authority. 2022c. <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

[41] Cfr. Al riguardo, Abrusci, E. 2021. House of Lords Communications and Digital Committee Inquiry into Digital Regulation -Written Evidence (DRG0009). <https://committees.parliament.uk/writtenevidence/40277/pdf/> (open in a new window).

[42] Come osservato dalla dottrina, Newson, Nicola. 2022. Digital Regulation in Focus. House of Lords Library. <https://lordslibrary.parliament.uk/digital-regulation> (open in a new window). Il limite più rilevante del DRCF risiede nella totale assenza di poteri coercitivi o di enforcement. Le sue valutazioni hanno natura meramente consultiva, e nessun regolatore è tenuto a conformarvisi. Di conseguenza, nei casi in cui un'autorità rifiuti di condividere informazioni o di coordinare la propria azione con un'altra, il DRCF non ha alcuno strumento per intervenire. Questa situazione genera una duplice conseguenza: a) una duplicazione dei costi e delle attività di enforcement, poiché più autorità possono aprire indagini parallele sullo stesso soggetto o fenomeno; b) rischio di decisioni incoerenti o contraddittorie, con effetti negativi sulla certezza giuridica e sull'efficacia delle tutele per cittadini e imprese.

Ove il modello adottato mutasse con l'attribuzione di poteri vincolanti, il DRCF potrebbe operare come "one-stop shop" regolatorio, assumendo decisioni uniche a valle di consultazioni tra le autorità coinvolte. In alternativa, il Forum potrebbe agire come organo di mediazione istituzionale, incaricato di risolvere i conflitti tra regolatori e assicurare la coerenza delle loro azioni.

Tuttavia, anche tale esperienza mostra limiti strutturali: la mancanza di un fondamento normativo vincolante può indebolirne la capacità di incidere sui processi decisionali e lasciare ampi margini di discrezionalità alle singole autorità partecipanti.

3.2.2. Le iniziative unilaterali: la cooperazione di matrice interpretativa

Un secondo modello di coordinamento è quello che potremmo definire "unilaterale" o di iniziativa interpretativa, nel quale la cooperazione si manifesta attraverso atti di indirizzo congiunti o linee guida non vincolanti, destinati a orientare l'applicazione coordinata delle normative di settore.

Emblematico è, in tal senso, il lavoro congiunto dell'EDPB e della Commissione europea, che hanno recentemente avviato la redazione di *Draft Joint Guidelines* sull'interazione tra GDPR e diritto antitrust; GDPR e Digital Services Act (DSA)[43] e GDPR e Digital Markets Act (DMA)[44].

Tali iniziative mirano a costruire un quadro interpretativo coerente che consenta di evitare duplicazioni istruttorie e contrasti applicativi, specialmente nei casi in cui il trattamento dei dati personali incida sulla concorrenza o sulla trasparenza dei servizi digitali. La logica sottesa è quella di una "integrazione funzionale" – già affermata dalla Corte di giustizia nel caso *Meta* – che riconduce le diverse discipline a una matrice comune di tutela della persona e di corretto funzionamento del mercato.

Pur non vincolanti, queste linee guida esercitano un effetto di "*soft law*" di crescente rilievo, orientando sia l'azione delle autorità nazionali sia le prassi aziendali dei principali operatori tecnologici.

3.2.3. Le iniziative bilaterali: la cooperazione operativa

Un terzo livello di cooperazione, di natura eminentemente operativa, è costituito dalle iniziative bilaterali, che trovano generalmente sviluppo in occasione di specifiche istruttorie. A livello nazionale, un caso paradig-

[43] <https://www.edpb.europa.eu/news/news/2025/interplay-between-dsa-and-gdpr-edpb-adopts-guidelines_en>.

[44] <https://digital-markets-act.ec.europa.eu/public-consultation-joint-guidelines-interplay-between-dma-and-gdpr-2025-10-09_en>.

matico è rappresentato dall'istruttoria A561 – App Tracking Transparency di Apple[45], condotta dall'Autorità Garante della Concorrenza e del Mercato (AGCM), nell'ambito della quale è stato richiesto il parere formale del Garante per la protezione dei dati personali.

Tale prassi, successivamente formalizzata nel Protocollo d'intesa tra AGCM e Garante Privacy, testimonia la progressiva affermazione di un approccio coordinato in sede istruttoria, finalizzato a prevenire sovrapposizioni di competenze e a garantire una valutazione convergente delle condotte digitali, sotto il duplice profilo della tutela dei dati personali e della concorrenza.

Il Protocollo disciplina una cooperazione strutturata e continuativa, prevedendo che ciascuna Autorità possa segnalare all'altra i casi di propria competenza qualora emergano potenziali violazioni di norme rientranti nell'area di attribuzione dell'altra Autorità. L'accordo stabilisce, altresì, l'obbligo di uno scambio periodico di informazioni relativo alle linee generali di intervento, alle attività svolte, ai procedimenti avviati in materie di interesse comune e agli esiti degli stessi.

Particolare rilevanza assume la collaborazione nello svolgimento di indagini conoscitive congiunte, da condursi coordinando risorse e competenze, anche al fine di formulare segnalazioni congiunte al Parlamento e al Governo su materie di interesse comune. Il Protocollo prevede, inoltre, la possibilità di attività ispettive congiunte, anche con il supporto dei Nuclei Speciali della Guardia di Finanza.

Inoltre, anche in assenza di una cornice normativa specifica, ma in applicazione del principio di leale cooperazione amministrativa, il Protocollo contempla meccanismi di consultazione reciproca in relazione alle istruttorie di rispettivo interesse. Tutte le attività comuni sono coordinate da un Tavolo tecnico, composto dai responsabili degli uffici competenti per le materie trattate, convocato su proposta di ciascuna Autorità secondo le esigenze operative.

Un ulteriore esempio della cooperazione istruttoria in assenza di una disciplina normativa definita è costituito dalla decisione dell'AGCM di non procedere ulteriormente ("non luogo a provvedere") in talune istruttorie relative al Digital Services Act (DSA)[46], in ragione della sostanziale coincidenza delle contestazioni mosse a livello nazionale e a livello europeo dalla Commissione. La motivazione di lasciare "carta bianca" alla Commis-

[45] A561 - APP TRACKING TRANSPARENCY DI APPLE Provvedimento avvio n. 30620.

[46] PS12658 - META-DEEP FAKE Provvedimento n. 31438.

sione è basata, da un punto di vista giuridico, sull'obbligo di assistenza reciproca, ai sensi dell'articolo 4, comma 3, del TUE, che deve regolare i rapporti tra l'Unione europea e gli Stati membri, comprese le Autorità amministrative. Il provvedimento, inoltre, afferma che il procedimento avviato dalla Commissione ai sensi del DSA sia in grado di assicurare la tutela degli interessi dei consumatori italiani eventualmente incisi dalle condotte contestate nell'avvio del caso PS12658.

Sebbene tale prassi testimoni un concreto esercizio del principio di coordinamento inter-amministrativo volto a prevenire il rischio di interventi duplicati e a garantire la coerenza dell'azione regolatoria complessiva, essa solleva criticità di ordine sistemico.

In particolare, l'applicazione estrema di questo principio rischia di tradursi in una totale obliterazione del ruolo dell'AGCM nell'ambito delle competenze attribuite dal Codice del Consumo, in relazione alle pratiche commerciali scorrette nel settore digitale che registrano una sovrapposizione con il DSA. Tale approccio, infatti, porterebbe di fatto a subordinare ogni intervento nazionale all'iniziativa della Commissione europea, privilegiando sistematicamente l'azione di quest'ultima anche nei casi in cui la normativa di cui alla direttiva 20025/29/ce come modificata dalla Direttiva Omnibus avrebbe consentito un intervento autonomo dell'Autorità.

Una simile impostazione appare anche non perfettamente in linea con la ormai nota giurisprudenza della Corte di Giustizia dell'Unione europea[47], la quale ha chiarito che la disciplina delle pratiche commerciali scorrette non si applica esclusivamente ai casi di conflitto con una disciplina settoriale. Ne consegue che una siffatta traduzione a livello procedimentale del principio di leale cooperazione, se portata all'estremo, rischia di comprimere ingiustificatamente la capacità di intervento dell'AGCM, potenzialmente determinando una perdita di efficacia delle tutele offerte ai consumatori digitali a livello domestico.

Nondimeno, la più recente prassi decisionale dell'AGCM sembra evidenziare un significativo mutamento di impostazione[48], meritevole di

[47] Corte di giustizia dell'Unione europea, sezione II, sentenza 13 settembre 2018, C- 54/17 e C-55/17 – Autorità Garante della Concorrenza e del Mercato Concorrenza – Pratiche commerciali scorrette – Fornitura non richiesta – Servizi comunicazione elettronica – Assenza di previa informazione dei consumatori – Fattispecie. Concorrenza – Pratiche commerciali scorrette – Fornitura non richiesta – Servizi comunicazione elettronica – Potere sanzionatorio – AGCM

[48] Cfr. Provvedimento del 4 novembre 2025 (PS12714). L'ipotesi istruttoria contestava a Google che la richiesta di consenso finalizzata a permettere l'uso combinato e incrociato

particolare attenzione proprio perché maturato nell'ambito di un provvedimento di accettazione di impegni, vale a dire in un contesto procedimentale connotato dal massimo grado di discrezionalità amministrativa. In tale occasione, l'Autorità, nel replicare alla deliberazione con cui AGCom aveva ritenuto di non rendere il parere richiesto ai sensi dell'articolo 27, comma 6, del Codice del consumo, ha sostanzialmente respinto il tentativo di ricondurre la fattispecie entro il perimetro applicativo del DSA.

Sotto questo profilo, il passaggio di maggiore rilievo non risiede tanto nella ricostruzione del rapporto tra DSA e DMA con riguardo alla specifica vicenda scrutinata, quanto nella riaffermazione di un principio di ordine generale: la disciplina dei servizi digitali, anche laddove venga in rilievo quale normativa settoriale europea, non determina di per sé alcun effetto di assorbimento dell'*enforcement* consumeristico rientrante nelle competenze dell'AGCM. La motivazione del provvedimento si muove, infatti, lungo una duplice direttrice argomentativa. Da un lato, l'AGCM esclude la stessa pertinenza delle disposizioni del DSA richiamate da AGCom, osservando come la condotta contestata non attenga né alla presenza di contenuti illeciti sui servizi intermediari né alla gestione di rischi sistemici, bensì alle modalità di redazione e diffusione di una richiesta di consenso formulata da un *gatekeeper* ai sensi dell'articolo 5, paragrafo 2 DMA. Dall'altro lato – ed è questo il profilo di maggiore interesse teorico – l'Autorità ribadisce espressamente che il DSA non pregiudica l'*acquis* in materia di tutela dei consumatori e che l'articolo 27, comma 1-*bis* del Codice del consumo continua a operare quale criterio generale di riparto preventivo delle competenze, riservando all'AGCM l'*enforcement* esclusivo delle pratiche commerciali scorrette anche nei casi di concorrenza normativa con discipline settoriali.

---

dei dati personali dell'utenza tra la pluralità dei suoi servizi – circolata su Google Search – sembrasse omettere informazioni rilevanti – o fornirle in modus lacunoso e impreciso – in relazione (i) al reale oggetto ed effetto che tale consenso produce sull'uso da parte di Google dei dati personali dell'utenza, (ii) alla varietà e quantità di servizi Google rispetto ai quali può aver luogo un uso 'combinato' e 'incrociato' dei dati personali dell'utenza, (iii) alla possibilità di modulare e personalizzare il consenso fornito limitandolo a solo alcuni dei servizi di Google. Sotto tale profilo veniva dunque contestata la violazione degli articoli 20, 21 e 22 del Codice del consumo. Inoltre, in avvio si contestava: (i) il blocco temporaneo del servizio Google Search finché non veniva assunta una decisione attiva da parte dell'utenza sulla richiesta di consenso, blocco che avrebbe potuto influenzare l'utenza ad assumere una decisione sotto la pressione risultante dall'impossibilità di fruire del servizio; (ii) la minaccia, nella richiesta di consenso, che laddove esso venisse negato, "alcune funzionalità (...) [dei] servizi Google saranno limitate o non saranno disponibili", potendo ciò indebitamente condizionare gli utenti ad acconsentire al collegamento dei servizi.

Il dato appare di particolare rilievo, poiché sembra segnare un parziale superamento di quell'approccio di *self-restraint* istituzionale che, in nome dell'esigenza di coordinamento tra autorità e della prevenzione del rischio di duplicazioni sanzionatorie o procedimentali, rischiava di tradursi in una sostanziale marginalizzazione del ruolo dell'AGCM nell'accertamento delle pratiche scorrette poste in essere nel contesto delle piattaforme digitali. La soluzione oggi accolta appare, per contro, maggiormente coerente con la già richiamata elaborazione della Corte di giustizia in tema di rapporti tra direttiva 2005/29/CE e discipline settoriali, secondo cui la normativa sulle pratiche commerciali scorrette arretra soltanto in presenza di disposizioni speciali che disciplinino aspetti specifici della pratica sleale imponendo obblighi incompatibili e privi di margini di discrezionalità.

Ne deriva, sul piano sistematico, una ricostruzione più equilibrata del rapporto tra principio di cooperazione e autonomia dell'*enforcement* nazionale. Il coordinamento inter-amministrativo, pur restando imprescindibile in un "ecosistema regolatorio multilivello" quale quello delineato dal DSA, non può essere interpretato nel senso di imporre una generalizzata deferenza dell'autorità nazionale competente per l'applicazione della direttiva sulle pratiche commerciali scorrette all'iniziativa delle autorità europee o di settore. Al contrario, esso richiede una verifica puntuale dell'oggetto della condotta, della funzione della norma settoriale eventualmente concorrente e, soprattutto, della persistente attitudine della disciplina sulle pratiche commerciali scorrette a offrire una tutela autonoma degli interessi economici del consumatore.

In questa prospettiva, la più recente evoluzione della prassi AGCM sembra offrire un'indicazione metodologica di più ampio respiro: il rapporto tra DSA e disciplina consumeristica non può essere risolto attraverso automatismi fondati sulla sola appartenenza della condotta al settore dei servizi digitali, ma deve essere governato secondo una logica di coordinamento, capace di preservare, in assenza di un'effettiva incompatibilità normativa, la pienezza degli strumenti di tutela predisposti dal diritto dei consumatori.

4. Verso una *governance* cooperativa delle istruttorie

Dalle esperienze sopra richiamate emerge un *trend* di fondo: il coordinamento delle istruttorie tende a configurarsi come prassi strutturale e non meramente eventuale, destinata a incidere profondamente sulla fisiologia del "*Regulatory State*" europeo. Il rischio, tuttavia, è che l'accumulo

di sedi di confronto – comitati, forum, gruppi di lavoro – finisca per generare costi di coordinamento crescenti, che si sommano ai costi dell'*enforcement* vero e proprio.

In questa prospettiva, appare opportuno che tali costi vengano considerati *ex ante* già nella fase di *impact assessment* della normativa europea, in modo da calibrare l'architettura regolatoria sulla capacità effettiva delle autorità di cooperare in modo efficiente.

In definitiva, il coordinamento delle istruttorie si pone come manifestazione concreta del principio di leale collaborazione, ma anche come banco di prova per il futuro assetto della regolazione europea: un assetto che, per essere sostenibile, dovrà conciliare la pluralità delle competenze con l'esigenza di un'azione amministrativa coerente, proporzionata e integrata.

Piattaforme e trattamento dei dati personali: l'approccio europeo

Aurora Saija

Piattaforme digitali e protezione dei dati personali: tra privacy, concorrenza e tutela dei consumatori.
Il contributo analizza il ruolo centrale dei dati personali nei modelli di business delle piattaforme digitali e le connesse criticità in materia di privacy, profilazione e decisioni automatizzate. Alla luce dell'interazione tra Regolamento (UE) 2016/679 (GDPR), Digital Services Act, Digital Markets Act e AI Act, il saggio esamina le sfide di regolazione ed enforcement e il ruolo del Garante per la protezione dei dati personali nel garantire un equilibrio tra innovazione, tutela dei diritti fondamentali e fiducia dei consumatori.

1. Piattaforme e trattamento dei dati personali: l'approccio europeo

Le piattaforme online sono ambienti in cui si instaurano relazioni personali e professionali, si realizzano transazioni, si diffondono idee e si acquisiscono informazioni. Ciò è reso possibile da una struttura che consente di facilitare l'interazione a distanza, anche su scala globale, tra due o più gruppi diversi di soggetti (*multi-sided nature*). In via di estrema semplificazione, tenuto conto della prospettiva rilevante ai fini di questo Rapporto, su un versante si trovano le imprese, intenzionate a rafforzare la propria immagine o espandere la propria presenza sul mercato rendendo più visibili e fruibili i propri prodotti e siti web, nonché a ottimizzare la produzione e il marketing mediante targetizzazione della clientela; sull'altro versante i consumatori, che hanno interesse a trovare ed eventualmente comparare in modo rapido beni, servizi e prezzi, così come a beneficiare di costi di

transazione ridotti, della disponibilità di servizi innovativi e della personalizzazione di offerte e funzionalità basata sull'intercettazione dei propri bisogni, gusti e interessi.

Quale che sia il modello di business prescelto, l'ambito di operatività o la dimensione, l'attività delle piattaforme online (quali motori di ricerca, siti comparatori, *marketplace*, fornitori di contenuti audio-visivi, social e professional network e così via) si fonda sulla raccolta e l'elaborazione di dati. Attraverso le nuove tecnologie il dato, e il dato personale in particolare, può essere archiviato, sezionato, analizzato, confrontato, condiviso e assume rilevanza come asset strategico da cui estrarre valore. Se i dati sono il nuovo petrolio, le piattaforme ne sono giganteschi serbatoi.

In ragione della centralità dei dati, la tutela della privacy e l'esigenza di assicurare un effettivo controllo sui dati da parte della persona a cui i dati si riferiscono assumono un ruolo cruciale nel sistema. Emergono nuovi e spesso imprevedibili rischi, amplificati man mano che le tecnologie si evolvono (si pensi all'avvento dell'intelligenza artificiale e ai sistemi di *big data analytics* e *data mining*) e si delineano nuove sfide per il quadro regolatorio e l'*enforcement*, così come per la compliance, alla ricerca del punto di equilibrio tra esigenze di tutela e necessità di non frenare lo sviluppo della *data economy* e le opportunità dell'innovazione *data-driven*.

L'Unione europea ha compiuto una scelta molto chiara in favore di un approccio che, muovendo dal riconoscimento del valore dei dati come leva per l'innovazione e la crescita economica, sia incentrato sull'utilizzo corretto, trasparente, responsabile e consapevole dei dati e sulla protezione dei diritti degli individui come presupposto per la libera circolazione dei dati stessi e la creazione di un mercato unico digitale. Ai principi e alle prescrizioni del GDPR, già ampiamente ispirati all'esigenza di definire un quadro più solido e coerente in materia di protezione dei dati personali, tenendo conto delle sfide poste dall'evoluzione tecnologica e dalla globalizzazione, si è affiancata la Dichiarazione europea sui diritti e principi digitali, che afferma la centralità della persona nel contesto della trasformazione digitale e impegna l'Unione europea e gli Stati membri a farsi promotori di questa visione anche in sede internazionale. In particolare, la Dichiarazione richiama il diritto delle persone a un ambiente digitale sicuro e protetto, che tuteli la vita privata fin dalla progettazione "traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate" e il diritto degli individui a un controllo effettivo su come sono utilizzati i propri dati e con chi sono condivisi. Una speciale attenzione è dedicata al tema della protezione dei bambini e dei giovani rispetto a determinate condotte proprie dell'ambiente digitale e delle

piattaforme (diffusione di contenuti dannosi e illegali, sfruttamento, manipolazione e abusi online nonché tracciamento, profilazione e targeting illegali, in particolare a fini commerciali) e all'esigenza di renderli più autonomi e responsabili nell'ambiente digitale, offrendo loro "opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate".

Sulla cornice di principi per la creazione della fiducia digitale fissati dal GDPR e richiamati dalla Dichiarazione si innestano le altre iniziative della Strategia digitale europea, che includono regole volte a prevenire gli abusi di potere economico delle piattaforme '*gatekeeper*', garantendo mercati aperti, equi e contendibili (*Digital Markets Act*-DMA), e regole per rafforzare la responsabilità delle grandi piattaforme nel contrasto alla disinformazione e alla diffusione di contenuti illeciti e per assicurare maggiore trasparenza nelle pratiche relative a pubblicità e sistemi di raccomandazione online, con specifiche misure a tutela dei minori (*Digital Services Act*-DSA). Va sottolineato che questi atti normativi, sia pure con formule diverse, fanno espressamente salvi il rispetto e l'applicazione del GDPR. Analogamente, il regolamento europeo sull'intelligenza artificiale (AI Act), che stabilisce i requisiti per la commercializzazione e l'utilizzo nel territorio dell'Unione dei sistemi di IA, come anticipato sempre più integrati nell'attività di profilazione svolta dalle piattaforme, lascia impregiudicate le norme in materia di protezione dei dati personali. Il diritto alla privacy e al controllo dei dati è e resta quindi uno dei pilastri dell'intero sistema.

2. Attività delle piattaforme e criticità per la protezione dei dati personali

Guardando all'operatività delle piattaforme, tra le principali aree critiche per la protezione dei dati personali si annoverano quelle di seguito sinteticamente illustrate. Come si vedrà, le questioni sono perlopiù legate all'attività di profilazione, intesa come trattamento automatizzato di dati personali per valutare, analizzare o prevedere determinati aspetti della persona (rendimento professionale, situazione economica, salute, preferenze personali, interessi, affidabilità, comportamento, ubicazione o spostamenti), che è al cuore dei modelli di business delle piattaforme. In questa breve, e necessariamente non esaustiva, esposizione verranno messi in rilievo gli indirizzi e i chiarimenti resi negli ultimi anni dalle autorità a diverso titolo chiamate ad interpretare e applicare le norme a tutela della privacy a livello

nazionale, europeo e internazionale.

2.1. Eccesso di dati raccolti

Un primo ambito problematico riguarda l'eccessiva ampiezza e pervasività della raccolta di dati (dagli identificativi classici agli identificativi online, dalle tracce di navigazione ai dati frutto di inferenze), che possono risultare in contrasto con i principi di correttezza, minimizzazione e limitazione delle finalità del trattamento posti dal GDPR, oltre ad aumentare i rischi di accessi non autorizzati, scraping indiscriminato e data breach. Va sottolineato che la correttezza/*fairness* si afferma sempre più come parametro di riferimento ai fini della valutazione di legittimità delle condotte relative alla fornitura di servizi online, in un'accezione ampia che comprende "il riconoscimento delle ragionevoli aspettative degli interessati, la considerazione di eventuali conseguenze negative per gli interessati a causa del trattamento e la valutazione del rapporto fra interessati e titolare del trattamento nonché degli effetti potenzialmente derivanti da squilibri in tale rapporto" (*European Data Protection Board* – EDPB, *Guidelines* 2/2019). In questa prospettiva, ad esempio, forme di profilazione molto intrusive nella sfera personale possono presentare di per sé una incompatibilità con il GDPR.

2.2. Insufficiente trasparenza

Vi è poi la questione della trasparenza, spesso insufficiente, nei confronti dell'interessato in ordine alle modalità e finalità del trattamento-profilazione svolto dalle piattaforme o ai tempi di conservazione dei dati. Per quanto l'utente medio che naviga online stia diventando progressivamente più consapevole del possibile utilizzo dei dati personali per finalità pubblicitarie, la giurisprudenza ha chiarito che resta fermo a carico delle piattaforme l'onere di adottare "un sistema informativo sulla profilazione dei dati personali chiaro, esaustivo e di immediata percezione, tanto più che non è irragionevole ritenere che la maggioranza degli utenti accede ai servizi in modo rapido, senza soffermarsi eccessivamente sulle indicazioni preliminari; per cui è necessario che le informazioni siano immediatamente percepibili, senza la necessità di interpretare le stesse o consultare ulteriori link" (Cons. Stato, sez. VI, sent. 7 gennaio 2025, n. 80). La mancanza di trasparenza non consente all'interessato di valutare in modo appropriato il 'costo' e le conseguenze del conferimento dei suoi dati.

2.3. Base giuridica del trattamento

Altro aspetto controverso è quello dell'individuazione, da effettuare alla luce del principio di accountability, della base giuridica più appropriata per la raccolta e l'utilizzo di dati da parte delle piattaforme. A valle delle pronunce che hanno escluso la possibilità di invocare la necessità-oggettiva indispensabilità del trattamento per l'esecuzione del contratto ed evidenziato la difficoltà di ricorrere al legittimo interesse per giustificare pratiche intrusive di profilazione e tracciamento a fini di marketing (C. Giust., sent. 4 luglio 2023, C-252/21, *Meta Platforms*; EDPB, *Guidelines 1/2024*; GPDP, provv. 7 luglio 2022, n. 248), alcune piattaforme hanno introdotto un modello '*pay or consent*', che pone, in sostanza, l'interessato di fronte alla scelta tra l'autorizzazione ad essere profilato a fini commerciali e il versamento di un corrispettivo monetario per la fruizione del servizio. Tale modalità risulta controversa in quanto non garantisce una genuina e libera (i.e. non condizionata dalla prospettiva di un possibile pregiudizio nel caso di mancato consenso) manifestazione di volontà dell'interessato. La posizione assunta al riguardo dall'EDPB è nel senso che spetti alla piattaforma offrire all'utente un'alternativa equivalente, gratuita e senza pubblicità comportamentale (EDPB, *Parere 8/2024*). Alla base di questo approccio vi è l'idea che determinati servizi offerti dalle piattaforme possono risultare insostituibili per la persona e decisivi per la partecipazione alla vita sociale. È ragionevole ritenere che a una diversa soluzione possa pervenirsi nelle ipotesi di applicazione del modello '*pay or consent*' ad opera di soggetti diversi dalle (grandi) piattaforme, qualora l'utente abbia la possibilità di accedere ad alternative soddisfacenti disponibili sul mercato.

Nella recente attività del Garante si segnala la decisione relativa a una piattaforma che raccoglieva i dati personali dei clienti (per conferimento diretto o acquisendoli da terzi su delega degli interessati) per elaborare e vendere profili di consumo e attribuire poi ai clienti stessi una percentuale dei ricavi ottenuti (GPDP, provv. 14 novembre 2024, n. 704). Il Garante ha ritenuto che il trattamento non potesse essere considerato necessario per l'esecuzione del contratto tra piattaforma e cliente e ha indicato nel consenso dell'interessato la base giuridica più appropriata, rilevando tuttavia nel caso di specie il rischio che il riconoscimento di un corrispettivo economico per la cessione di dati potesse pregiudicare la natura libera del consenso, in particolare per le persone vulnerabili.

Per assicurare la piena consapevolezza della persona, la richiesta di consenso deve in ogni caso essere specifica in relazione a finalità di trattamento identificate in modo chiaro e preciso. Secondo l'orientamento consolidato del Garante, la capacità di autodeterminazione non è assicurata

quando si raccoglie il consenso in modo indifferenziato per perseguire distinte finalità, ben potendo essere ciascuna di esse perseguita singolarmente in presenza di un'autonoma valutazione e determinazione dell'interessato. Nella stessa prospettiva è da stigmatizzare la pratica di utilizzare, nell'individuazione delle finalità del trattamento, formule vaghe, che facciano generico riferimento al miglioramento dell'esperienza utente o a scopi di marketing.

2.4. I dark pattern

Tra le condotte delle piattaforme in contrasto con le disposizioni a tutela dei dati personali, con speciale riguardo ai principi di correttezza, trasparenza e *privacy-by-design*, un'attenzione particolare meritano i dark pattern, intesi come interfacce e processi di navigazione progettati per sfruttare i bias cognitivi e indurre gli utenti a prendere decisioni involontarie e potenzialmente dannose dal punto di vista della privacy. Secondo la tipizzazione effettuata dall'EDPB con riferimento alle piattaforme di social media (*Guidelines 03/2022*), tali pratiche decettive includono: il sovraccarico di richieste/opzioni/possibilità, tali da sollecitare gli utenti a condividere più dati possibili o consentire involontariamente al trattamento (*overloading*); la progettazione di interfacce che portino gli utenti a trascurare gli aspetti di protezione dei dati (*skipping*); le tecniche che influenzano le scelte degli utenti facendo appello alle loro emozioni o utilizzando sollecitazioni visive (*stirring*); gli ostacoli alla possibilità degli utenti di informarsi correttamente sul trattamento e gestire i propri dati (*obstructing*); la mancanza di coerenza e chiarezza nella progettazione delle interfacce, che rende difficile per l'utente avvalersi degli strumenti di controllo della privacy e comprendere la finalità del trattamento (*fickle*); la progettazione delle interfacce in modo da nascondere informazioni o strumenti di controllo della privacy, lasciando gli utenti nell'incertezza (*left in the dark*). Molto opportunamente l'EDPB ha formulato raccomandazioni che mirano sia a guidare la progettazione delle interfacce in modo da evitare i dark pattern, sia a sensibilizzare maggiormente gli utenti sui propri diritti e sui rischi potenziali derivanti dalla condivisione di una quantità eccessiva di dati.

L'importanza del tema ha determinato inoltre un'iniziativa di cooperazione internazionale, sotto forma di un'indagine congiunta (*sweep*) sui dark pattern utilizzati da siti web e app, nell'ambito del *Global Privacy Enforcement Network*, per la prima volta insieme all'analoga rete delle autorità a tutela dei consumatori (*International Consumer Protection and Enforcement Network*). Si tratta di un modello apprezzabile di coordinamento tra autorità preposte all'*enforcement* di norme diverse ma strettamente connesse, che è

auspicabile prosegua nel segno del dialogo costruttivo e della sinergia di competenze.

2.5. Le decisioni interamente automatizzate

Un rischio significativo di compressione dei diritti e delle libertà fondamentali caratterizza l'utilizzo della profilazione nell'ambito di processi decisionali automatizzati. Per tale motivo il legislatore europeo ha previsto un quadro di garanzie rafforzate (art. 22 del GDPR), riconoscendo all'interessato il diritto di non essere sottoposto a decisioni interamente automatizzate che incidono significativamente sulla sua sfera personale, a meno che la decisione sia necessaria per l'esecuzione di un contratto, o sia autorizzata, con adeguate misure di tutela, dal diritto europeo o nazionale, oppure sia stato acquisito un consenso esplicito dell'interessato stesso. In queste ipotesi, l'interessato – oltre a dover essere preventivamente informato sulla logica utilizzata ai fini della profilazione (da intendersi come schema esecutivo dell'algoritmo, che specifica i passi da eseguire in sequenza per giungere al risultato, C. Cass., sez. I civ., ord. 6 ottobre 2023, n. 28538) e sulle possibili conseguenze – ha il diritto di chiedere l'intervento umano, esprimere la propria opinione e, previo l'ottenimento di spiegazioni concise e comprensibili sulla procedura e i principi alla base del trattamento (C. Giust., sent. 27 febbraio 2025, C-203/22, *DB*), contestare la decisione.

2.6. Ia ed effetto manipolativo

Su come evitare che le tecniche di profilazione e personalizzazione comportino una lesione della sfera individuale, oltre alle importanti indicazioni fornite dall'EDPB (*Guidelines wp251rev.01*), utili chiarimenti emergono dalle recenti Linee guida della Commissione europea sulle pratiche di intelligenza artificiale vietate ai sensi dell'AI Act (C(2025) 5052 final). La Commissione sottolinea l'esigenza di distinguere tra manipolazione, che restringe l'autonomia dell'individuo, e persuasione, che opera nei confini della trasparenza e del rispetto dell'individuo. Ne deriva, in linea di principio (e sempre fatta salva la compliance con il GDPR oltre che con il DSA), che sono legittime le forme di raccomandazione e advertising personalizzato realizzate dalle piattaforme sulla base di algoritmi trasparenti e preferenze dell'utente, mentre non sono ammissibili, ad esempio, sistemi di IA volti a inferire le emozioni dei consumatori in modo nascosto per offrire prodotti a prezzi più elevati in uno specifico momento, sfruttando la maggiore propensione all'acquisto dell'interessato.

2.7. La questione dell'age verification

Il rapporto tra minori e piattaforme merita una considerazione particolare. È noto che, quando sono coinvolti minori, eventuali violazioni in materia di trattamento dei dati personali possono più facilmente tradursi in rischi gravi per la sicurezza e l'incolumità, ad esempio se in base alla profilazione vengono proposti contenuti inadatti o violenti o addirittura suggeriti comportamenti autolesionistici, nonché in caso di accesso non autorizzato ad informazioni che potrebbero consentire a terzi malintenzionati l'identificazione e l'adescamento del minore (OCSE, *Towards Digital Safety by Design for Children*, 2024). Una questione ulteriore riguarda le misure di tutela, in particolare i meccanismi di *age verification*, che potrebbero essere configurati in modo da comportare da parte della piattaforma l'acquisizione ingiustificata, in contrasto col principio di minimizzazione, di informazioni sensibili o dati biometrici relativi al minore.

Per far fronte alle questioni menzionate, è essenziale promuovere l'adozione di architetture privacy specificamente '*child-friendly*' e assicurare che ai minori siano fornite informazioni semplici, chiare e facilmente accessibili riguardo al trattamento dei loro dati e ai diritti conseguenti. Accanto a un *enforcement* rigoroso delle regole da parte delle autorità preposte (si pensi ai provvedimenti del Garante nei confronti di Tik Tok o del chatbot Replika), assumono quindi fondamentale importanza le iniziative di soft law, quali raccomandazioni, best practices e codici di condotta, che orientino le piattaforme verso la migliore attuazione dei principi di *privacy-by-design* e *privacy-by-default* con riferimento ai servizi di intermediazione online fruibili dai minori. Data la rilevanza e l'impatto *cross-border* delle questioni in gioco, il confronto di esperienze (GPDP, *Vulnerable Individuals. Tools for Online Protection. Children and Age Verification - Spring Conference* 2023) e l'elaborazione di soluzioni condivise a livello UE (come previsto ad esempio nell'ambito *European strategy for a better internet for kids - BIK+, 2022)* dovrebbero rappresentare la via maestra.

3. Sfide per la regolazione e l'*enforcement* ed esigenza di coordinamento degli attori coinvolti

Il quadro normativo relativo all'attività delle piattaforme è oggi reso complesso dall'interazione di varie discipline, il cui *enforcement* è affidato ad autorità diverse. La profilazione, ad esempio, che in quanto trattamento di dati personali risponde alle regole del GDPR, soggiace al contempo alle norme a tutela dei consumatori (potendo l'assenza di trasparenza circa lo

sfruttamento commerciale dei dati del consumatore dar luogo a una pratica commerciale scorretta ed essendo previsto un obbligo informativo precontrattuale specifico in caso di personalizzazione del prezzo basata su un processo decisionale automatizzato) nonché ai requisiti e alle prescrizioni specifiche contenuti nel DMA (obbligo di chiedere il consenso degli utenti per combinare i loro dati personali tra i servizi o di rendere comunque accessibile un'alternativa meno personalizzata ma equivalente; obbligo di presentare una descrizione, sottoposta ad audit indipendente, di tutte le tecniche di profilazione dei consumatori realizzate), nel DSA (obbligo di assicurare la riconoscibilità della pubblicità personalizzata e di consentire l'identificazione dei parametri utilizzati per determinarne il destinatario; divieto di pubblicità personalizzata basata su categorie di dati sensibili o rivolta a minori) e ai divieti dell'AI Act quando l'algoritmo di profilazione possa determinare manipolazione comportamentale e danneggiare le persone o sia funzionale al *social scoring*. Un caso analogo è quello delle condotte qualificabili come *dark pattern*, che sono suscettibili di ricadere nel campo di applicazione non solo del GDPR, ma anche della disciplina in tema di pratiche commerciali scorrette e del DSA.

A fronte di uno scenario caratterizzato da pluralità di norme e interventi che insistono potenzialmente sulle stesse fattispecie, l'Unione europea sta oggi valutando l'introduzione di un ulteriore strumento legislativo, un *Digital Fairness Act*, per rafforzare la protezione dei consumatori rispetto a determinate pratiche tipiche del contesto digitale (tra cui *dark pattern*, design che crea dipendenza, personalizzazione dei prezzi e della pubblicità, rinnovi automatici e recesso dai contratti online) e colmare i gap di tutela percepiti. Nell'ambito di questa iniziativa, l'Unione si interroga anche sull'opportunità di misure di semplificazione della legislazione volte a ridurre determinati oneri per le imprese.

L'obiettivo da perseguire, per un mercato unico digitale che contribuisca al rilancio della competitività europea, dovrebbe essere un quadro di riferimento semplice e snello, basato sui principi fondamentali della trasparenza e della correttezza e sul pieno riconoscimento del diritto dell'individuo al controllo dei propri dati personali. L'approccio lungimirante della *privacy-by-design-and-by-default* introdotto dal GDPR può, se correttamente implementato, già consentire di evitare molte delle criticità per la protezione dei dati legate all'attività delle piattaforme. Sulla base dell'esperienza, per prevenire il rischio di incoerenze nella regolazione andrebbe seguita l'indicazione del Consiglio UE secondo cui l'adozione di ogni norma contenente previsioni in materia di trattamento di dati personali dovrebbe essere preceduta da una solida analisi di impatto (*Council position and findings*

on the application of the GDPR, 15507/23, 17 november 2023, para. 40), non limitandosi al semplice richiamo della formula che lascia impregiudicata l'applicazione del GDPR.

Le Linee guida e i pareri dell'EDPB hanno già contribuito in modo significativo, come accennato in precedenza, a chiarire alcuni snodi cruciali del regime applicabile alle piattaforme e a promuovere un approccio armonizzato all'applicazione delle regole da parte delle autorità nazionali, fondamentale nel contesto della digitalizzazione e della globalizzazione dell'economia. Di particolare rilievo sono le recenti Linee guida sull'interazione tra GDPR e DSA, in cui vengono considerate e analizzate le disposizioni di quest'ultimo che implicano il trattamento dei dati personali da parte dei prestatori intermediari di servizi, per assicurare la compatibilità con il GDPR degli adempimenti previsti.

Altrettanto fondamentali per il buon funzionamento del sistema sono gli strumenti di co-regolazione previsti dal GDPR, in particolare i Codici di condotta, che possono consentire di adattare la disciplina alle sfide poste dalle nuove tecnologie secondo una visione condivisa dagli operatori, aumentando la fiducia e agevolando la compliance. È importante proseguire anche il ricorso alla consultazione come metodo per ricercare, nel dialogo con gli stakeholder, soluzioni coerenti e rendere la regolazione "il più possibile aderente alle istanze sociali" (GDPD, *Potere e responsabilità. La cultura della protezione dei dati,* Relazione del Presidente Pasquale Stanzione 2024).

Per rafforzare il livello di consapevolezza dei consumatori circa i propri diritti nel contesto online e nei rapporti con le piattaforme è richiesto un impegno collettivo, a vari livelli. Le autorità, e il Garante in particolare, già svolgono in relazione alle rispettive attribuzioni un'opera fondamentale di sensibilizzazione e promozione dell'educazione digitale. L'organizzazione di iniziative di formazione, soprattutto a beneficio delle giovani generazioni con campagne a livello scolastico, può rappresentare un terreno di elezione per sviluppare una cooperazione ad hoc tra autorità, associazioni di consumatori e operatori economici. L'esigenza di predisporre misure di alfabetizzazione degli utenti è peraltro costantemente ribadita dalle istituzioni europee (si pensi alle previsioni che stabiliscono un vero e proprio obbligo in questo senso a carico delle piattaforme per la condivisione di contenuti audiovisivi) ed è da ultimo stata recepita anche nell'ambito del regolamento sull'intelligenza artificiale.

L'esistenza di una pluralità di autorità competenti all'*enforcement* delle diverse norme pone la questione delle possibili sovrapposizioni e determina incertezze per gli operatori. L'esigenza di un efficace coordinamento tra autorità, ai fini di una convergenza di approcci interpretativi e di un *enfor-*

cement più efficace, è quanto mai sentita. I protocolli sono uno strumento utile, per assicurare una maggiore coerenza nelle valutazioni. Molto opportunamente, ad esempio, il protocollo tra AGCM e Garante valorizza la consultazione reciproca nell'ambito delle rispettive istruttorie. Un passo ulteriore che appare oggi sempre più auspicabile consiste nella previsione di una sede stabile di dialogo e confronto, estesa alle diverse autorità con competenze in materia di piattaforme e di digitale.

Data la dimensione globale delle sfide connesse all'economia digitale, anche la cooperazione tra ordinamenti diventa sempre più indispensabile. L'OCSE ha recentemente auspicato, ad esempio, l'interazione e lo sviluppo di policy integrate tra le community AI e *data protection* sulle questioni di comune interesse, per evitare duplicazione di interventi e applicazione di misure divergenti, che aumentano la complessità della *compliance* e dell'e*nforcement* (OECD, *AI, Data Governance and Privacy. Synergies and Areas of International Co-operation,* Artificial Intelligence Papers no. 22/2024). La spinta all'innovazione non implica infatti un arretramento in termini di tutele, ma richiede la ricerca di un assetto di regole e poteri equilibrato e ancorato alla salvaguardia dei diritti e delle libertà fondamentali, nel segno della proporzionalità.

Autorità per le garanzie nelle comunicazioni

Francesca Pellicanò[49] e *Rosaria Petti*[50]

Il contributo esamina il ruolo dell'Autorità per le garanzie nelle comunicazioni nell'attuazione del Digital Services Act e del European Media Freedom Act, soffermandosi sulle sfide di enforcement e sulla posizione di potere delle piattaforme nella mediazione dell'informazione. Viene approfondito il delicato equilibrio tra libertà d'espressione, pluralismo, responsabilità delle piattaforme e tutela dell'interesse pubblico, in un contesto che richiede trasparenza, coordinamento e coerenza nell'attuazione delle nuove regole.

1. **Premessa** (R.P.)

Negli ultimi anni, il panorama economico, tecnologico e sociale presenta cambiamenti epocali in diversi ambiti. L'evoluzione in atto facilita l'innovazione e l'efficienza produttiva; tuttavia, solleva, nel contempo, esigenze ancor più pressanti di tutela dei diritti fondamentali dell'individuo.

L'analisi delle tutele non prescinde però dall'analisi economica dei mercati, dei servizi e degli attori coinvolti nel processo innovativo in atto.

Un primo aspetto da analizzare è l'elemento proprietario, caratterizzato da un forte predominio dell'iniziativa privata.

È noto che i prodotti/servizi commerciali offerti dalle grandi piattaforme digitali consentono una notevole disponibilità di grandi quantità di dati (big data). L'accesso ai dati, quindi, costituisce un primo *asset* chiave detenuto dalle piattaforme, ma non solo. Le piattaforme posseggono oggi il controllo su altri *asset* rilevanti quali l'infrastruttura computazionale e la capacità di sviluppare e addestrare i modelli fondamentali.

Tali aspetti, uniti alla privatizzazione di questa filiera, non neutrale e nelle mani delle grandi multinazionali statunitensi e cinesi, sollevano questioni urgenti di regolazione, trasparenza e controllo democratico. Ecco un

[49] Le opinioni espresse sono personali e non impegnano in alcun modo la posizione dell'Autorità per le garanzie nelle comunicazioni. Ogni errore od omissione è imputabile unicamente all'autrice.

[50] Le opinioni espresse sono personali e non impegnano in alcun modo l'Autorità per le garanzie nelle comunicazioni.

secondo punto di valutazione.

Si pensi, ad esempio, alle modalità con cui l'IA può influenzare l'opinione e la formazione del dibattito pubblico, alla qualità dell'informazione e della partecipazione democratica. Si possono poi verificare forme di vulnerabilità a danno del principio di non discriminazione, quando sistemi di IA vengono addestrati su *dataset* storici, parziali o sbilanciati che ampliano i *bias*, generando trattamenti differenziati a danno di categorie protette o svantaggiate.

I modelli di business delle grandi piattaforme digitali utilizzano l'IA come leva competitiva per potenziare servizi già esistenti, ma la offrono anche come prodotto autonomo sul mercato.

Se si guarda all'intelligenza artificiale, poi, come un'infrastruttura generalizzata, capace di intervenire su lavoro, istruzione, sanità, giustizia, cultura, si intuisce facilmente il rischio sotteso. Talvolta logiche proprietarie opache tratteggiano lo sviluppo di questo nuovo sistema e inevitabilmente rischiano di avere un adeguato e pericoloso coinvolgimento dell'interesse collettivo.

Proprio per affrontare queste sfide, l'Unione Europea ha introdotto l'*Artificial Intelligence Act* (Regolamento UE 2024/1689, c.d. *AI Act*), un quadro regolatorio che punta a bilanciare innovazione e sicurezza.

Parallelamente, il *Digital Services Act* (Regolamento UE 2022/2065, c.d. *DSA*) ha ridefinito l'architettura istituzionale della *governance* del digitale nell'Unione Europea, prevedendo che ogni Stato membro designi un *Digital Services Coordinator* (c.d. *DSC*), responsabile dell'attuazione del Regolamento e della cooperazione tra le Autorità competenti. In Italia, tale funzione, come noto, è stata attribuita all'Autorità per le garanzie nelle comunicazioni.

Ulteriore aspetto di riflessione, in un contesto così variegato, riguarda anche il coordinamento tra Autorità amministrative indipendenti (AAI) trasversali, elemento cruciale per evitare possibili conflitti di competenza, specialmente in ambiti di interesse pubblico generale, e per garantire un'azione amministrativa più efficace.

La convivenza tra Autorità indipendenti trasversali, istituite a tutela di specifici interessi pubblici di portata generale, e Autorità di settore, preposte in via esclusiva a uno specifico settore economico, ha spesso dato luogo in passato a interferenze tra le rispettive attribuzioni.

Finora il coordinamento è stato attuato attraverso meccanismi di cooperazione e di dialogo, basati sullo scambio di informazioni e sulla definizione di ambiti di intervento complementari, per superare le interferenze tra le rispettive attribuzioni e assicurare un'adeguata tutela degli interessi pubblici.

Tuttavia, oggi, in un panorama in cui la verticalità dei settori si affievolisce in favore dell'orizzontalità, si rende ancor più necessario un intervento coordinato e trasversale.

In tal senso, inoltre, si pone la più recente produzione legislativa europea sui servizi digitali. Il già menzionato *AI Act*, ad esempio, è un regolamento "orizzontale", destinato ad applicarsi trasversalmente a tutti i settori economici, avendo riguardo alle implicazioni dirette e ai rischi connessi alla diffusione di software e altri strumenti tecnologici fondati sull'impiego di *AI*. Il Regolamento è dunque destinato a operare in parallelo, anzi, in sinergia, con i quadri regolamentari settoriali in cui tali prodotti trovano impiego.

2. L'*enforcement* tra luci e ombre (R.P.)

Nel rapporto Consumerism dello scorso anno, si sottolineava come le Autorità si trovino a operare in un rammendo costante, continuo, tra la regolazione europea e nazionale, e tra i 'silos regolatori' verticali e orizzontali (rispettivamente, regole settoriali dei diversi mercati e regole generali, che si applicano a tutti i settori, ma non sempre in modo univoco). La disomogeneità di questo sistema, dominata da orizzontalità e verticalità, vede sempre più l'intersecarsi di una pluralità di discipline di settore che talvolta si sovrappongono, altre volte convivono nel segno della complementarità tra loro e con le regole generali.

Questo è uno dei motivi per cui è così rilevante la prassi delle Autorità, cui ormai il legislatore europeo (prima ancora che nazionale) ha attribuito competenze e poteri. Dominare questa frammentazione non è circostanza di poco momento, ma il contributo che le Autorità sono in grado di fornire ai fini della definizione di quello che, in dottrina, è stato definito come "circolo regolatorio", è, soprattutto, nel contesto attuale, imprescindibile.

Recentemente, poi, la diffusione di sistemi di intelligenza artificiale ha messo a dura prova i regolatori nazionali, tenuto conto anche dell'esigenza di garantire un *enforcement* che si colloca sempre più al di fuori dei confini europei. Negli ultimi anni, infatti, il tema prioritario sul 'banco' è quello di individuare lo strumento più adeguato a garantire l'*enforcement* extra-UE di un provvedimento amministrativo di una Autorità di uno Stato membro.

Certo, a una prima lettura, potrebbe facilmente giungere in soccorso la disciplina in materia di responsabilità degli ISP, come regolata dal DSA.

Difatti, agli articoli 4 ss., il DSA in parte riforma la responsabilità degli *Internet Service Provider* (già disciplinata dalla Direttiva e-commerce e attuata in Italia con il decreto legislativo 9 aprile 2003, n. 70).

Come noto, gli ISP beneficiano di esenzioni di responsabilità declinate a seconda della tipologia di *provider* ricoperta (*mere conduit, caching, hosting*), purché si limitino a un ruolo tecnico e passivo, senza conoscenza o controllo sui contenuti, e intervengano tempestivamente in caso di illiceità accertata.

Tuttavia, le esenzioni dalla responsabilità stabilite nel DSA lasciano comunque impregiudicata la possibilità di azioni inibitorie di altro tipo nei confronti degli ISP, anche qualora essi soddisfino le condizioni stabilite nell'ambito di tali esenzioni. Siffatte azioni inibitorie sono disciplinate dal successivo articolo 9 del DSA e consistono in ordini di organi giurisdizionali o Autorità amministrative, emessi in conformità del diritto dell'Unione, che obbligano a porre fine a una violazione o impedirla, anche con la rimozione dei contenuti illegali specificati nei suddetti ordini, o la disabilitazione dell'accesso a tali contenuti.

In termini più pratici, è necessario un ordine di contrasto ai contenuti illegali. Sempre però il DSA prevede che l'Autorità amministrativa competente in Italia a darvi attuazione sia AGCom, in qualità di designato Coordinatore dei servizi digitali, ossia l'Autorità responsabile della vigilanza e dell'applicazione del DSA in Italia.

Verosimilmente le altre Autorità dovrebbero rivolgersi all'Autorità per le garanzie nelle comunicazioni per richiedere un ordine di contrasto ai contenuti illegali. Ecco che, dunque, ai fini di garantire un'efficace tutela, il tema strettamente connesso è quello della cooperazione tra i coordinatori dei servizi digitali, la Commissione europea e le altre Autorità, anche nel caso in cui queste ultime non siano designate come autorità coordinatrici dei servizi digitali a livello nazionale.

In tal senso, va segnalato come allo stato, in sede istituzionale, non siano state individuate soluzioni pratiche al problema dell'*enforcement* di provvedimenti emessi da una Autorità nazionale diversa dal coordinatore dei servizi digitali, lasciando agli Stati membri il compito di individuare meccanismi di cooperazione efficaci che consentano di razionalizzare il lavoro dei diversi attori che potrebbero dover intervenire nei contesti contemplati dal DSA.

Un timido accenno, privo, allo stato, di una concreta soluzione, va riscontrato nell'azione dell'*European Data Protection Board*, che lo scorso 12 settembre ha pubblicato il testo, sottoposto fino al 31 ottobre a consultazione pubblica, delle linee guida 3/2025 circa l'interazione tra il *General*

Data Protection Regulation (GDPR) e il DSA, sottoponendo proprio il tema in questione.

Emerge quindi con urgenza un'interpretazione coerente e armonizzata di quelle normative che perseguono obiettivi diversi, ma complementari; ciò al fine di favorire un ambiente online sicuro, tenuto altresì conto che il DSA, regolamentazione per eccellenza dei servizi digitali, espressamente non pregiudica l'applicabilità né deroga quale *lex specialis* (art. 2 par. 4 lett. g) ad altre normative di settore.

3. Piattaforme, leggi europee e poteri di intervento (F.P.)

Le piattaforme digitali – specialmente quelle "molto grandi" (VLOPs, Very Large Online Platforms) – hanno assunto un ruolo centrale nella mediazione dell'informazione, nel filtraggio, nell'amplificazione, nella moderazione, nella raccomandazione di contenuti. Ciò comporta che esse non siano meri vettori neutrali, ma attori con potere significativo nei confronti di utenti, editori, istituzioni, opinione pubblica.

Alcuni dei nodi critici sollevati dalle piattaforme sono afferenti alla trasparenza operativa (come e con quali criteri le decisioni su cosa mostrare o cosa rimuovere vengono prese), alle responsabilità e ai poteri di intervento rispetto a contenuti illegali o nocivi, all'influenza sulla libertà di espressione, pluralismo, indipendenza editoriale e ad aspetti afferenti alla concentrazione di potere economico e informativo.

Le norme europee DSA ed EMFA affrontano queste criticità, seppure con approcci diversi e con tensioni o limiti residui. Il *Digital Services Act* (Regolamento UE 2022/2065) aggiorna il quadro normativo relativo ai servizi digitali, superando le lacune della Direttiva sul commercio elettronico (2000/31/CE).

I punti salienti relativi al potere delle piattaforme sono:

– **Classificazione differenziata**: le piattaforme di dimensioni molto grandi (VLOPs) sono soggette a obblighi più gravosi, data la loro estesa influenza.

– **Obblighi di diligenza (due diligence) nei confronti dei contenuti illegali e dei rischi sistemici**: procedure per la segnalazione e rimozione dei contenuti illegali, obblighi per prevenire la diffusione di disinformazione, protezione dei minori, trasparenza negli algoritmi di raccomandazione, ecc.

– **Trasparenza e mezzi di ricorso**: motivazioni chiare per le decisioni di moderazione / rimozione dei contenuti, diritto degli utenti a pre-

sentare reclami, rapporti di trasparenza annuali, database di trasparenza.
– **Supervisione e sanzioni**: le autorità nazionali competenti ("*Digital Services Coordinators*") cooperano con la Commissione europea. I poteri di intervento prevedono anche l'irrogazione di sanzioni amministrative per violazioni gravi da parte delle piattaforme.
Questi strumenti assegnano alle piattaforme una posizione regolata: non più "ambienti sregolati" ma soggetti che devono rispettare standard relativi a diritti fondamentali, trasparenza, responsabilità.

Un ulteriore tassello è rappresentato dalla rafforzata protezione per i media e il pluralismo introdotta dall'EMFA. L'*European Media Freedom Act* (Regolamento UE 2024/1083) è un regolamento volto a rafforzare la libertà, il pluralismo e l'indipendenza dei media nell'Unione Europea, entrato in vigore ad agosto 2025.

L'EMFA intende garantire che i media possano operare senza ingerenze politiche, che ci sia trasparenza nella proprietà, che gli editori/media service providers (MSPs) abbiano garanzie in termini di indipendenza, pluralismo e libertà di informazione.

L'EMFA mira poi a definire un "*status* speciale" per i media professionali, prevedendo garanzie procedurali particolari nei casi in cui tali media vengano soggetti alle decisioni delle piattaforme.

L'adozione congiunta di DSA ed EMFA crea un quadro sovrapposto in cui le piattaforme digitali godono di obblighi differenziati, e i media professionali (o che si qualificano come tali) ottengono protezioni aggiuntive. Tra i principali punti di intersezione spicca il "*Media privilege*", previsto dall'articolo 18 dell'EMFA per i fornitori di servizi media. Ciò significa che, se un MSP dichiara la propria qualità (e rispetta requisiti di trasparenza e indipendenza), la piattaforma "molto grande" è obbligata a notificare prima di sospendere o limitare la visibilità di contenuti, e a dare la possibilità di replica in 24 ore. Tale previsione introduce una deroga alla procedura standard del DSA, secondo cui le piattaforme possono moderare contenuti basandosi sui propri termini e condizioni, purché rispettino i principi generali di trasparenza e ricorso. Ora, però, per gli MSP dichiarati esistono procedure speciali. Per godere dello "status media", il soggetto deve soddisfare requisiti quali indipendenza editoriale, rispetto di standard professionali ed etici, trasparenza, non dipendenza da influenze politiche o statali. L'EMFA richiede che il soggetto "media" soddisfi standard per la trasparenza, controllo sull'origine dei finanziamenti, rispetto dell'etica, ecc. Il diritto di risposta, il preavviso prima che la decisione di limitazione o sospensione abbia effetto, la priorità nei reclami per i media professionali, e

un dialogo strutturato tra grandi piattaforme / motori di ricerca, fornitori di media e società civile sono tutti elementi che rafforzano il potere negoziale dei media rispetto alle piattaforme. A ciò si accompagnano, però, limiti strutturali e criticità: il "media privilege" non è automatico, in quanto il "soggetto media" deve dichiararsi come tale e dimostrare che soddisfa i requisiti normativi. La piattaforma (VLOP) ha il compito di verificare tale dichiarazione, il che può comportare discrezionalità nelle scelte. Infine, EMFA e DSA permettono che certe limitazioni siano fatte anche per media professionalmente qualificati, se emergono casi di crisi, violazione grave, o rischi sistemici. L'equilibrio tra libertà espressione / indipendenza dei media e responsabilità delle piattaforme resta delicato.

4. Il potere-privilegio: sfide giuridiche e democratiche (F.P.)

Nonostante l'innovazione giuridica rappresentata dalle piattaforme digitali, restano questioni non risolte, sollevate dalla dottrina, o potenziali rischi. In primo luogo, la delega privata di poteri pubblici: secondo alcuni, si delega alle piattaforme private la responsabilità di decidere cosa è lecito mostrare / rimuovere, con regole che le obbligano a certe procedure, ma che lasciano ampio margine discrezionale su ciò che è "incompatibile" con i propri termini. Alcune voci critiche mettono in guardia sul fatto che la normativa rischia di "privatizzare" il controllo sul discorso pubblico. Ci si chiede, inoltre, come si verifichi concretamente la "indipendenza editoriale", in quanto, se non si garantisce coerenza, il *media privilege* potrebbe generare disparità o essere usato strumentalmente. Inoltre, l'EMFA, per quanto rappresenti un importante passo avanti, non risolve del tutto la tensione relativa al pluralismo, con il rischio che poche grandi piattaforme dominino la distribuzione dei media, influenzando la visibilità e l'accesso all'informazione. Il pluralismo richiede non solo libertà formale, ma condizioni concrete (accesso, remunerazione, interoperabilità, visibilità) che non sono tutte garantite dalla normativa. D'altro canto, non possono non menzionarsi le tensioni con la libertà d'impresa, in quanto le piattaforme sono imprese private con propri modelli economici (pubblicità, algoritmi, personalizzazione) per cui imposizioni troppo rigide possono incidere su innovazione, margini di profitto, competitività internazionale. La normativa cerca di bilanciare questo aspetto, ma non è detto che non emerga conflitto giuridico o economico. Resta valido anche il tema dell'efficacia dell'attuazione: controlli nazionali, cooperazione europea, risorse, responsabilità reale. Anche il miglior quadro normativo resta inefficace senza *enforcement*,

trasparenza, capacità regolamentare e soprattutto con il rischio di implementazioni disomogenee tra Stati membri. In conclusione, DSA ed EMFA costituiscono passi importanti per strutturare la responsabilità delle piattaforme digitali, intervenire sul loro potere e garantire che il pluralismo dei media, la libertà di espressione e l'indipendenza editoriale non restino meri principi formali. In particolare, l'EMFA aggiunge un livello di tutela che prima non esisteva per i media professionali, introducendo il concetto di "*media privilege*" che comporta garanzie procedurali specifiche.

Tuttavia, il successo di queste norme dipenderà non solo dai testi, ma da come vengono applicate nella pratica: dall'efficacia dei controlli, dalla trasparenza reale, dalla cura nel definire i soggetti qualificati come media, e dalla vigilanza affinché le piattaforme non diventino arbitri privati del discorso pubblico senza responsabilità.

Piattaforme *online* e ruolo dell'AGCM

Sara Perugini[51]

In una società segnata dalla digitalizzazione e dall'affermarsi di nuovi mercati virtuali, le piattaforme online costituiscono un punto di snodo fondamentale dello scambio, titolari di una posizione di vantaggio competitivo in grado di condizionare la libera scelta del consumatore. Il settore di mercato richiede un costante adeguamento delle norme da parte dell'Unione Europea che è intervenuta sia in ambito concorrenziale che consumeristico. Scopo della presente analisi è indagare il ruolo che – alla luce degli interventi regolatori euro-unitari – l'AGCM è chiamata a ricoprire al fine di garantire competitività tra le imprese e benessere dei consumatori.

1. Premessa

Che le piattaforme *online*, divenute ormai uno strumento irrinunciabile per l'esercizio delle libertà economiche e della stessa cittadinanza, rappresentino i protagonisti dell'economia digitale e dei nuovi modelli di *business* e mercati (c.d. a due versanti) è oramai indiscusso. Altrettanto nota è la centralità assunta dai dati dei consumatori, controprestazione del servizio offerto e oggetto di investimento primario da parte del mercato ai quali vengono applicati algoritmi sempre più sofisticati in grado di comprendere relazioni, tendenze, principi e processi. Le attuali tecnologie digitali, infatti, consentono di raccogliere, elaborare, utilizzare e archiviare ingenti quantitativi di dati con modalità del tutto innovative in termini di volumi e varietà delle informazioni nonché di velocità di trattamento.

In punto di disciplina, la continua evoluzione di questo settore di mercato richiede un costante adeguamento delle norme da parte dell'Unione Europea che è intervenuta con una rapida reazione regolatoria del potere di mercato delle piattaforme digitali varando il *Digital Markets*

[51] Le opinioni dell'autrice non impegnano l'Istituzione cui appartiene.

Act inteso ad assicurare l'equità e la contendibilità dei mercati digitali e adottando, sotto il profilo consumeristico, una serie di iniziative legislative tese ad attualizzare la normativa orizzontale esistente o ad introdurre nuove regole sul piano sostanziale. Il riferimento è al pacchetto di modernizzazione del diritto dei consumi contenuto nella Direttiva n. 2019/2161/UE (c.d. Direttiva *Omnibus*)[52] e al *Digital Services Act* (DSA), cui si deve l'introduzione delle più ampie e incisive riforme in ambito digitale.

La Direttiva *Omnibus* ha completato il percorso di ampliamento del raggio di applicazione del diritto dei consumi intrapreso dalla Direttiva *Digital Content and Services* (Direttiva 2019/770/UE)[53], stabilendo espressamente il principio, già affermatosi in via di prassi sul piano nazionale[54],

[52] Il provvedimento – nato nell'ambito del c.d. *New Deal for Consumers* con l'intento di rimediare alle lacune e alle incongruenze dell'*acquis* in materia di tutela del consumatore – integra e modifica le direttive in tema di pratiche commerciali scorrette (2005/29/CE), diritti dei consumatori nei contratti (2011/83/UE), clausole vessatorie (93/13/CEE) e indicazione dei prezzi (98/6/CE). Invero la Direttiva recepita in Italia con il decreto legislativo 26/2023 segna la più ampia e incisiva riforma del diritto dei consumi di competenza dell'AGCM anche sul piano dell'efficacia dell'*enforcement*. È previsto, infatti, un aumento delle sanzioni pecuniarie comminabili in relazione alle infrazioni diffuse e alle infrazioni di rilievo unionale, nonché l'innalzamento del massimo edittale da 5 a 10 milioni di euro con riferimento alle sanzioni applicabili alle infrazioni nazionali.

[53] La Direttiva 2019/770/UE ha esteso l'ambito di applicazione della garanzia legale di conformità anche ai contratti di fornitura di contenuto digitale e di servizi digitali che prevedono l'impegno del consumatore a rendere disponibili al professionista i propri dati personali.

[54] Cfr. provv. n. 26597 dell'11 maggio 2017, PS/10601, *Whatsapp trasferimento dati a Facebook*, in *Boll.* 18/2017. Invero, il principio era stato sancito a più riprese dalla Commissione Europea che già nell'esaminare i profili concorrenziali dell'acquisizione di WhatsApp da parte di Facebook, aveva incluso numerose considerazioni sul valore economico dei dati degli utenti dei *consumer communication services* evidenziando come, in genere, gli operatori di *social network* offrano i loro servizi "gratuitamente" ricavando, tuttavia, una remunerazione non pecuniaria dalla pubblicità e dai servizi *premium*. Nelle stesse decisioni, sempre presupponendo il valore economico dei dati, aveva analizzato l'effetto della concentrazione tra Facebook e WhatsApp in termini di «*Data collected from WhatsApp's users*» affermando che «[*t*]*his would have the effect of reinforcing Facebook's position in the online advertising market or sub segments thereof*» (cfr. COMP/M.7217 – Facebook/Whatsapp, §129 ss.). Successivamente, anche negli orientamenti del 25 maggio 2016 per l'attuazione e applicazione della Direttiva 2005/29/UE in materia di pratiche commerciali scorrette, veniva testualmente affermato che «*i dati personali, le preferenze dei consumatori, e altri contenuti generati dagli utenti hanno un valore economico de facto e vengono venduti a terzi*». Per una analisi sia consentito rinviare a S. Perugini,

secondo cui le discipline in materia di pratiche commerciali scorrette e *consumer rights* trovano applicazione anche rispetto ai contratti di fornitura di contenuti e/o servizi digitali che non prevedono la corresponsione di un prezzo. Al fine di aumentare la trasparenza sul mercato *online* la Direttiva ha inoltre previsto obblighi informativi supplementari per i contratti a distanza conclusi sulle piattaforme *online* oltre che regole più stringenti in relazione, tra l'altro, alle recensioni *online*, alla pubblicità occulta e al posizionamento dei prodotti nei motori di ricerca.

Il *Digital Services Act* (DSA) ha introdotto, secondo un sistema di gradazione delle responsabilità in funzione della dimensione dei fornitori di servizi digitali, precisi obblighi a carico delle piattaforme in relazione ai contenuti postati dagli utenti (*user-generated content*) e il rafforzamento della tutela dei loro diritti fondamentali contro i contenuti illegali e la disinformazione. Normazione alla quale si aggiunge il più recente Regolamento (UE) n. 2024/1689 recante l'*AI Act* entrato in vigore il 1°agosto 2024[55].

Invero, alcune delle suddette novità legislative – il *Digital Markets Act*, il *Digital Services Act* e l'*AI Act* – pongono il rapporto tra le nuove discipline e quelle affidate all'*enforcement* tradizionale dell'Autorità di concorrenza in termini non sempre chiari conferendo, lo vedremo, nuova attualità al principio di leale collaborazione.

Alle sfide tecnologiche si aggiungono le sfide geopolitiche legate essenzialmente ai conflitti in Medio Oriente e ad un sistema del commercio internazionale scosso dall'introduzione di un pervasivo reticolo di dazi, che distorcono il confronto concorrenziale tra imprese e tra Paesi.

Considerato il contesto, scopo della presente analisi è indagare il ruolo che – alla luce degli interventi regolatori euro-unitari – l'AGCM è chiamata a ricoprire al fine di garantire competitività tra le imprese e benessere dei consumatori.

L'AGCM di fronte alle sfide della Data Economy, in *Consumerism 2018, undicesimo Rapporto annuale*, p. 25 nonché Id. *Social Economy e tutela del consumatore: il ruolo dell'AGCM*, in *Consumerism 2017*, *decimo Rapporto annuale*, 2017, p. 29.

[55] In proposito Cfr. S. Perugini, *L'Agcm di fronte all'intelligenza artificiale* in *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Ruolo delle Autorità Indipendenti* (a cura di) F. Bassan e M. Rabitti, RomaTRE Press, 2025, pp. 57 ss.

2. DSA e Codice del Consumo

La finalità del *Digital service act* è quella di assicurare la sicurezza dell'ambiente digitale e di creare un quadro armonizzato di regole che ha come destinatarie le piattaforme *online*, rafforzando la tutela dei diritti degli utenti contro contenuti illegali e disinformazione. Un obiettivo in linea di massima diverso da quello che persegue la normativa a tutela del consumatore.

Il diverso interesse tutelato dal Regolamento porterebbe ad escludere la sussistenza di un rischio di interferenza con le discipline di vocazione consumeristica. Una più attenta analisi porta tuttavia a rilevare che diverse norme del Regolamento presentano potenziali interferenze con la disciplina in materia di pratiche commerciali scorrette.

Invero, l'analisi di queste interferenze conduce ad un giudizio di complementarità tra le due discipline espressamente fatta salva dal Regolamento all'art. 2, co. 4, lett. f) e al Considerando 10 e data l'assenza, almeno in astratto, di prescrizioni tra loro palesemente incompatibili che diano vita ad una divergenza insanabile, secondo il noto insegnamento della Corte di Giustizia[56].

A questo tipo di esito, di compatibilità tra DSA e disciplina delle pratiche commerciali scorrette e, quindi, di complementarità, conduce l'analisi di molte delle disposizioni contenute nel Regolamento. Oltre alla disposizione concernente la trasparenza delle interfacce *online* che, per espressa previsione del legislatore, non trova applicazione rispetto alle pratiche commerciali[57] sembra possano considerarsi non problematiche in punto di compatibilità con la disciplina p.c.s., quelle in tema di proceduralizzazione delle attività di moderazione dei contenuti (artt. 17 e 23 Reg.), di protezione online dei minori (art. 28 Reg.), di misure per l'attenuazione dei rischi sistemici (art. 35 Reg.), di tracciabilità degli operatori (art. 30 e 31 Reg.), di obblighi informativi sui sistemi di raccomandazione

[56] Con sentenza del 13 settembre 2018, la Corte di Giustizia ha precisato che il contrasto cui si riferisce l'articolo 3, paragrafo 4, della direttiva 2005/29/Ue, da un lato, riguarda solo norme dell'Unione e non norme nazionali che non costituiscono diretta trasposizione di disposizioni europee; dall'altro, che lo stesso sussiste solo quando disposizioni estranee alla direttiva 2005/29/Ue, disciplinanti aspetti specifici delle pratiche commerciali sleali, impongono ai professionisti, senza alcun margine di manovra, obblighi incompatibili con quelli stabiliti dalla direttiva 2005/29/Ue, dando vita ad una divergenza che non ammette la coesistenza di entrambi i plessi normativi.

[57] Cfr. art. 25, paragrafo 3, del Regolamento.

(art. 27 par. 1 Reg.), di adozione da parte delle piattaforme *online* di codici di condotta (art. 45 e ss.), nonché di *sistemi di raccomandazione* (art. 27 par. 2 e art. 38 Reg.). Tutto ciò in astratto perché, in sede di *enforcement*, il rapporto tra le due discipline deve essere analizzato prestando attenzione al caso concreto: verificando, in particolare, se l'aspetto che viene specificamente in considerazione sia effettivamente disciplinato da una delle prescrizioni presenti nel Regolamento e in che modo tale prescrizione interferisca con la disciplina in materia di pratiche commerciali.

Pensiamo al caso chiuso nei confronti di TikTok (PS12543)[58] nell'ambito del quale – a fronte di eccezioni sollevate dalla parte – la stessa Autorità ha ribadito l'applicazione del Codice del Consumo alle fattispecie oggetto di contestazione "*in ragione del suo carattere orizzontale e dell'ampiezza della nozione di pratica commerciale*" che "*si estende a tutte le attività poste in essere dai professionisti nei confronti degli utenti di servizi digitali prima, durante e dopo l'operazione commerciale*".

Sotto il profilo dell'*enforcement*, il Regolamento prevede una *governance* molto articolata, introducendo meccanismi di cooperazione tra la Commissione, le autorità incaricate dell'attuazione del DSA e gli organismi designati come Coordinatori dei servizi digitali (in Italia, AGCOM).

Il Regolamento, dopo aver stabilito che esso non pregiudica l'applicazione della normativa a tutela dei consumatori, tuttavia non introduce alcuna regola concreta sulla cooperazione con le Autorità preposte. Diverse dunque le criticità e incertezze che possono sorgere sul piano applicativo: sia in ambito nazionale nei rapporti dell'AGCM con le altre Autorità, que-

[58] Muovendo dalla rilevata circolazione sulla piattaforma Tiktok di video raffiguranti giovani che adottano comportamenti autolesionistici (in particolare, la c.d. sfida della "cicatrice francese"), l'Autorità ha accertato l'inadeguatezza delle misure di controllo e di vigilanza adottate dalle società del gruppo TikTok sui contenuti pubblicati dagli utenti, in contrasto con le linee guida dalla stessa piattaforma adottate e pubblicate, in violazione degli artt. 20, comma 2 e 3, e 21, comma 2, lettera b) del Codice del consumo, nonché, per tale via, la minaccia alla sicurezza psico-fisica di bambini e adolescenti esposti alla visione di tali contenuti ex art. 21, comma 4 del Codice del consumo. L'Autorità ha accertato, altresì, la sussistenza di una condotta aggressiva consistente nell'utilizzo da parte di TikTok di un sistema di raccomandazione basato su tecniche di profilazione algoritmica che sfruttavano la vulnerabilità di gruppi di consumatori, riproponendo ad essi in maniera mirata contenuti potenzialmente dannosi, così indebitamente condizionandone il comportamento in violazione dell'art. 25, comma 1, lettera c) del Codice del consumo. A conclusione dell'istruttoria l'Autorità ha irrogato in solido alle società TikTok Technology Limited, TikTok Italy S.r.l e TikTok Information Technologies UK Limited una sanzione pecuniaria di 10 milioni di euro pari al massimo edittale previsto del Codice del consumo.

stione che sembra tuttavia trovare soluzione nell'art. 27, co. 1-*bis* del Codice del consumo che, come noto, definisce un criterio di ripartizione preventiva delle competenze tra l'AGCM e il regolatore di settore e prescrive la consultazione obbligatoria; sia in ambito sovranazionale, con la Commissione Europea *in primis*, che ha competenza esclusiva sulle V.L.O.Ps, ma non solo con essa.

A tale ultimo riguardo, può tuttavia, sin da subito evidenziarsi come, pur in assenza di una regola esplicita nel testo del Regolamento, la prassi seguita dall'Autorità nell'esercizio della propria azione di *enforcement* sia caratterizzata da una costante interlocuzione con l'attività condotta dalla Commissione europea in materia di DSA.

Il coordinamento che caratterizza i rapporti tra le due Istituzioni emerge, ad esempio, in relazione ai casi avviati dall'Autorità e dalla Commissione in applicazione, rispettivamente, della disciplina p.c.s. e DSA nei confronti delle società del gruppo Meta. L'Autorità, come già evidenziato nell'introduzione al Rapporto, ha concluso il caso *Meta – deep fake* (PS12658) con un non luogo a provvedere in quanto – anche a seguito delle interlocuzioni intercorse con gli uffici della Commissione preposti all'applicazione del DSA – ha ritenuto che il procedimento dalla stessa avviato ai sensi del DSA fosse "*in grado di assicurare la tutela degli interessi dei consumatori italiani eventualmente incisi dalle condotte contestate nell'avvio del caso PS12658*"[59].

3. Piattaforme, concorrenza e DMA

Sotto il profilo concorrenziale, nel settore che ci occupa, le significative economie di scala e di scopo e gli effetti di rete determinano una progressiva concentrazione di potere di mercato in capo ad un numero relativamente ridotto di soggetti, che divengono gli interlocutori necessari degli operatori economici che utilizzano la piattaforma.

[59] Occorre inoltre ricordare che sul versante nazionale il legislatore, nel designare l'AGCOM quale Coordinatore nazionale dei Servizi Digitali, ha esplicitamente previsto che «*L'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione*». cfr. art. 15 co. 2 del D.L. 15 settembre 2023, n. 123 convertito con modificazioni dalla L. 13 novembre 2023, n. 159.

Nei mercati interessati, il tradizionale paradigma concorrenziale che si esplica nel confronto tra più imprese è sostituito dalla successione diacronica di una serie di (quasi) monopoli, determinata da innovazioni dirompenti in ambito tecnologico e/o nei modelli di *business*.

In questi contesti, l'adozione da parte degli operatori dominanti di condotte di impresa che ostacolino l'emersione di nuovi prodotti e di imprese concorrenti cristallizza la situazione esistente, soffocando l'innovazione a discapito dei consumatori.

Il potere di mercato delle piattaforme digitali di maggiori dimensioni è amplificato dalla disponibilità di significative quantità di dati relativi agli utenti, la cui rilevanza concorrenziale si apprezza sotto una molteplicità di profili[60].

Nel mondo digitale, un nodo nevralgico dell'intero impianto economico è inoltre rappresentato dal rapporto tra proprietà intellettuale e concorrenza.

Le privative – brevetti, marchi, *copyright*, segreti industriali – nascono per premiare chi innova, offrendo una protezione temporanea che stimola la creazione. Quando si sommano, tuttavia, a un monopolio sostanziale su interfacce, dati o infrastrutture digitali, questi strumenti possono diventare una barriera d'accesso, ostacolando la libera concorrenza nel mercato. Pensiamo ai diritti IP: restano strumenti fondamentali per premiare l'innovazione ma, se impiegati in contesti segnati da forti squilibri di potere, possono diventare leve per escludere la concorrenza.

Il rischio concorrenziale non si limita a ciò che è detto apertamente: spesso si nasconde nelle condizioni di accesso, nella selettività delle concessioni, nella costruzione di ecosistemi che, pur legali sulla carta, escludono nella sostanza.

In questo contesto, la Commissione Europea e le autorità nazionali di concorrenza hanno applicato con la necessaria duttilità le regole *antitrust* del Trattato, reprimendo tempestivamente e con successo le condotte di impresa suscettibili di pregiudicare le dinamiche concorrenziali del mercato.

[60] L'accesso ai dati consente di migliorare l'esperienza di consumo e la qualità del prodotto, innescando un circolo virtuoso che – espandendo la base di utenti e consentendo la generazione di ulteriori dati – conduce ad una situazione in cui i concorrenti di minori dimensioni non sono realisticamente in grado di scalzare l'impresa dominante; in secondo luogo, qualora gli utilizzatori non abbiano il controllo dei dati da essi generati, l'impossibilità di trasferirli ad un altro operatore può costituire un rilevante disincentivo allo *switching*; infine, l'accesso ai dati può fornire alle imprese dominanti uno strumento di protezione rispetto all'innovazione che potrebbe scalfirne il primato.

L'AGCM, ad esempio, ha recentemente avviato, in cooperazione con i competenti uffici della Commissione Europea, un procedimento in cui si ipotizza la sussistenza di un abuso di posizione dominante da parte del gruppo Meta[61] per aver preinstallato il proprio servizio di IA (Meta AI) abbinandolo all'*app* WhatsApp senza che gli utenti lo abbiano chiesto. Secondo l'Autorità Meta appare in grado di trainare la propria base utenti nel nuovo mercato, non attraverso una concorrenza basata sui meriti, ma "imponendo" agli utenti la disponibilità dei due servizi distinti con potenziale pregiudizio dei servizi concorrenti. Esisterebbe, pertanto, il rischio che gli utenti possano restare "bloccati" o funzionalmente dipendenti da Meta AI anche perché tale servizio, utilizzando le informazioni fornite nel tempo, sarebbe in grado di dare risposte sempre più utili e rilevanti[62].

Attenzione è stata riservata anche al tema della interoperabilità. L'Autorità ha infatti sanzionato le società Alphabet Inc., Google LLC e Google Italy S.r.l. Google[63] per abuso di posizione dominante in quanto non avevano consentito l'interoperabilità dell'*app* JuicePass con Android Auto, una specifica funzionalità di Android che permette di utilizzare le *app* quando l'utente è alla guida nel rispetto dei requisiti di sicurezza e di riduzione della distrazione. Ad esito del procedimento, oltre ad irrogare una sanzione di circa 100 milioni di euro, l'*Antitrust* ha imposto a Google di mettere a disposizione di Enel X Italia, così come di altri sviluppatori di *app*, strumenti per la programmazione di *app* interoperabili con Android Auto[64].

Sul piano regolatorio l'Unione Europea ha definito una rapida reazione varando nel 2022 il *Digital Markets Act*, uno strumento legislativo inteso ad assicurare l'equità e la contendibilità dei mercati digitali con il quale sono stati introdotti nuovi obblighi per le piattaforme che occupano posizioni centrali (i c.d. *gatekeepers*): interoperabilità, accesso equo, trasparenza.

Invero, l'architettura del Regolamento riflette l'esperienza applicativa maturata e le competenze specifiche acquisite dalle autorità di concorrenza. Lo strumento legislativo, difatti, impone alle piattaforme dotate di un significativo potere di mercato divieti e obblighi comportamentali che, in larga misura, discendono proprio dagli accertamenti istruttori condotti dalle autorità della Rete Europea della Concorrenza.

[61] Meta Platforms Inc., Meta Platforms Ireland Limited, WhatsApp Ireland Limited e Facebook Italy S.r.l.

[62] Cfr. provv. di avvio n. 31634 del 22 luglio 2025, A576 *Meta AI*, in *Boll.* n. 30/2025.

[63] Alphabet Inc., Google LLC e Google Italy S.r.l.

[64] Cfr. provv. n. 29645, del 27 aprile 2021, A529 *Google, Compatibilità App Enel X Italia con sistema Android Auto,* in *Boll.* n. 20/2021.

Anche in questa materia le interferenze con il diritto *antitrust* sono pertanto inevitabili. L'efficace applicazione del nuovo quadro regolamentare viene, tuttavia, garantita dal legislatore attraverso l'esplicito riconoscimento della sua complementarità con il diritto *antitrust*.

In particolare, il *Considerando n. 11* del Regolamento afferma che le norme *antitrust* proteggono interessi diversi da quelli protetti dalle norme del DMA e sono pertanto complementari e non sovrapponibili a queste. Su questa base, l'art. 1, par. 6 del DMA sancisce che il nuovo Regolamento non pregiudica l'applicazione degli articoli 101 e 102 TFUE, né delle norme nazionali di concorrenza.

In realtà, gli scopi dichiarati del Regolamento – equità e contendibilità dei mercati digitali – non possono ritenersi affatto estranei alle finalità *antitrust* tanto che, come detto, molti dei divieti introdotti dal DMA in capo ai *gatekeeper* coincidono con gli esiti di istruttorie *antitrust* concluse in precedenza dalle autorità nazionali. La scelta normativa è comunque chiara, nel senso della possibilità di applicazione cumulativa delle norme *antitrust* generali e di quelle del DMA, quest'ultime di competenza esclusiva della Commissione Europea.

Un valido esempio della virtuosa complementarità che può caratterizzare il rapporto tra la normativa *antitrust* e regolazione UE è rappresentato dal caso chiuso nei confronti di Booking[65]. L'istruttoria avviata per abuso di posizione dominante è stata chiusa con accoglimento degli impegni presentati dall'operatore del tutto coerenti con gli obblighi e i divieti previsti dal DMA in materia di clausole di parità dei prezzi.

Sul piano della cooperazione tra la Commissione e le Autorità nazionali di concorrenza, il sistema si ispira almeno in parte al Regolamento n 1/2003: l'articolo 37 stabilisce un obbligo permanente di collaborazione informativa tra la Commissione e gli Stati in applicazione del DMA, mentre l'art. 38 impone "*alle autorità nazionali competenti degli Stati membri*" di comunicare alla Commissione l'intento di avviare un procedimento contro un *gatekeeper* in base alle norme di concorrenza, ovvero di applicare una qualche misura a carico di un *gatekeeper*.

A riguardo, l'Autorità *Antitrust* ha adottato nel 2024 il Regolamento sulle forme di collaborazione e cooperazione ai sensi dell'articolo 18 della legge n. 214/2023, recante Misure per l'attuazione del DMA[66].

---

[65] Cfr. Provv. n. 31412 del 17 dicembre 2024, A558, *Booking / Programmi offerti alle strutture ricettive italiane e concorrenza tra le OTA*, in *Boll.* n. 49/2024.

[66] In forza dell'art. 18 della Legge annuale per il mercato la concorrenza, è noto che l'AGCM è l'Autorità designata per l'esecuzione del Regolamento (UE) 2022/1925 e lo

4. Considerazioni conclusive

Negli ultimi anni, al fine di garantire uno spazio unico digitale europeo e irrobustire le strutture fisiche della società digitale il legislatore europeo ha emanato una serie di atti normativi derivati, volti a disciplinare i vari aspetti della società digitale: dati, intelligenza artificiale e piattaforme. A tale proliferazione normativa si è inevitabilmente accompagnata la predisposizione di autorità tecniche di settore o, comunque, l'ampliamento dei poteri e delle funzioni delle autorità già esistenti.

Gli sviluppi legislativi intervenuti nel settore e tra questi in particolare l'adozione del DMA e del DSA hanno conferito nuova centralità al principio di leale collaborazione tra Autorità *Antitrust* e autorità di regolazione. Un rapporto sul quale molto è stato costruito nel tempo dalla prassi autoregolante delle stesse autorità coinvolte. Il pensiero va ai numerosi Protocolli di intesa sottoscritti dall'Autorità *Antitrust* – da ultimo, è stato firmato quello con il Garante Privacy[67] – che vanno ben oltre i termini della consultazione obbligatoria prevista nei settori regolati e sono una buona testimonianza della determinazione con cui viene ricercato e coltivato il confronto e la cooperazione inter-istituzionale.

In un quadro normativo complesso dove coesistono plessi normativi tra loro complementari e più autorità pubbliche operanti a diversi livelli, sembra pertanto ormai diffusa la consapevolezza che il coordinamento e la leale collaborazione siano essenziali per assicurare efficacia e deterrenza all'azione pubblica tutela dei diritti dei cittadini e equilibrio del sistema nel suo complesso.

stesso articolo dispone, al comma 2, che "*l'AGCM pone in essere tutte le forme di collaborazione e cooperazione previste dal citato regolamento (UE) 2022/1925, ivi inclusa l'assistenza nel corso delle ispezioni richieste dalla Commissione Europea, all'uopo adottando propri regolamenti compatibili con le procedure già previste in materia di concorrenza*".

[67] Il Protocollo è stato sottoscritto il 29 luglio 2025. L'obiettivo dell'accordo è quello di perseguire una più efficace azione delle due Autorità in ambiti attinenti alle rispettive sfere di attività e di interesse comune attraverso il coordinamento dei propri interventi in casi particolari in cui è rilevante il trattamento e l'utilizzo dei dati di carattere personale.

Autorità di regolazione dei trasporti e piattaforme digitali di mobilità: profili regolatori e prospettive di riforma. V*erso un nuovo modello di governance multilivello*

Federico Nespega[68]

L'emergere delle piattaforme digitali nei mercati della mobilità ha ridefinito i rapporti tra operatori tradizionali, intermediari globali e utenza, spostando il baricentro del potere economico dal controllo delle infrastrutture materiali al controllo di dati e interfacce. In questo contesto ibrido, l'Autorità di Regolazione dei Trasporti, nata per presidiare l'accesso equo e la concorrenza nei settori a rete, è oggi chiamata a confrontarsi con regole orizzontali europee – in particolare il Digital Markets Act (DMA) e il Digital Services Act (DSA) – e con nuove esigenze di tutela, trasparenza algoritmica e interoperabilità dei dati.

Il contributo: (i) ricostruisce il quadro normativo e i poteri dell'Autorità alla luce del diritto dei mercati digitali; (ii) analizza le principali frizioni concorrenziali e le ricadute sulla protezione dell'utenza, con particolare riguardo all'asimmetria regolatoria e all'apertura dei mercati MaaS; (iii) delinea linee di riforma e modelli di coordinamento inter-autorità per una governance multilivello capace di integrare la dimensione fisica e quella informativa della mobilità.

Il lavoro evidenzia che la sostenibilità giuridico-economica dell'ecosistema della mobilità digitale dipende da una regolazione sistemica e cooperativa, capace di coniugare apertura, interoperabilità e tutela effettiva degli utenti.

[68] Avvocato del Foro di Roma, Dottorando di Ricerca in Mercati, Impresa e Consumatori presso Università degli Studi Roma Tre.

1. Introduzione: piattaforme digitali e trasformazione dei mercati della mobilità

Negli ultimi anni, l'emergere delle piattaforme digitali nei mercati della mobilità ha determinato una trasformazione strutturale della morfologia dei sistemi di trasporto, incidendo non soltanto sugli equilibri concorrenziali, ma anche sugli assetti istituzionali e regolatori che ne presidiano il funzionamento. L'intermediazione algoritmica, la raccolta e l'elaborazione massiva dei dati, nonché la capacità di governare in tempo reale i flussi informativi, costituiscono oggi fattori determinanti di potere economico, ridefinendo la tradizionale dialettica tra vettori, gestori di infrastrutture e utenza finale.

Il paradigma infrastrutturale classico – incentrato su concessioni pubbliche, accessi regolati e meccanismi tariffari – si confronta con modelli nei quali la leva strategica non risiede più esclusivamente nel controllo materiale della rete, bensì nella disponibilità e nel governo delle interfacce digitali che strutturano l'incontro tra domanda e offerta di mobilità[69]. Le piattaforme digitali cessano così di essere meri strumenti di intermediazione e assumono la funzione di vere e proprie infrastrutture immateriali del mercato, capaci di incidere sull'accesso ai servizi, sulla visibilità degli operatori, sulla formazione algoritmica dei prezzi e, più in generale, sulle condizioni di contendibilità dei mercati della mobilità.

La trasformazione digitale della mobilità evidenzia quindi la progressiva crisi del modello di regolazione settoriale tradizionale, fondato sulla separazione tra infrastruttura materiale, servizio e intermediazione. Nei mercati della mobilità digitale, infatti, il potere economico tende a concentrarsi non soltanto nel controllo delle reti fisiche, ma soprattutto nella gestione dei dati, delle interfacce e degli ecosistemi informativi che organizzano l'accesso ai servizi. La piattaforma digitale, da semplice operatore economico, assume così la fisionomia di gatekeeper informazionale, in grado di orientare le dinamiche concorrenziali e le scelte dell'utenza ben prima della fase transazionale.

In questo contesto, il trasporto pubblico e privato assume progressivamente i tratti di un ecosistema digitale a rete multilivello e interconnesso, nel quale dimensione fisica e dimensione informativa risultano ormai inscindibili. Sicché la mobilità digitale si configura non soltanto come fenomeno tecnologico, ma come terreno di ridefinizione dei rapporti tra potere econo-

[69] Sulle piattaforme digitali come nuove "infrastrutture di mercato", v. M. Rizzolli, *Mercati digitali e regolazione economica*, Bologna, 2023, p. 45 ss.

mico privato, infrastrutture essenziali e funzione pubblica della regolazione.

L'Autorità di Regolazione dei Trasporti (ART), istituita per garantire l'accesso equo e non discriminatorio alle infrastrutture materiali e presidiare la concorrenza nei settori a rete, si trova oggi a operare all'interno di un perimetro regolatorio profondamente mutato. L'ambito di intervento non coincide più con la sola dimensione infrastrutturale tradizionale – ferroviaria, autostradale o del trasporto pubblico locale – ma si estende a servizi digitalmente intermediati, quali ride-hailing, car e bike sharing, piattaforme di micro-mobilità e architetture di Mobility as a Service (MaaS).

Tale mutamento non è meramente tecnologico, ma giuridico e istituzionale. Esso impone di ripensare il ruolo della regolazione economica nei mercati della mobilità e di interrogarsi sulla capacità degli strumenti tradizionali di garantire i principi di accesso equo e non discriminatorio, neutralità competitiva, proporzionalità degli oneri regolatori e tutela effettiva dell'utenza in mercati sempre più caratterizzati da asimmetrie informative, concentrazione dei dati e poteri algoritmici privati.

A complicare ulteriormente il quadro interviene la progressiva costruzione di un diritto europeo dei mercati digitali, fondato su discipline orizzontali – in particolare Digital Services Act (DSA) e Digital Markets Act (DMA) – che incidono trasversalmente anche sui servizi di mobilità digitale. In tale contesto, la regolazione della mobilità non può più essere ricondotta a compartimenti amministrativi stagni, ma si sviluppa all'interno di un sistema di strutturale interdipendenza tra discipline, autorità indipendenti e livelli di governo, nel quale la cooperazione regolatoria costituisce un elemento funzionale e permanente dell'*enforcement*.

L'obiettivo del presente contributo è proporre una lettura giuridico-economica sistemica della trasformazione in atto, analizzando le principali frizioni tra disciplina settoriale dei trasporti e diritto europeo dei mercati digitali, con particolare riguardo ai temi dell'asimmetria regolatoria, dell'interoperabilità dei dati e del coordinamento tra autorità indipendenti. Il lavoro si propone inoltre di delineare possibili linee evolutive verso un modello di governance multilivello e cooperativa della mobilità digitale, capace di integrare regolazione delle infrastrutture materiali, accesso ai dati e tutela concorrenziale.

La mobilità digitale invero costituisce un laboratorio paradigmatico della trasformazione del diritto pubblico dell'economia europeo, nel quale la regolazione non è più chiamata soltanto a disciplinare l'accesso alle infrastrutture fisiche, ma anche a governare l'accesso ai dati, alle interfacce e ai mercati informazionali che strutturano l'economia contemporanea delle piattaforme.

2. L'Autorità di Regolazione dei Trasporti: un regolatore settoriale nell'era delle piattaforme

L'Autorità di Regolazione dei Trasporti (ART) è stata istituita con Decreto-legge 6 dicembre 2011, n. 201 come autorità indipendente dotata di poteri regolatori e sanzionatori nei settori ferroviario, autostradale e del trasporto pubblico locale[70]. Il suo mandato originario si colloca nell'alveo del regulatory state classico[71], incentrato su strumenti di regolazione economica volti a garantire condizioni di concorrenza e accesso equo in mercati liberalizzati, ma caratterizzati da strutture oligopolistiche e dalla presenza di infrastrutture essenziali.

L'azione dell'Autorità si è articolata lungo tre direttrici principali:

(1) definizione di criteri e condizioni per l'accesso equo e non discriminatorio alle infrastrutture;
(2) disciplina dei diritti esclusivi e dei corrispettivi di accesso;
(3) vigilanza sugli assetti tariffari e sulla qualità dei servizi.

Si tratta di funzioni tipiche di un'autorità di regolazione settoriale, fondate su una chiara delimitazione del perimetro regolatorio e su una struttura di mercato centrata su operatori fisicamente insediati e su infrastrutture materiali – ferroviarie, autostradali o di trasporto pubblico locale – generalmente soggette a regimi concessori e a forme di controllo pubblico. Questo assetto ha consentito per oltre un decennio di presidiare i mercati della mobilità secondo logiche consolidate di accesso e controllo tariffario, con interventi prevalentemente ex ante e incentrati sulla rete fisica. Di fatto il rapporto tra infrastruttura e mercato appariva relativamente stabile: il controllo della rete coincideva, nella sostanza, con il controllo delle condizioni di accesso competitivo al mercato.

La progressiva affermazione delle piattaforme digitali della mobilità altera profondamente questo paradigma, sicché il modello, si trova oggi sottoposto a una pressione trasformativa senza precedenti.

I players non si limitano solo a facilitare l'incontro tra domanda e offerta, ma intervengono direttamente nella struttura concorrenziale dei mercati, organizzando algoritmicamente i servizi, definendo priorità distributive, selezionando gli operatori, orientando la visibilità delle offerte e in-

[70] Cfr. Decreto-legge 6 dicembre 2011, n. 201, convertito con modificazioni in legge 22 dicembre 2011, n. 214.

[71] Cfr. M. Thatcher, A. Stone Sweet, *The Politics of Delegation,* West European Politics, 2002; M. Levi-Faur, Regulatory Capitalism, Oxford University Press, 2005.

cidendo sulle modalità di formazione dei prezzi[72]. In altri termini, esse costituiscono nuove "infrastrutture immateriali" che si affiancano e, in parte, si sovrappongono a quelle materiali, tendendo ad assumere funzioni para-regolatorie ed esercitando un potere di mercato che non è (ancora) pienamente ricompreso nel perimetro regolatorio settoriale.

Esperienze recenti in segmenti contigui *(trasporto aereo Point-to-Point; logistica/ultimo miglio)* mostrano come il controllo del canale distributivo digitale possa accentuare fenomeni di chiusura e dipendenza da un unico intermediario, con riflessi sulla contendibilità dei mercati.

Appare subito chiaro il prodursi di effetti rilevanti sul ruolo e sulla funzione delle autorità indipendenti settoriali, tantoché l'autorità settoriale dei trasporti si trova a operare all'interno di mercati nei quali il potere economico tende progressivamente a spostarsi dalla dimensione materiale a quella informazionale, rendendo sempre meno netta la distinzione tra regolazione infrastrutturale, regolazione dei dati e disciplina della concorrenza.

Di fronte a questa evoluzione, le autorità di regolazione tradizionali rischiano di scivolare in una posizione marginale rispetto ai nuovi centri di potere economico e tecnologico, ove non siano poste nelle condizioni di adattare strumenti, finalità e modelli di intervento alla struttura dei mercati digitali.

La questione cruciale non consiste tanto (o non solo) nell'estendere formalmente le competenze dell'Autorità, quanto nel ripensarne la funzione sistemica: da regolatore dell'accesso fisico a garante di un ecosistema policentrico, in cui la mobilità fisica e quella digitale rappresentano due dimensioni inscindibili dello stesso mercato.

L'ambito di intervento dell'ART non coincide più con la sola dimensione infrastrutturale tradizionale – ferroviaria, autostradale o del trasporto pubblico locale – ma si estende progressivamente a servizi digitalmente intermediati, quali *ride-hailing*, *car* e *bike sharing*, piattaforme di micromobilità e architetture di *Mobility as a Service (MaaS)*, nelle quali dimensione fisica e dimensione informativa risultano strettamente integrate.

In questa prospettiva, la regolazione dei trasporti non può più essere confinata all'ambito infrastrutturale tradizionale, ma tende progressivamente a trasformarsi in una regolazione integrata capace di intervenire tanto sui nodi materiali quanto su quelli informativi, e di interagire con altre autorità e livelli di governo, in un contesto multilivello segnato da sovrapposizioni normative e interdipendenze istituzionali, garantendo così una più ampia governance cooperativa dei mercati digitali della mobilità.

[72] Sul potere delle piattaforme come "gatekeepers" nei settori regolati, v. G. COLANGELO, Piattaforme digitali e concorrenza, Torino, 2022.

3. Il diritto europeo dei mercati digitali e la mobilità come settore ibrido

A complicare ulteriormente il quadro regolatorio, si inserisce il più ampio e progressivo sviluppo di un diritto europeo dei mercati digitali, caratterizzato da discipline orizzontali che operano trasversalmente rispetto ai settori economici tradizionali. L'adozione del Digital Services Act e del Digital Markets Act segna l'ingresso di un modello di regolazione preventiva e strutturale, fondato su obblighi ex ante per le piattaforme digitali, con l'obiettivo di assicurare contendibilità, trasparenza e corretto funzionamento dei mercati digitali.

Si tratta di discipline che non regolano direttamente il settore dei trasporti, ma che incidono in modo significativo anche sui servizi di mobilità digitalmente intermediati, in ragione della funzione svolta dalle piattaforme quali snodi essenziali dell'accesso al mercato. Proprio la natura "orizzontale" del diritto europeo dei mercati digitali contribuisce a ridefinire il rapporto tra regolazione settoriale e regolazione generale, imponendo un progressivo superamento della tradizionale separazione tra infrastruttura fisica, servizio e intermediazione digitale.

Basta appena ricordare che il *DMA* assume una particolare rilevanza sistemica, introducendo infatti obblighi specifici per i cosiddetti *gatekeepers*, imponendo regole in materia di interoperabilità, portabilità dei dati, neutralità delle interfacce e divieto di *self-preferencing*. L'accesso competitivo ai mercati della mobilità non dipende più esclusivamente dalla disponibilità di infrastrutture fisiche, ma anche – e sempre più – dalla possibilità di accedere ai dati, alle API, ai sistemi di prenotazione, alle informazioni sui flussi di utenza e agli ecosistemi digitali attraverso i quali la domanda viene organizzata e indirizzata.

In tale contesto, gli obblighi di interoperabilità previsti dal DMA, se correttamente implementati, possono incidere direttamente sulla contendibilità dei mercati MaaS, favorendo l'apertura degli ecosistemi digitali, la riduzione delle barriere all'ingresso e la possibilità per operatori terzi di competere in condizioni eque e non discriminatorie[73].

Parallelamente, il DSA provvede ad imporre obblighi di trasparenza e accountability algoritmica che assumono particolare rilievo nei servizi di mobilità digitalmente intermediati per mitigare la possibilità che possa esservi una compressione di libertà di scelta dei consumatori e di concorren-

[73] Ove invece il controllo delle interfacce e dei dati poteva sempre determinare effetti escludenti analoghi a quelli tradizionalmente associati al controllo delle infrastrutture essenziali.

ziale del mercato.

La governance algoritmica della mobilità si traduce così in una nuova forma di potere economico privato, esercitato attraverso il controllo delle informazioni e delle modalità di accesso ai servizi, con effetti che trascendono la dimensione puramente tecnologica e investono direttamente la struttura concorrenziale dei mercati della mobilità.

Suddetta trasformazione pone problemi inediti anche sul piano istituzionale, imponendo un coordinamento stabile tra diritto della concorrenza, regolazione economica, tutela dei dati personali, disciplina delle piattaforme digitali e protezione dei consumatori.

Affinché tali potenzialità possano tradursi in risultati effettivi, è tuttavia necessario evitare fenomeni di sovrapposizione, frammentazione o vuoti regolatori. Ciò impone un raccordo organico disciplina digitale europea e disciplina settoriale nazionale, in cui l'Autorità di Regolazione dei Trasporti possa assumere una funzione di raccordo sistemico tra regolazione delle infrastrutture materiali e governo delle piattaforme digitali della mobilità[74].

4. Asimmetria regolatoria e interoperabilità dei dati: il nodo concorrenziale e la tutela dell'utenza

Una delle principali criticità che emergono nel confronto tra disciplina settoriale dei trasporti e diritto europeo dei mercati digitali concerne la crescente asimmetria regolatoria tra operatori tradizionali e piattaforme digitali[75]. Gli operatori storici restano assoggettati a un sistema articolato di vincoli autorizzativi, concessori e tariffari, espressione della natura pubblicistica delle infrastrutture e dell'interesse generale connesso alla loro gestione. Le piattaforme digitali, al contrario, operano frequentemente all'interno di un perimetro regolatorio meno vincolato, pur esercitando un potere di mercato e di organizzazione dell'offerta spesso superiore a quello dei soggetti tradizionalmente regolati.

L'asimmetria regolatoria non consiste soltanto nella differente intensità degli obblighi gravanti sugli operatori economici, ma nel progressivo

[74] La regolazione economica della mobilità non potrà più limitarsi al presidio delle reti fisiche, ma dovrà estendersi alla governance degli accessi digitali e alla gestione dei dati come leva competitiva e strategica.

[75] Sull'asimmetria regolatoria nei mercati digitali si veda, tra gli altri, F. Cafaggi, Regolazione e concorrenza nell'economia delle piattaforme, in Mercato concorrenza regole, 2022, p. 327 ss.

disallineamento tra concentrazione del potere economico e livello di regolazione applicabile. Mentre i vettori tradizionali operano entro schemi giuridici rigidamente definiti, le piattaforme digitali beneficiano di ampi margini di autonomia strategica, potendo sfruttare economie di rete, controllo esclusivo dei dati e capacità di organizzare algoritmicamente l'incontro tra domanda e offerta. Tale configurazione incide direttamente sui principi di concorrenza effettiva e neutralità competitiva, alterando le condizioni di contendibilità dei mercati della mobilità.

La posizione di *gatekeeper* informazionale assunta da determinati operatori digitali consente infatti di influenzare a monte la dinamica concorrenziale, incidendo sull'accesso al mercato, sulla visibilità degli operatori terzi e sulla stessa organizzazione della domanda. Il controllo delle interfacce digitali e dei flussi informativi può produrre effetti di chiusura, integrazione verticale e segmentazione artificiale del mercato, ponendo questioni che si collocano al crocevia tra abuso di posizione dominante ex art. 102 TFUE e regolazione settoriale ex ante.

In questo quadro, la piena realizzazione di ecosistemi di Mobility as a Service aperti e competitivi presuppone un elevato livello di interoperabilità dei dati, non soltanto sul piano tecnico ma anche – e soprattutto – su quello giuridico-regolatorio[76]. Gli standard comuni e le condizioni di accesso alle informazioni essenziali – orari, disponibilità dei mezzi, tariffe, flussi di utenza – costituiscono infatti una "infrastruttura immateriale essenziale" ai fini della contendibilità dei mercati. In assenza di norme vincolanti e di meccanismi efficaci di *enforcement*, l'interoperabilità rischia di ridursi a un principio meramente programmatico, incapace di prevenire fenomeni di chiusura, integrazione verticale e controllo esclusivo dei canali distributivi da parte di pochi operatori dominanti.

L'Autorità di Regolazione dei Trasporti è dunque chiamata a superare ogni residua neutralità rispetto all'organizzazione dei servizi digitali di intermediazione, assumendo un ruolo proattivo e sistemico nella definizione e nell'attuazione delle regole sull'accesso ai dati, alle API e alle interfacce digitali.

Tali regole devono essere costruite nel rispetto dei principi di proporzionalità, trasparenza e non discriminazione, nonché in coerenza con gli obblighi previsti dal Digital Markets Act e con il quadro costituzionale e unionale che presidia la libertà di concorrenza (artt. 41 e 117 Cost.; artt.

[76] Sulla rilevanza dell'interoperabilità nei servizi di mobilità digitale, v. Commissione europea, Data Strategy, COM(2020) 66 final, e Sustainable and Smart Mobility Strategy, COM(2020) 789 final.

101-102 TFUE). Sul piano della tutela dell'utenza, ciò si traduce in trasparenza dei sistemi di raccomandazione, chiara evidenza di *sponsorship*, *surcharge* e commissioni che incidono sulla comparazione delle offerte, nonché nel *pass-through* dei diritti (rimborsi e indennizzi) lungo gli itinerari intermodali acquistati tramite piattaforma.

La regolazione dell'accesso informazionale diviene così il naturale completamento della regolazione dell'accesso infrastrutturale tradizionale, segnando il passaggio da un modello di governo delle reti materiali a una forma di governance dei mercati digitali della mobilità. In un ecosistema sempre più ibrido e data-driven, la tutela della concorrenza e dell'utenza dipende ormai dalla capacità della regolazione di presidiare non soltanto le infrastrutture fisiche, ma anche i dati, le interfacce e gli ecosistemi informativi che strutturano l'economia contemporanea delle piattaforme.

5. Coordinamento tra autorità indipendenti: verso una governance cooperativa e il principio di leale cooperazione

La trasformazione digitale dei mercati non comporta soltanto un ampliamento degli spazi economici oggetto di regolazio

ne, ma determina anche una progressiva moltiplicazione e sovrapposizione dei centri regolatori, con conseguenti problemi di frammentazione istituzionale, incertezza applicativa ed effettività dell'*enforcement*. La stratificazione normativa europea – General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), AI Act e disciplina consumeristica – ha dato vita a un mosaico regolatorio policentrico, nel quale più amministrazioni risultano contemporaneamente legittimate a intervenire, spesso in assenza di criteri di riparto pienamente definiti e di meccanismi strutturati di coordinamento.

Anche nel settore della mobilità, l'intervento dell'Autorità di Regolazione dei Trasporti si intreccia con quello di altre autorità indipendenti, ciascuna titolare di competenze funzionali specifiche:

– l'Autorità Garante della Concorrenza e del Mercato, per i profili concorrenziali e antitrust;
– l'Autorità per le Garanzie nelle Comunicazioni, per la disciplina delle interfacce digitali e delle comunicazioni elettroniche;
– l'Autorità di Regolazione per Energia Reti e Ambiente, per le interconnessioni infrastrutturali e i servizi intermodali;
– il Garante per la protezione dei dati personali, per la dimensione data-driven dei servizi di mobilità.

La pluralità di centri regolatori non rappresenta un fenomeno patologico o contingente, ma costituisce un elemento strutturale dei mercati digitali contemporanei. La medesima piattaforma può infatti porre simultaneamente questioni di concorrenza, trasparenza algoritmica, protezione dei dati personali, interoperabilità infrastrutturale e tutela dei consumatori, rendendo inevitabile l'interazione tra discipline e autorità differenti.

Trova ingresso in questa sede opportunamente il consolidato principio di leale cooperazione amministrativa – sancito dall'art. 97 Cost. e dall'art. 4 TUE – assume un ruolo centrale, configurandosi quale fondamento costituzionale e unionale di un'azione regolatoria coerente, proporzionata e integrata. Tale principio impone alle autorità coinvolte di attivare forme di cooperazione stabile e non meramente occasionale, idonee a prevenire conflitti di competenza, evitare duplicazioni istruttorie e garantire certezza regolatoria agli operatori economici.

Ed ancora la giurisprudenza amministrativa e unionale ha progressivamente chiarito la portata sistemica di tale esigenza. Il Consiglio di Stato, con la sentenza n. 497/2024 (caso Telepass), ha affermato che l'assenza di interlocuzione tra autorità competenti può integrare un vizio procedimentale rilevante, evidenziando come la frammentazione dell'*enforcement* rischi di compromettere la coerenza dell'azione amministrativa. Parallelamente, la Corte di giustizia dell'Unione europea, nella pronuncia Meta Platforms Inc. (C-252/21)[77], ha riconosciuto la necessità di un *enforcement* coordinato tra diritto antitrust e tutela dei dati personali, chiarendo che il trattamento dei dati costituisce un elemento strutturale del potere economico delle piattaforme digitali.

Questi precedenti tracciano un percorso chiaro, tale per cui nei mercati digitali non è più possibile operare in compartimenti stagni. Il coordinamento tra autorità non è un'opzione organizzativa, ma un requisito funzionale e strutturale dell'azione regolatoria. Tale logica deve essere trasposta in modo sistematico anche nel settore della mobilità, dove la frammentazione istituzionale rischia di compromettere lo sviluppo di modelli di trasporto integrati e interoperabili, moltiplicando i costi di coordinamento e riducendo la certezza delle regole.

Il problema assume anche una dimensione propriamente regolatoria. La proliferazione delle sedi di confronto e dei meccanismi di raccordo inter-istituzionale comporta infatti costi amministrativi crescenti, che incidono tanto sull'efficienza dell'*enforcement* quanto sulla certezza del quadro

[77] Cfr. Corte di giustizia dell'Unione europea, 4 luglio 2023, C-252/21, Meta Platforms Inc. e altri.

normativo per gli operatori economici. La qualità della regolazione non dipende più soltanto dal contenuto delle norme, ma anche dalla capacità delle istituzioni di coordinare efficacemente l'esercizio delle rispettive competenze all'interno di mercati caratterizzati da elevata interdipendenza tecnologica e normativa.

Una governance cooperativa, fondata su meccanismi di dialogo strutturato, scambio informativo e co-decisione regolatoria, rappresenta quindi una condizione imprescindibile per un sistema efficace e coerente di vigilanza sui mercati della mobilità digitale. L'istituzionalizzazione di forme permanenti di cooperazione inter-autorità – ad esempio mediante la creazione di un Forum nazionale per la mobilità digitale – consentirebbe di tradurre il principio di leale cooperazione in una prassi amministrativa stabile e prevedibile, rafforzando al contempo la certezza giuridica per gli operatori economici.

Esigenza confermata e strettamente collegata anche al principio di buona amministrazione sancito dall'art. 41 della Carta dei diritti fondamentali dell'Unione europea, che impone alle autorità pubbliche di agire in modo trasparente, prevedibile e coordinato. Nei mercati digitali della mobilità, la cooperazione inter-istituzionale diviene pertanto non soltanto uno strumento organizzativo, ma una componente essenziale della stessa legittimità e sostenibilità dell'azione regolatoria.

6. Prospettive di riforma: una Better Regulation per la mobilità digitale

La costruzione di una governance regolatoria adeguata alla complessità dei mercati digitali della mobilità non può esaurirsi in interventi settoriali isolati o in meri adattamenti incrementali degli strumenti esistenti. Essa richiede un ripensamento sistemico dell'architettura normativa e istituzionale, capace di assicurare un equilibrio coerente tra concorrenza, tutela dell'utenza, interoperabilità delle infrastrutture e sostenibilità dell'*enforcement* pubblico.

L'obiettivo non consiste nell'ampliare meccanicamente le competenze delle singole autorità indipendenti, ma nel definire un modello multilivello di regolazione cooperativa, idoneo a prevenire conflitti istituzionali, ridurre i costi di coordinamento amministrativo e garantire prevedibilità e certezza giuridica agli operatori economici. Tanto è vero che nei mercati digitali della mobilità la qualità della regolazione dipende sempre meno dalla mera produzione normativa e sempre più dalla capacità delle istituzioni di coordinare efficacemente l'esercizio delle rispettive funzioni.

Questo processo di riforma si articola su due piani strettamente connessi.

(i) A monte, nella fase di disegno dell'architettura regolatoria, è necessario introdurre strumenti strutturati di valutazione ex ante dei costi di coordinamento inter-amministrativo, secondo la logica della Better Regulation Agenda 2.0[78]. La qualità della regolazione non può essere misurata solo in termini di oneri per gli operatori, ma deve considerare la capacità amministrativa di *enforcement*, la prevedibilità delle interazioni istituzionali e la coerenza complessiva dell'azione pubblica. Nei mercati caratterizzati da sovrapposizione di competenze e pluralità di fonti normative, la qualità della regolazione coincide sempre più con la qualità del coordinamento istituzionale, da attuarsi secondo i principi di proporzionalità, coerenza e certezza regolatoria.

(ii) A valle, è necessario procedere all'istituzionalizzazione di forme stabili e non occasionali di cooperazione inter-autorità. Una soluzione praticabile è la creazione di un Forum permanente per la mobilità digitale, sul modello del Digital Regulation Cooperation Forum britannico. Tale organismo, riunendo l'Autorità di Regolazione dei Trasporti, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali, consentirebbe di definire linee interpretative comuni, condividere informazioni istruttorie, coordinare l'*enforcement* e garantire uniformità applicativa senza necessità di un accentramento formale delle competenze. In tal modo, la cooperazione inter-autorità cesserebbe di essere un rimedio contingente e diverrebbe parte integrante e permanente dell'azione regolatoria, in attuazione del principio di leale cooperazione amministrativa che informa sia l'ordinamento nazionale (art. 97 Cost.) sia quello europeo (art. 4 TUE).

Un ulteriore asse strategico di riforma riguarda la definizione di standard giuridici e tecnici vincolanti per l'interoperabilità dei dati di mobilità, intesa come condizione regolatoria di accesso al mercato per le piattaforme digitali. L'interoperabilità – prevista e rafforzata dal Digital Markets Act e dal diritto UE in materia di servizi digitali e infrastrutture – rappresenta una leva per riequilibrare l'asimmetria regolatoria oggi esistente, garantendo pluralismo competitivo, apertura dei mercati e tutela effettiva

[78] Cfr. Commissione europea, Better Regulation: Joining forces to make better laws, COM(2021) 219 final.

dell'utenza. Essa non costituisce un mero requisito tecnico, ma un principio ordinatore dell'ecosistema regolatorio, da cui dipendono la contendibilità dei mercati, la trasparenza degli algoritmi, la possibilità per nuovi operatori di entrare e la libertà di scelta per i consumatori[79].

L'attuazione di questo modello richiede strumenti operativi coerenti: sandbox regolatorie, valutazioni ex post degli effetti concorrenziali, regole uniformi per l'accesso ai dati e meccanismi procedimentali coordinati tra le autorità competenti.

Nel complesso, tali direttrici delineano un modello di regolazione multilivello, cooperativo e interoperabile, in grado di coniugare efficienza amministrativa, apertura dei mercati e tutela dell'interesse generale, nel rispetto del principio – di matrice costituzionale e unionale – della libertà di concorrenza (artt. 41 e 117 Cost.; artt. 101-102 TFUE). In questa prospettiva, la regolazione non è chiamata soltanto a governare l'innovazione tecnologica, ma a orientarla verso assetti di mercato aperti, trasparenti e contendibili, coerenti con la funzione pubblica e sistemica dei servizi di mobilità nell'economia digitale contemporanea.

7. Conclusioni. Verso una nuova stagione della regolazione dei trasporti

La transizione verso sistemi di mobilità digitale non rappresenta un mero fenomeno tecnologico, ma una sfida strutturale per il diritto pubblico dell'economia e per i modelli tradizionali di regolazione settoriale. L'accesso ai mercati non è più determinato esclusivamente dal controllo delle infrastrutture materiali, ma sempre più dal potere di governare interfacce digitali, flussi informativi e dati; questi elemento sembrano capaci di definire le dinamiche concorrenziali e sulle scelte degli utenti.

Per affrontare questa trasformazione, l'Autorità di Regolazione dei Trasporti è chiamata a superare la logica infrastrutturale tradizionale e ad assumere un ruolo strategico nella garanzia dell'accesso equo, trasparente e interoperabile alle infrastrutture immateriali della mobilità.

[79] In tal senso, particolare rilievo assume lo sviluppo di sistemi di bigliettazione elettronica integrata e di servizi di sharing interoperabili quali nodi essenziali degli ecosistemi MaaS. (*Bigliettazione elettronica integrata e sharing come nodi MaaS. Adozione di standard vincolanti per emissione, riconoscimento e validazione cross-provider dei titoli; API aperte per disponibilità, prenotazione e pricing di car/bike sharing; divieto di esclusive che ostacolino multi-homing e aggregazione multi-app; regole chiare su rimborsi/indennizzi e integrazione tariffaria lungo l'intero percorso intermodale*).

Ciò implica un'azione non isolata, ma pienamente integrata in una rete stabile di cooperazione inter-autorità, in cui i profili concorrenziali, di tutela dei dati, di interoperabilità e di accesso siano affrontati in modo coerente e sistemico.

Una simile trasformazione non può essere affrontata mediante strumenti regolatori isolati o secondo logiche amministrative verticali. Al contrario, sono decisamente richieste forme stabili di cooperazione inter-istituzionale, capaci di integrare in modo coerente profili concorrenziali, tutela dei dati personali, interoperabilità tecnologica, protezione dei consumatori e regolazione economica dei servizi. Nei mercati digitali della mobilità, il coordinamento tra autorità indipendenti non costituisce più un rimedio eccezionale a fenomeni di sovrapposizione normativa, ma rappresenta una componente strutturale e permanente dell'*enforcement* regolatorio.

Parallelamente, anche il legislatore nazionale ed europeo sarà chiamato a calibrare con maggiore precisione la produzione normativa, riducendo frammentazioni, duplicazioni e costi di coordinamento derivanti dalla proliferazione delle competenze e delle discipline applicabili. La qualità della regolazione dipenderà sempre più dalla capacità di costruire meccanismi multilivello di governance, idonei a coniugare specializzazione tecnica, coerenza sistemica e certezza giuridica, in attuazione del principio di leale cooperazione amministrativa (art. 97 Cost.; art. 4 TUE) e del principio di buona amministrazione sancito dall'art. 41 della Carta dei diritti fondamentali dell'Unione europea.

Il settore della mobilità costituisce un laboratorio paradigmatico per sperimentare nuovi assetti regolatori: come avvenuto per le telecomunicazioni e i servizi digitali, può divenire terreno di consolidamento di una governance cooperativa e interoperabile, nella quale la cooperazione inter-autorità cessa di essere un rimedio praeter legem e si afferma come architrave dell'azione regolatoria.

La regolazione della mobilità digitale non si esaurisce dunque in una questione tecnica o settoriale, ma investe direttamente la capacità del diritto pubblico dell'economia di governare l'economia contemporanea delle piattaforme. La costruzione di un equilibrio sostenibile tra infrastrutture materiali e infrastrutture informazionali costituisce oggi una delle principali sfide sistemiche del modello regolatorio europeo, dalla quale dipendono la tutela della concorrenza, la trasparenza dei mercati, la libertà di scelta dei consumatori e l'effettività dell'azione pubblica nell'economia digitale.

A tutto dire, la mobilità digitale si configura pertanto come un banco di prova privilegiato per misurare la futura capacità della regolazione europea di adattarsi ai processi di trasformazione dell'economia delle piat-

taforme, superando definitivamente il paradigma verticale della regolazione settoriale e orientandosi verso un modello di governance multilivello, cooperativo e integrato.

Piattaforme digitali e diritti dei consumatori. Il ruolo di Arera

Cristiana Lauri

Il contributo analizza l'impatto delle piattaforme digitali nei settori regolati dall'Autorità di Regolazione per Energia Reti e Ambiente, con particolare riferimento ai processi di digitalizzazione, agli obblighi per gli operatori e al rafforzamento delle tutele consumeristiche. Viene approfondito il ruolo delle piattaforme come strumenti di trasparenza, fiducia e semplificazione amministrativa, nonché le sfide poste dall'uso dell'intelligenza artificiale nei processi regolatori. L'analisi mette in luce l'evoluzione dell'azione di ARERA verso un modello regolatorio fondato su trasparenza, tracciabilità e centralità del consumatore.

1. Piattaforme e mercati regolati da Arera: lo stato dell'arte

Il grado di incidenza del fenomeno dell'irruzione delle piattaforme tecnologiche nei mercati regolati da ARERA si è sviluppato negli ultimi anni a diverse velocità. La ragione, è evidente, si può rintracciare osservando il lascito di un disomogeneo livello di sviluppo dei mercati e del relativo sistema di regolazione fondato su apparati settoriali e a lungo tra loro non comunicanti.

Per i settori dell'energia elettrica e del gas, l'introduzione e l'implementazione di soluzioni tecnologiche avanzate sono state accompagnate da un quadro normativo europeo sviluppatosi negli anni: la Direttiva 2006/32/CE sull'efficienza energetica e il successivo recepimento del cosiddetto Terzo Pacchetto Energia hanno imposto agli Stati membri l'obbligo di promuovere la diffusione di sistemi di misurazione intelligenti, al fine di incentivare la partecipazione attiva dei consumatori ai mercati energetici e favorire lo sviluppo di servizi basati sui dati raccolti tramite tali di-

spositivi. Più recentemente, la Direttiva (UE) 2019/944, ("Direttiva Energia") ha ridefinito le condizioni per la diffusione dei contatori intelligenti nel settore dell'energia elettrica, subordinandole ai risultati delle analisi costi-benefici.

Con riferimento al servizio di fornitura del gas, il d.lgs. 4 luglio 2014, n. 102 ha recepito la Direttiva Europea 2012/27/UE in materia di efficienza energetica, stabilendo principi e obblighi finalizzati a migliorare le prestazioni energetiche del Paese e a promuovere un uso più razionale ed efficiente delle risorse disponibili.

A livello europeo il Regolamento (UE) 2019/943 e la Direttiva (UE) 2019/944 hanno condotto al "Clean Energy Package" che ha promosso fortemente la digitalizzazione attraverso gli obiettivi di implementazione delle *smart grids* e dei sistemi di gestione intelligenti[80].

A differenza dei settori dell'energia e del gas, quello del sistema idrico non è stato oggetto di un impianto normativo esteso e coerente né di una regolazione tale da imporre l'adozione o l'implementazione di soluzioni tecnologiche. Gli sviluppi di settore sono ancora largamente rimessi alle sperimentazioni di mercato.

Il settore dei rifiuti gode di alcune peculiarità che rendono il processo di digitalizzazione del settore ancor più delicato, soprattutto alla luce della forte differenziazione nei costi del servizio, ai notevoli squilibri in termini di qualità dello stesso e, non ultimo, per i significativi livelli di morosità che lo caratterizzano a causa dell'impossibilità di adottare misure di contrasto efficaci come la sospensione.

Non da ultimo, ancora in divenire è il sistema di regole relativo ai servizi di teleriscaldamento e teleraffrescamento, dove le esigenze richieste dalle caratteristiche tecniche degli impianti e le particolarità delle tecnologie implementate, nonchè la relativa novità dell'ambito in punto regolatorio, configurano i contorni di mercati ancora limitati.

Ma la riflessione sull'erompere delle piattaforme in tali settori non si arresta alle soluzioni introdotte per innovare i prodotti e i servizi e il loro funzionamento. Piattaforme aventi una rilevanza essenziale per il settore sono anche quelle a servizio del buon funzionamento del mercato in sè in quanto serventi a garantire un rapporto equilibrato tra operatori economici e consumatori, nell'ambito di un sistema giuridico globale che si va ristrutturando anche nel suo impianto di principi. Vi rientrano tutti gli strumenti che la transizione digitale ha inteso valorizzare nell'ambito dell'Agenda di-

[80] Recentemente, sulla digitalizzazione del settore energetico, v. M. Tresca, *La trasformazione digitale del settore energetico: strumenti di regolazione e nuovi attori*, in Diritto Costituzionale. Rivista Quadrimestrale, n. 2, 2022, p. 199.

gitale UE, come ad esempio le anagrafi digitali, il sistema SPID, gli elenchi sottoposti a controllo delle Autorità di regolazione.

Si inserisce in tale quadro anche un conseguente riflesso sul piano comunicativo, vera e propria leva strategica dell'azione regolatoria. Ciò è dimostrato dall'attività istituzionale svolta dalla stessa ARERA da questo punto di vista. Ne sono esempio gli account sulle piattaforme social (tutorial sul canale YouTube dell'Autorità), le campagne informative televisive, radiofoniche e approfondimenti giornalistici (tra cui campagne condivise con altre Autorità, come ad esempio quella realizzata con AGCM per difendere dai *call center* aggressivi), tese ad accompagnare i cittadini e le imprese nei momenti di svolta regolatoria e assicurare diffusione e trasparenza delle informazioni (tra le più recenti: Nuova Bolletta e Scontrino dell'Energia), anche avendo riguardo ai *target* – quanto a temi e localizzazione – delle singole azioni regolatorie.

ARERA, nella presente stagione storica, supera la logica *top-down* nel passaggio delle informazioni e diviene un "attore istituzionale consapevole" (come si legge nella Relazione 2025) "capace di ascoltare la società e leggere il contesto, mediare tra spinte diverse, e offrire una direzione chiara in una fase di transizione".

2. Gli obblighi per gli operatori

L'elevazione a principio della fiducia tra operatori economici del mercato e consumatori – privati, ma anche pubblici – è uno dei capisaldi su cui sviluppare sistemi di regole funzionanti nell'ambito di un mercato che si sviluppa su piattaforme interconnesse.

Molteplici sono gli esempi.

Tra di essi figura l'aggiornamento del Regolamento UE n. 1227/2011 sull'integrità e la trasparenza dei mercati energetici all'ingrosso - REMIT (*Regulation on Wholesale Energy Market Integrity and Transparency*), cui è stata data attuazione in Italia con la legge 30 ottobre 2014, n. 161/2014, successivamente modificato con il Regolamento UE n. 1106/2024 in data 11 aprile 2024 (in vigore dal 7 maggio 2024) "per quanto riguarda il miglioramento della protezione dell'Unione dalla manipolazione del mercato nel mercato dell'energia all'ingrosso".

Il Regolamento dispone un allineamento delle norme dell'UE sulla trasparenza e l'integrità dei mercati dell'energia con quelle applicabili nei mercati finanziari, estendendo il perimetro applicativo relativo ai divieti di *insider trading* (cfr. art. 3) e di manipolazione di mercato (cfr. art. 5) del pre-

cedente Regolamento UE n. 1227/2011 ai prodotti energetici all'ingrosso che sono anche strumenti finanziari.

Il Regolamento REMIT mira a "promuovere una concorrenza aperta e leale sui mercati dell'energia all'ingrosso a beneficio dei consumatori finali". Come viene precisato nel primo Considerato del Regolamento UE n. 1227/2011 "è importante assicurare che i consumatori e altri soggetti del mercato possano nutrire fiducia nell'integrità dei mercati dell'elettricità e del gas, che i prezzi fissati sui mercati dell'energia all'ingrosso riflettano un'interazione equa e concorrenziale tra domanda e offerta e che non sia possibile trarre profitto dagli abusi di mercato". A tal proposito, il Regolamento UE n. 1106/2024 è intervenuto al fine di "rafforzare la fiducia dei cittadini nel funzionamento dei mercati dell'energia all'ingrosso e proteggere efficacemente l'Unione dagli abusi di mercato" attraverso modifiche al Regolamento (UE) n. 1227/2011 "per garantire ulteriore trasparenza e aumentare le capacità di monitoraggio, contribuendo in tal modo alla stabilizzazione dei prezzi dell'energia e alla protezione dei consumatori, nonché per garantire indagini e azioni di contrasto più efficaci nei casi di potenziale abuso di mercato colmando le carenze individuate nel quadro attuale".

In particolare, REMIT introduce regole specifiche volte a: definire le pratiche abusive, relativamente a manipolazione (o tentata manipolazione) di mercato e *insider trading*; identificare e contrastare i casi di manipolazione (o tentata manipolazione) di mercato e di insider trading attraverso un sistema di monitoraggio dei mercati energetici europei; vietare le suddette pratiche abusive nei mercati dell'energia (elettricità e gas) all'ingrosso; imporre agli operatori di mercato di pubblicare le "informazioni privilegiate" in loro possesso; adottare le opportune iniziative di verifica e controllo prevedendo che le Autorità nazionali di regolazione (e ACER in alcuni casi) dispongano di specifici poteri di indagine, *enforcement* e sanzione. Impone inoltre alle "persone che predispongono o eseguono operazioni a titolo professionale" di segnalare all'ACER e all'Autorità nazionale di regolazione (in Italia, ARERA) le transazioni sospette che vengono identificate.

REMIT, in questa prospettiva, introduce specifici obblighi.

L'art. 9 REMIT prevede che gli operatori di mercato che concludono transazioni che devono essere segnalate all'ACER (a norma dell'articolo 8, comma 1), siano tenuti alla registrazione presso l'autorità nazionale di regolazione dello Stato membro in cui sono stabiliti o sono residenti. L'Autorità ha sviluppato il Registro nazionale degli operatori di mercato ai sensi della deliberazione 5 marzo 2015, 86/2015/E/com, a cui gli operatori già accreditati presso l'Anagrafica Operatori possono accedere utilizzando le medesime credenziali.

Vi è poi un obbligo, ai sensi dell'art. 4, di pubblicazione delle informazioni privilegiate ("un'informazione che ha carattere preciso, che non è stata resa pubblica, che concerne, direttamente o indirettamente, uno o più prodotti energetici all'ingrosso e che, se resa pubblica, potrebbe verosimilmente influire in modo sensibile sui prezzi di tali prodotti", ai sensi dell'art. 2). Gli operatori di mercato sono tenuti a rendere pubbliche le informazioni privilegiate che detengono tramite le *Inside Information Platform*. La divulgazione deve quindi essere effettuata in modo da garantire la pubblicità, l'effettività e l'efficacia della stessa. Deve svolgersi in maniera tempestiva, simultanea e integrale. Le *Inside Information Platform* garantiscono che le informazioni privilegiate siano rese pubbliche secondo modalità che consentano un accesso immediato a tali informazioni, anche attraverso un sito web o un'interfaccia chiara di programmazione delle applicazioni, e una valutazione completa, corretta e tempestiva di tali informazioni da parte del pubblico.

L'obbligo di essere autorizzati come piattaforma di informazioni privilegiate (ai sensi dell'articolo 4) si applica alle persone che intendono gestire una piattaforma per la divulgazione di informazioni privilegiate.

L'articolo 5 prevede inoltre che l'operatore di mercato che effettua negoziazione algoritmica in uno Stato membro lo notifichi all'Autorità nazionale di regolazione dello Stato membro in cui è registrato a norma dell'art. 9, comma 1, e all'ACER.

Anche l'operatore di mercato che fornisce accesso elettronico diretto a un mercato organizzato (OMP) è sottoposto al medesimo obbligo di notifica.

Il Regolamento attribuisce alle Autorità nazionali di regolazione il compito di vigilare sul rispetto del regolamento e a tal fine, di cooperare con l'ACER all'attività di monitoraggio dei mercati energetici all'ingrosso e, in alcuni casi specifici, alle azioni di *enforcement* svolte dalla stessa ACER.

Il coinvolgimento riguarda anche soggetti operanti sul piano nazionale, nello specifico: il Gestore dei mercati energetici (GME) e il Gestore della rete elettrica di trasmissione nazionale (Terna); l'AGCM, per il coordinamento nello svolgimento di indagini relative a casi di sospetta violazione dei divieti di manipolazione del mercato e di insider trading e/o per l'attuazione dell'obbligo di pubblicazione di informazioni privilegiate; la CONSOB con riferimento al coordinamento nello svolgimento di indagini relative a casi di sospetta violazione del divieto di *insider trading*.

3. Le tutele consumeristiche: il telemarketing e la qualità dei servizi

Due provvedimenti adottati negli ultimi mesi hanno contribuito a potenziare il sistema di tutele per i consumatori nel contesto delle evoluzioni di mercati che sviluppano le transazioni più rilevanti attraverso piattaforme.

La delibera 395/2024/R/COM ha rappresentato un ulteriore tassello di novità nell'ambito dei tavoli di confronto sul superamento delle tutele di prezzo di ARERA con le Associazioni dei consumatori.

La sua introduzione risponde all'esigenza di potenziare le tutele per i clienti in un mercato in cui in tempi recenti numerosi contratti di energia e gas sono stati oggetto di modifiche, per una serie di ragioni legate sia al prosieguo dei processi di definitiva liberalizzazione dei mercati, sia agli aumenti imprevedibili dei prezzi, dovuti prima al superamento della crisi pandemica da Covid-19 e poi al conflitto Russo-Ucraino e ai riflessi sui mercati.

Ai sensi del provvedimento, dal 1° gennaio 2025 sono entrate in vigore nuove regole per i contratti di energia elettrica e gas, con l'obiettivo di offrire maggiori garanzie e trasparenza sia in fase di sottoscrizione di una nuova offerta per i contratti conclusi fuori dai locali commerciali oppure a distanza (come i contratti via telefono), sia in fase contrattuale nel caso di variazioni delle condizioni da parte del venditore.

La delibera è implementazione delle modifiche al Codice del Consumo disposte dal d.lgs n. 26/2023 e dalla Legge concorrenza 2022 e intende rafforzare gli obblighi dei venditori in caso di modifica delle condizioni contrattuali e armonizzare la disciplina in materia di offerte PLACET e di servizio di tutela della vulnerabilità.

Tra le novità più rilevanti:

– l'obbligo in capo al venditore nel caso di contratti conclusi fuori dai locali commerciali oppure a distanza di fornire ai clienti domestici, se disponibili, le informazioni sui mezzi di comunicazione elettronica che consentano lo scambio di messaggi scritti su un supporto durevole, in grado di riportare data e ora della comunicazione;
– per i contratti via telefono, ai fini della validità del consenso per la stipula del contratto, si prevede che il cliente confermi di aver ricevuto il documento scritto con tutte le condizioni contrattuali, trasmesso su supporto cartaceo o su un altro supporto durevole disponibile e accessibile;

– nel caso di contratti stipulati nel contesto di visite non richieste di un venditore ("porta a porta") presso l'abitazione di un cliente domestico oppure di escursioni organizzate da un venditore a scopo commerciale il diritto di ripensamento viene esteso da 14 a 30 giorni.

È stato innovato, inoltre, il regime delle comunicazioni relative alle modifiche delle condizioni contrattuali (variazioni unilaterali, evoluzioni automatiche e rinnovi), che dovranno essere fornite ai clienti su un supporto durevole, preventivamente accettato dal cliente, e, nel caso di variazioni unilaterali e rinnovi, dovranno avere contenuto vincolato alle specifiche previsioni regolatorie ed essere separate da comunicazioni di altra natura, quali ad esempio le comunicazioni a scopi commerciali. Inoltre, nel caso di comunicazioni telematiche, l'intestazione della comunicazione deve coincidere con l'eventuale oggetto del messaggio di trasmissione.

La delibera specifica che le variazioni unilaterali e i rinnovi dovranno essere comunicati con un preavviso non inferiore a 3 mesi, ridotto a 1 mese solo nel caso in cui la variazione unilaterale comporti una riduzione dei corrispettivi determinati dal venditore. In caso di mancato rispetto del termine di preavviso, il venditore deve corrispondere un indennizzo automatico al cliente finale.

È stata inoltre confermata, anche ai fini del rispetto delle tempistiche di preavviso per le comunicazioni delle modifiche contrattuali disciplinate dall'Autorità, l'applicazione degli articoli 1334 e 1335 del Codice civile che, da un lato, correlano la produzione degli effetti giuridici degli atti unilaterali al momento in cui pervengono a conoscenza del destinatario e, dall'altro lato, presumono che il destinatario abbia avuto conoscenza dell'atto nel momento in cui lo stesso atto sia pervenuto al suo indirizzo.

Nel caso di controversie legate all'efficacia della variazione unilaterale e del rinnovo delle condizioni economiche, a seguito di una eventuale contestazione sulla ricezione dell'atto da parte del cliente, grava sul venditore l'onere della prova dell'invio e del recapito degli atti.

Il rafforzamento delle tutele del consumatore emerge anche dall'affermazione della responsabilità dei venditori per quanto riguarda il rispetto del Codice di condotta commerciale e dei diritti dei clienti anche con riferimento ai servizi *telemarketing* e *teleselling* affidati a terzi, indipendentemente dalla tecnologia o dalle modalità organizzative adottate per promuovere e concludere i contratti.

Una ulteriore tappa significativa del percorso regolatorio seguito da ARERA è la deliberazione 399/2025/R/com, adottata il 5 agosto 2025, riguardante la qualità dei servizi di vendita di energia elettrica e gas naturale,

e volta ad introdurre un nuovo Testo Integrato della Qualità della Vendita (TIQV), la cui entrata in vigore è prevista dal 1° gennaio 2026.

La riforma nasce dall'esigenza di aggiornare le regole vigenti alla luce del mutato contesto normativo europeo (le citate Direttive (UE) 2019/944 sul mercato interno dell'energia elettrica e alla direttiva e (UE) 2024/1788 sul mercato del gas e dell'idrogeno), nonché delle opportunità offerte dalla digitalizzazione e dall'impiego di tecnologie innovative nei processi di *customer care*.

Il TIQV si pone, infatti, una triplice finalità: rafforzare la tutela dei clienti finali; incrementare la trasparenza del rapporto contrattuale e promuovere modalità innovative ed efficienti di gestione dei reclami e delle richieste di informazioni.

La delibera interviene sugli indicatori di qualità commerciale relativi alle principali prestazioni dei venditori: i tempi di risposta motivata ai reclami scritti, i tempi di rettifica di fatturazione e di doppia fatturazione, nonché il tempo di risposta a richieste scritte di informazioni, distinguendo tra standard specifici e standard generali e introducendo un sistema di indennizzi automatici aggiornato nel valore base a 30 euro in caso di inadempimento, con regole più stringenti per i casi di reiterata violazione.

Essa innova inoltre il sistema dei canali di contatto e di comunicazione stabilendo l'obbligo per i venditori di garantire almeno un canale telefonico, uno postale e uno telematico, con specifica attenzione all'accessibilità per le persone con disabilità, e a mantenere attivi per almeno sei mesi, anche dopo la cessazione del contratto, i servizi digitali riservati all'area personale del cliente, così da consentire la gestione di eventuali pendenze contrattuali, l'accesso a bollette e documenti e l'inoltro di reclami.

ARERA interviene inoltre sulla disciplina relativa ai servizi telefonici, estendendo gli obblighi di qualità anche ai venditori di minori dimensioni e introducendo una regolazione specifica sull'uso di assistenti vocali basati su intelligenza artificiale, imponendo l'obbligo di preavvisare il cliente quando l'interazione è gestita da un sistema automatizzato e di garantire sempre la possibilità di trasferimento a un operatore umano, al fine di evitare limitazioni all'esercizio del diritto all'informazione.

Un altro punto toccato riguarda la classificazione dei reclami e delle richieste di informazioni. Si stabilisce che qualunque comunicazione del cliente che comporti un'attività di verifica puntuale debba essere qualificata come reclamo e viene imposta ai venditori la redazione delle risposte secondo una sequenza predefinita e comprensibile (contenente formule quali: "Il Suo reclamo", "Le nostre verifiche", "Le nostre conclusioni", "I Suoi diritti"), così da garantire uniformità e chiarezza nell'informazione.

Viene infine regolato l'aspetto della pubblicità dei dati prevedendo l'obbligo per i venditori di pubblicare annualmente sui propri siti internet, secondo un formato uniforme denominato "Scheda qualità", i livelli di qualità previsti dalla regolazione e quelli effettivamente conseguiti, così da consentire ai clienti un confronto immediato e comparabile delle performance degli operatori, rafforzando in tal modo la concorrenza sul mercato libero e la consapevolezza dei consumatori.

4. Costruire la fiducia tra operatori economici e consumatori

Le piattaforme rappresentano nell'attuale momento di evoluzione dei settori e delle loro regole uno degli strumenti più significativi per coniugare le innovazioni offerte dal mercato e le esigenze regolatorie: favoriscono l'incontro tra domanda e offerta; monitorano le attività e i soggetti che operano nei mercati; agevolano l'accesso ai sistemi di tutela da parte dei consumatori e molto altro.

Si assiste alla creazione di nuovi spazi di mercato e alla comparsa di nuovi servizi in cui le piattaforme sono in grado di rispondere a esigenze concrete delle aziende che operano nei settori regolati da ARERA, con l'ambizione di superare il mero rispetto di indicatori, obblighi e standard introdotti dall'Autorità, cogliendo le opportunità della digitalizzazione nel monitoraggio dei servizi per un conseguente miglioramento degli stessi.

In questo scenario compaiono sul mercato piattaforme in grado di adattarsi ai software gestionali aziendali, permettendo di estrarre i dati registrati e riadattarli in modo automatico agli obblighi imposti da ARERA, per comunicarli nel formato richiesto in tempi rapidi e in formati accessibili e verificabili.

Tutti i settori sono innovati da tali opportunità, in grado di accompagnare gli operatori ad affrontare le sfide in termini di potenziali riconfigurazioni dei processi, rapporti, costi ed eventuali sanzioni.

Un ambito di intervento è quello della raccolta e trasporto dei rifiuti urbani, spazzamento e lavaggio strade, innovato dal Testo unico per la regolazione della qualità del servizio di gestione dei rifiuti urbani (TQRIF) – adottato con la delibera 15/2022/R/rif e ampliato con la delibera 387/2023/R/rif – Entro la fine di marzo 2026 gli operatori saranno chiamati ad adempiere agli obblighi di comunicazione telematica ad ARERA, nella prospettiva di uniformare i livelli di qualità contrattuale e tecnica dei servizi di igiene ambientale offerti agli utenti, secondo quanto imposto dagli standard minimi individuati. Tutte le informazioni e dati concernenti le presta-

zioni soggette a livelli di qualità, devono essere registrati su piattaforma informatica e comunicati annualmente all'Autorità tramite l'invio della reportistica relativa alla qualità contrattuale e tecnica del servizio di gestione dei rifiuti urbani.

Prevedendo tale complessità, alcuni operatori hanno introdotto nel mercato soluzioni per offrire ai gestori strumenti per semplificare il processo di rendicontazione previsto dal TQRIF, nella prospettiva di trasformare l'obbligo di adeguamento alle nuove regole in una occasione per aumentare efficienza e qualità attraverso il monitoraggio dei servizi.

Un altro esempio è dato dalle piattaforme introdotte per il compostaggio domestico. Attraverso app e collegando la propria utenza alla compostiera ricevuta dai Comuni, attraverso un Qr Code univoco è possibile geolocalizzarsi e, successivamente, auto monitorare l'attività, al fine di accedere alla riduzione in bolletta della tassa rifiuti.

Amministrazioni comunali e gestori dei servizi adottano veri e propri "albi dei compostatori digitali", una versione contemporanea del registro comunale in cui sono iscritti gli utenti che dichiarano di trattare in autonomia i rifiuti organici, conferendoli in compostiera. Il tracciamento viene dunque svolto dagli stessi utenti, spostando l'onere dai Comuni su di essi. Per i Comuni sarà più agevole rendicontare tale quantità nei sistemi O.R.SO (Osservatorio Rifiuti Sovraregionale) e contabilizzarla per la riduzione delle ecotasse e l'accesso alle premialità, ove previste.

Tali soluzioni rispondono alle esigenze introdotte dall'UE nell'ambito della strategia economia circolare, che a livello unionale mira a rendere tracciabile e misurabile il compostaggio domestico: mettendo in rete tutti i soggetti coinvolti, tali albi consentono di calcolare la quantità di rifiuti organici gestiti tramite autocompostaggio.

Sempre in tema di raccolta di rifiuti sul territorio le piattaforme supportano anche l'attività di raccolta dei dati degli svuotamenti effettuati, fondamentale per migliorare la qualità della raccolta e arrivare ad applicare una tariffa più equa, basata sulla reale produzione di rifiuti di ciascuna utenza e cioè sull'effettivo "consumo" del servizio similmente a quanto accade nei mercati dell'energia, del gas e idrico. I dati raccolti quotidianamente tramite lettura vengono trasmessi da remoto a un gestionale, che riverserà l'analisi svolta sul documento di fatturazione che, secondo il c.d. sistema di tariffazione puntuale, premierà i consumatori più virtuosi nella differenziazione dei rifiuti con benefici diretti in bolletta. Tale servizio è possibile grazie ad App che forniscono informazioni complete e geolocalizzate sulle modalità e le tempistiche di conferimento dei rifiuti, identificandoli attraverso scansione del codice a barre o riconoscimento fotografico. In tempo

reale la piattaforma indica i contenitori in cui conferire il prodotto o il punto di raccolta più vicino, visualizzando una mappa.

L'ISPRA – che monitora i Comuni nel percorso di adozione della tariffazione puntuale[81] – ha evidenziato come tale sistema, basato sui principi europei di "chi inquina paga" e "Pay-As-You-Throw", consente agli utenti di beneficiare di tariffe più vantaggiose attraverso la misurazione dei rifiuti conferiti. Questo meccanismo premiale diventa un elemento chiave nell'incoraggiare comportamenti ambientali responsabili, superando un approccio puramente sanzionatorio".

Dal punto di vista dell'accessibilità e delle tutele, dirimente è l'introduzione ormai generalizzata dello SPID è utilizzabile per accedere ai servizi. Ad esempio: l'Area Clienti del GSE consente l'accesso tramite SPID per verificare lo stato delle pratiche, richiedere un servizio e chiedere supporto; nei portali ENEA, l'autenticazione tramite SPID rappresenta ormai l'unica modalità di accesso per i nuovi account e per l'inserimento di nuove asseverazioni sui portali dedicati a Ecobonus, Superbonus 110% e Bonus Casa; tramite l'accesso al Portale Consumi di Acquirente Unico è invece possibile visualizzare informazioni dettagliate sulle proprie forniture di luce e gas, come letture e consumi; la stessa regola anche per l'accesso alla piattaforma operativa sviluppata con ANCI "SGATE", che rappresenta un'esperienza in via di ampliamento.

Dal punto di vista della tenuta istituzionale e del coordinamento, l'implementazione di piattaforme sempre più in grado di generare impatti positivi sui mercati regolati da ARERA, richiede interventi coordinati anche con le altre Autorità, sia a livello sovranazionale – ACER – sia sul piano interno, con AGID e AGCM *in primis*.

5. Prospettive regolatorie

Dalla ricerca condotta emerge l'introduzione di riforme dalla portata effettivamente innovativa e tese a veicolare semplificazione amministrativa e potenziamento delle tutele sostanziali dei clienti finali, attraverso un sistema che si fonda sui canoni di trasparenza, tracciabilità, fiducia, effettività, prestazioni di qualità, coerentemente con i regolamenti e le direttive europee nonchè con il quadro di principi del Codice del Consumo.

Le nuove regole non si limitano a definire standard formali, ma

[81] Nel 2022 i comuni che adottavano il sistema di tariffazione puntuale del servizio di gestione dei rifiuti urbani erano 1278; nel 2017, soltanto 341.

mirano a promuovere un miglioramento in termini di qualità dei servizi e delle tutele per i consumatori, nella prospettiva di garantire un rapporto equilibrato e corretto tra venditori e clienti, accrescendo la fiducia dei consumatori e rafforzando le dinamiche concorrenziali nei settori regolati dall'Autorità.

Il ruolo di garanzia di ARERA si manifesta nella qualità tecnica dell'azione regolatoria così come nella capacità di comunicare la stessa in modo trasparente e intellegibile per i cittadini, contribuendo a creare un clima di fiducia e certezza in un sistema che attraversa un clima di profonda trasformazione.

Nella stessa Relazione è ARERA a evidenziare i due nodi principali che caratterizzano l'impiego di strumenti di IA nei propri processi decisionali, ponendo l'accento sull'irrinunciabile requisito dell'Explainable Artificial Intelligence (XAI) ritenuto condizione necessaria per garantire la legittimità, la trasparenza e l'affidabilità delle decisioni automatizzate o assistite da IA all'interno dei sistemi di regolazione – in ciascuna delle attività per cui in ambito regolatorio questa può essere utilizzata: analisi di conformità alle normative, sorveglianza dei mercati, fino all'elaborazione di scenari previsionali su cui fondare scelte regolative o sanzionatorie.

Il primo nodo critico, "di natura epistemica" riguarda la comprensibilità e spiegabilità di una decisione presa da un algoritmo complesso, considerando che caratteristiche dei modelli "black-box". Qui l'adeguamento del sistema non si arresta su un piano della correttezza statistica ma richiama la necessità di una motivazione accessibile e coerente con l'ordinamento, sia in fase istruttoria, sia in sede di controllo e contenzioso.

Il secondo nodo è istituzionale e mette in guardia da derive di deresponsabilizzazione dell'Autorità regolatrice. All'opposto, l'uso dell'IA rappresenta una grande occasione per il rafforzamento delle garanzie procedurali, al fine di evitare che le decisioni siano percepite come arbitrarie o indecifrabili in un contesto di decisione pubblica.

La sfida è dunque quella di inserire ARERA in un circuito di produzione del sapere in cui Autorità e piattaforme, in un gioco di specchi che vede al centro i consumatori, riflettendo i bisogni le aspettative di quest'ultimi e traducendoli in un'azione regolatoria efficace, capace di veicolare le migliori tecnologie ed effettivamente rispondente alle esigenze della generalità in maniera targetizzata nel tempo e nello spazio.

Le piattaforme digitali nella pubblica amministrazione e negli appalti pubblici: trasparenza, innovazione e fiducia come strumenti per un nuovo rapporto tra Stato e cittadini

Serafina Piantedosi[82]

La cosiddetta platformization (o piattaformizzazione) dell'economia e della società contemporanea, diffusasi innanzitutto nel settore privato, coinvolge anche la pubblica amministrazione, dal momento che lo Stato adotta piattaforme digitali sempre più avanzate per incrementare qualità e quantità dei servizi offerti ai cittadini.
Il percorso verso la digitalizzazione delle pubbliche amministrazioni italiane, guidato dall'adozione di piattaforme digitali sempre più avanzate, non è solo una sfida tecnologica, ma un'occasione per ridefinire le relazioni tra istituzioni e cittadini. Per realizzare tale obiettivo, però, c'è bisogno di fiducia nell'attività amministrativa digitale, che rappresenta la dimensione valoriale e relazionale della sicurezza informatica, quella che trasforma la mera protezione tecnica in un patto di affidabilità tra tecnologia, istituzioni e cittadini.

1. Le piattaforme digitali nella pubblica amministrazione

La cosiddetta *platformization* (o piattaformizzazione) dell'economia e della società contemporanea, diffusasi innanzitutto nel settore privato, coinvolge anche la pubblica amministrazione, dal momento che lo Stato adotta piattaforme digitali sempre più avanzate per incrementare qualità e quantità dei servizi offerti ai cittadini.

La crisi pandemica ha determinato un'accelerazione del processo di sviluppo digitale all'interno della pubblica amministrazione, imponendo lo svolgimento dell'attività amministrativa mediante strumenti in-

[82] Si precisa che le opinioni espresse dall'autrice sono frutto del suo personale convincimento e non possono in alcun modo essere ritenute come rappresentative di orientamenti dell'Autorità nazionale anticorruzione o impegnative per la stessa.

formatici e telematici.

A seguito della modifica dell'art. 3-*bis* l. 7 agosto 1990, n. 241[83] intervenuta ad opera dell'art. 12, comma 1 lett. b), d.l. 16 luglio 2020, n. 76[84], l'utilizzo delle ICT da parte della pubblica amministrazione è diventato espressione del diritto ad una buona amministrazione, dal momento che nell'ambito del procedimento amministrativo le pubbliche amministrazioni hanno l'obbligo di agire mediante strumenti informatici e telematici per conseguire una maggiore efficienza e, in particolare, nella prospettiva di poter svolgere un'adeguata e sollecita istruttoria del procedimento amministrativo.

L'impiego delle ICT non si ferma alla gestione del procedimento amministrativo, ma sulla base della previsione di cui all'art. 12 del d.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale)[85], deve riguardare tutte le ipotesi di interazione tra le pubbliche amministrazioni ed i privati, così da consentire un facile accesso alla consultazione dei dati, la circolazione e lo scambio di informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi fra le diverse amministrazioni.

A tal fine, le pubbliche amministrazioni hanno l'obbligo di sviluppare e consolidare i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione in via telematica di servizi a cittadini ed imprese, anche con l'intervento di piattaforme fornite da privati.

Sulla scorta di tali previsioni, sono state implementate molteplici infrastrutture digitali per fornire servizi ai cittadini, alle imprese e agli enti pubblici, come il Sistema Pubblico di Identità Digitale (SPID), PagoPA, il Fascicolo Sanitario Elettronico (FSE), il Sistema Tessera Sanitaria (TS), l'App Io, il Sistema per l'Accesso alle Camere di Commercio, la piattaforma di interscambio gestito dall'Agenzia delle Entrate per la fatturazione elettronica (SdI).

Tali piattaforme costituiscono solo una parte dell'infrastruttura digitale messa a disposizione dalla pubblica amministrazione italiana al fine di garantire semplificazione, digitalizzazione e trasparenza e la loro implementazione costituisce uno degli obiettivi del Piano triennale per l'informatica nella Pubblica Amministrazione 2024/2026[86].

[83] Legge 7 agosto 1990, n. 24 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" (GU n.192 del 18-08-1990).

[84] Decreto-legge 16 luglio 2020, n. 76 "Misure urgenti per la semplificazione e l'innovazione digitale", convertito con modificazioni dalla L. 11 settembre 2020, n. 120 (in S.O. n. 33, relativo alla G.U. 14/09/2020, n. 228).

[85] Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), GU n.112 del 16-05-2005 - Suppl. Ordinario n. 93.

[86] Il Piano triennale per l'informatica nella Pubblica Amministrazione 2024/2026 è con-

In tale contesto il cittadino diviene il centro di un ecosistema interconnesso, finalizzato a facilitare l'accesso ai servizi pubblici, rafforzare il rapporto tra pubblica amministrazione e utenti e costruire un'amministrazione più efficiente, accessibile e affidabile.

Nel caso delle piattaforme pubblicistiche non si pongono le stesse criticità tipiche delle piattaforme private in termini di concentrazione di potere economico o tecnologico, né il rischio di creare rapporti di dipendenza tra operatori economici e gestori della piattaforma[87]. Le piattaforme pubblicistiche, infatti, sono concepite come strumenti di accesso aperto, trasparente e non discriminatorio, che garantiscono pari opportunità a tutti i soggetti che intendono interagire con la pubblica amministrazione[88]. Tuttavia, l'adozione di tali strumenti comporta altre sfide significative di natura organizzativa, tecnica e giuridica, che incidono profondamente sull'efficacia del processo di digitalizzazione amministrativa. In primo luogo, l'amministrazione è chiamata a farsi carico delle conseguenze negative legate al c.d. divario digitale (*digital gap*) fra le diverse fasce della popolazione, per cui deve adottare soluzioni organizzative e infrastrutturali idonee a evitare nuove forme di esclusione o disparità di trattamento tra cittadini in ragione del loro diverso livello di "alfabetizzazione informatica" e della loro diversa disponibilità degli strumenti informatici (e dell'accesso alla rete).

2. Oltre la sicurezza: costruire fiducia nelle piattaforme pubbliche

La gestione digitale dei procedimenti amministrativi espone, poi, la pubblica amministrazione a rischi connessi alla sicurezza informatica e alla protezione della *privacy*. La concentrazione e l'interconnessione di grandi moli di dati personali e sensibili – spesso relativi a cittadini, imprese e funzionari pubblici – richiedono misure di sicurezza avanzate, conformi

sultabile al seguente *link* <https://www.agid.gov.it/sites/agid/files/2024-06/piano_triennale_per_linformatica_nella_pa_2024-2026.pdf>.

[87] Sul punto si veda F. Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Rubbettino, Soveria Mannelli, 2019.

[88] Una compiuta analisi sui vantaggi offerti dalle piattaforme pubbliche si rinviene in I. Calzada, "Democratic Erosion of Data-Opolies: Decentralized Web3 Technological Paradigm Shift Amidst AI Disruption", in *Big Data Cogn. Comput,* 2024, 8, 26. L'A. auspica ecosistemi di dati equi, fondati sulla sovranità digitale e sull'autogoverno dei dati da parte dei cittadini, opponendo al dominio delle "*data-opolies*" delle grandi piattaforme private, un modello trasparente, inclusivo ed emancipatorio di democrazia guidata dai dati.

ai principi del Codice dell'amministrazione digitale e al Regolamento UE 2016/679 (GDPR)[89]. Le pubbliche amministrazioni devono garantire la riservatezza, l'integrità e la disponibilità dei dati, prevenendo accessi non autorizzati, attacchi informatici e perdite di informazioni. In tale contesto, la *cybersecurity* e la tutela della *privacy* costituiscono presupposti indispensabili per mantenere la fiducia dei cittadini e la "legittimazione democratica" dell'azione amministrativa digitale.

Fondamentale, pertanto, diviene il concetto di "fiducia digitale" che può essere intesa come l'insieme di garanzie e di certezze che cittadini, imprese e istituzioni ripongono nei sistemi informatici e nei servizi *online* con cui interagiscono. Essa si fonda sulla percezione di sicurezza, integrità e affidabilità delle tecnologie digitali e dei soggetti che le gestiscono. In termini pratici, la fiducia digitale nasce dalla consapevolezza che i propri dati personali sono tutelati in modo conforme alla normativa, che le informazioni vengono trattate in modo trasparente e che le operazioni elettroniche rispettano principi etici e leggi nazionali e sovranazionali. Si tratta, dunque, di una forma di "fiducia istituzionalizzata" che non dipende solo dalla tecnologia, ma anche dalla trasparenza delle prassi, dalla responsabilità degli operatori pubblici e privati e dalla capacità di assicurare una *governance* digitale orientata alla tutela dei diritti fondamentali.

Pur essendo concetti strettamente correlati, la fiducia digitale e la sicurezza informatica, però, rappresentano due ambiti distinti.

La sicurezza informatica, infatti, si concentra sugli aspetti tecnici e operativi della protezione dei dati e delle reti e include strumenti, protocolli e misure volti a impedire accessi non autorizzati, guasti, perdite di dati o attacchi informatici. Essa costituisce una componente fondamentale, ma non esaustiva, della fiducia digitale.

La fiducia digitale, invece, abbraccia una prospettiva più ampia: oltre alla sicurezza informatica, comprende la protezione della *privacy*, la trasparenza delle decisioni algoritmiche, la correttezza etica nella gestione delle informazioni e il rispetto della normativa vigente in materia di digitalizzazione e trattamento dei dati. Un'organizzazione può quindi disporre di solide barriere informatiche ma, se non opera in modo trasparente o non rispetta principi di responsabilità sociale, la fiducia degli utenti rimane compromessa. In altre parole, la fiducia digitale rappresenta la dimensione

[89] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), GU L 119 del 4 maggio 2016.

valoriale e relazionale della sicurezza informatica, quella che trasforma la mera protezione tecnica in un patto di affidabilità tra tecnologia, istituzioni e cittadini.

3. Le piattaforme digitali negli appalti pubblici

Nelle procedure ad evidenza pubblica l'utilizzo delle infrastrutture digitali, a partire dal 1 gennaio 2024, è divenuto obbligatorio per tutte le fasi del ciclo di vita dei contratti pubblici, che inizia con la programmazione e l'assegnazione del CIG, lo svolgimento della gara, fino a ricomprendere le attività riferite alla conclusione e poi all'esecuzione contrattuale.

È sorto, quindi, un ecosistema nazionale di approvvigionamento digitale (*e-procurement*)[90], costituito dalle piattaforme e dai servizi digitali infrastrutturali abilitanti la gestione del ciclo di vita dei contratti pubblici e dalle piattaforme di approvvigionamento digitale utilizzate dalle stazioni appaltanti.

In particolare, ai sensi dell'art. 22, d.lgs. n. 36/2023 (Codice dei contratti pubblici)[91], le piattaforme e i servizi digitali consentono: «*a) la re-*

[90] La nozione di ecosistema – ritenuta evocativa della indispensabile interoperabilità delle sue componenti – trova riscontro anche nel «*Piano triennale per l'informatica nella Pubblica amministrazione 2024-2026*» dell'AGID, nel quale si sottolinea la necessità che «*ogni singolo ente pubblico divenga un "ecosistema amministrativo digitale", alla cui base ci siano piattaforme organizzative e tecnologiche, ma in cui il valore pubblico sia generato in maniera attiva da cittadini, imprese e operatori pubblici*».

In questo contesto, l'AGID sottolinea come sia necessario «*introdurre dei "processi digitali collettivi" basati su e-service, ovvero interfacce che scambiano dati/informazioni in maniera automatica e interoperabile*».

[91] Decreto legislativo 31 marzo 2023, n. 36, "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici" (G.U. n. 77 del 31 marzo 2023 - S.O. n. 12). Sul tema della digitalizzazione dei contratti pubblici nel nuovo Codice degli appalti si veda B. Marchetti, B.G. Mattarella (a cura di), *La digitalizzazione dei contratti pubblici nel nuovo Codice, Giappichelli,* 2024. Come evidenziato dalla Relazione illustrativa al Decreto legislativo 31 marzo 2023, n. 36, la digitalizzazione costituisce «*una efficace misura di prevenzione della corruzione in quanto consente trasparenza, tracciabilità, partecipazione, controllo di tutte le attività, in modo da assicurare il rispetto della legalità. Il settore delle commesse pubbliche rappresenta, infatti, un'attività fortemente esposta a condotte corruttive, in ragione del potenziale economico che esprime e, quindi, occorrono presidi efficaci e qualificati per fare in modo che le risorse stanziate non vengano distolte dal perseguimento degli interessi pubblici*».

dazione o l'acquisizione degli atti in formato nativo digitale; b) la pubblicazione e la trasmissione dei dati e documenti alla Banca dati nazionale dei contratti pubblici; c) l'accesso elettronico alla documentazione di gara; d) la presentazione del documento di gara unico europeo in formato digitale e l'interoperabilità con il fascicolo virtuale dell'operatore economico; e) la presentazione delle offerte; f) l'apertura, la gestione e la conservazione del fascicolo di gara in modalità digitale; g) il controllo tecnico, contabile e amministrativo dei contratti anche in fase di esecuzione e la gestione delle garanzie».

Inoltre, tutti gli step della procedura ad evidenza pubblica devono svolgersi su piattaforme telematiche "certificate", le c.d. Piattaforme di Approvvigionamento Digitale (PAD)[92] che assicurino l'interoperabilità dei servizi svolti e la confluenza delle informazioni su un'unica banca dati, ossia la Banca Dati Nazionale dei Contratti Pubblici (BDNCP)[93] istituita presso l'ANAC che diventa, così, il collettore nazionale per gli appalti, anche ai fini dello svolgimento di una serie di adempimenti e servizi nevralgici per la legittimità delle procedure di gara, quale ad esempio la pubblicità legale.

[92] L'articolo 25 del d.lgs. n. 36/2023 stabilisce che le Piattaforme di Approvvigionamento Digitale (PAD) sono costituite dall'insieme dei servizi e dei sistemi informatici, interconnessi e interoperanti, utilizzati dalle stazioni appaltanti e dagli enti concedenti per svolgere una o più attività nell'ambito del ciclo di vita digitale dei contratti pubblici e per assicurarne la piena digitalizzazione. A tal fine, interagiscono con i servizi della BDNCP, nonché con i servizi della Piattaforma Digitale Nazionale Dati (PDND), di cui all'articolo 50-*ter* del d.lgs. 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale", garantendo trasparenza, sicurezza e tracciabilità e sostituendo i processi cartacei dal 1° gennaio 2024.

[93] La BDNCP presenta un'architettura complessa, articolata in sei sezioni: 1) l'Anagrafe Unica delle Stazioni Appaltanti (AUSA), istituita dall'articolo 33-*ter* del d.l. 18 ottobre 2012, n. 179, "*Ulteriori misure urgenti per la crescita del Paese*", convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221, nell'ambito della quale opera il sistema di qualificazione delle stazioni appaltanti; 2) la Piattaforma Contratti Pubblici (PCP), che rappresenta il complesso dei servizi *web* e di interoperabilità attraverso i quali le Piattaforme di Approvvigionamento Digitale (PAD) delle stazioni appaltanti interoperano con la BDNCP per la gestione digitale del ciclo di vita dei contratti pubblici; 3) la Piattaforma per la pubblicità legale degli atti, che risponde, per l'appunto, alla finalità di garantire la pubblicità legale degli atti, anche mediante la trasmissione dei dati all'Ufficio delle pubblicazioni dell'Unione europea; 4) il Fascicolo Virtuale dell'Operatore Economico (FVOE), che raccoglie le informazioni, i dati e i documenti da utilizzare a comprova dell'assenza delle cause di esclusione di cui agli articoli 94 e 95 del Codice e del possesso dei requisiti speciali di cui agli articoli 100 e 103 e all'Allegato II.12, per la partecipazione e l'esecuzione dei contratti pubblici; 5) il Casellario Informatico dei contratti pubblici di lavori, servizi e forniture, nel quale sono annotati i dati, le notizie e le informazioni relativi agli operatori economici; 6) l'Anagrafe degli operatori economici di cui all'articolo 31 del Codice.

Le PAD, in particolare, sono costituite dall'insieme dei servizi e dei sistemi informatici, interconnessi e interoperanti, utilizzati dalle stazioni appaltanti e dagli enti concedenti per svolgere una o più attività del ciclo di vita dei contratti pubblici e per assicurarne la piena digitalizzazione. A tal fine, le piattaforme di approvvigionamento digitale interagiscono con i servizi della Banca dati nazionale dei contratti pubblici nonché con i servizi della Piattaforma digitale nazionale dati.

L'introduzione di tali piattaforme di approvvigionamento ha forse rappresentato la modifica normativa che ha avuto maggiori riscontri pratici nel mondo delle commesse pubbliche, rivoluzionando sia le modalità di svolgimento della gara, sia le interazioni tra stazioni appaltanti e operatori economici.

Le PAD, infatti, non si limitano a sancire la definitiva trasposizione delle procedure di gara dalla carta al digitale, ma velocizzano la circolazione delle informazioni e dei dati tra le amministrazioni e i partecipanti, semplificano le verifiche dei requisiti grazie all'integrazione con il Fascicolo Virtuale dell'Operatore Economico (FVOE)[94] e le banche dati digitali, ma soprattutto sono rivoluzionarie sotto il profilo della prevenzione della corruzione, dal momento che la tecnologia adottata consente di mantenere traccia inalterabile di tutte le operazioni e dei flussi di dati, rendendo pubbliche e accessibili molte informazioni chiave come bandi, offerte, aggiudicazioni e motivazioni delle scelte della stazione appaltante.

In tal modo, si riducono drasticamente le zone d'ombra e le occasioni di scambio illecito o di favoritismo.

Il fulcro dell'*e-procurement* nazionale, poi, è rappresentato dalla BDNCP, che riunisce tutti i dati dei contratti pubblici di qualsiasi importo e tipologia per garantire trasparenza e tracciabilità delle procedure di gara e delle fasi antecedenti e successive alla stessa.

La BDNCP, allo stesso tempo, consente un monitoraggio sull'andamento generale della contrattualistica pubblica e costituisce uno strumento efficace per verificare il rispetto della legalità dell'azione

[94] Il Fascicolo Virtuale dell'Operatore Economico incarna il principio della cosiddetta "decertificazione": i dati di un operatore economico già in possesso di una pubblica amministrazione non possono essere richiesti all'operatore economico stesso, secondo il principio dell'"*once only*". Inoltre, il FVOE elimina la necessità di riprodurre, nelle successive procedure di affidamento di contratti pubblici alle quali l'operatore economico intenda partecipare, i medesimi dati e le stesse certificazioni già presenti nel fascicolo, in una versione ancora in corso di validità.

amministrativa[95].

Per il tramite dell'interconnessione tra la BDNCP e il FVOE le stazioni appaltanti possono verificare il possesso dei requisiti in capo agli operatori economici mediante l'accesso ad un unico luogo, senza dover consultare molteplici banche dati pubbliche o interpellare singoli enti detentori delle informazioni richieste, così attuando in concreto il principio secondo cui la pubblica amministrazione non può chiedere al cittadino un documento di cui già dispone.

La BDNCP è disegnata dal Codice dei contratti pubblici non più solo come strumento conoscitivo relativo alla procedura di evidenza pubblica, ma come mezzo per erogare servizi alle stazioni appaltanti, agli enti concedenti e agli operatori economici, svolgendo una serie di funzioni, essenzialmente riconducibili alla prestazione di servizi informativi.

Più in particolare, la BDNCP si articola in sei sezioni: a) anagrafe unica delle stazioni appaltanti (AUSA); b) piattaforma contratti pubblici (PCP); c) piattaforma per la pubblicità legale degli atti; d) fascicolo virtuale dell'operatore economico (FVOE) e) il casellario informatico; f) anagrafe degli operatori economici.

La Banca dati, inoltre, interopera con i soggetti fruitori dei servizi da questa erogati e con i soggetti erogatori dei servizi ad essa necessari, per il tramite della Piattaforma digitale nazionale dei dati (PDND), la quale è gestita dalla Presidenza del Consiglio dei Ministri ed è costituita da un'infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici[96].

La BDNCP assicura la tempestiva pubblicazione dei dati, anche attraverso la Piattaforma unica della trasparenza gestita da ANAC.

Tale piattaforma è richiamata dall'art. 28, comma 3, Cod. contratti pubblici, ed è autonoma rispetto alla BDNCP, in quanto non ne costituisce una sezione.

Sulla Piattaforma Unica della Trasparenza vengono pubblicati, in formato aperto, i dati relativi ai contratti pubblici, e, nello specifico, sono pubblicati "*la struttura proponente, l'oggetto del bando, l'elenco degli operatori invitati a presentare offerte, l'aggiudicatario, l'importo di aggiudicazione, i tempi di completa-*

[95] Le modalità di funzionamento della BDNCP sono stabilite nel provvedimento *ex* articolo 23 del Codice, adottato con Delibera ANAC n. 261 del 20 giugno 2023.

[96] Sul tema dell'interoperabilità tra piattaforme digitali nel settore dei contratti pubblici si veda G. Carullo, "Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici", in *federalismi.it,* 19/2023, pp. 110-127.

mento dei lavori, servizi o forniture e l'importo delle somme liquidate".

La Piattaforma Unica della Trasparenza a regime costituirà un unico punto di accesso a dati, informazioni e documenti pubblicati nella sezione "Amministrazione Trasparente" dei siti istituzionali delle pubbliche amministrazioni, così da facilitarne la consultazione.

Di recente, ANAC in collaborazione con il CNR ha lanciato la nuova piattaforma "TrasparenzAI", che costituisce uno strumento informatico sperimentale per l'analisi automatica della sezione "Amministrazione Trasparente" dei siti *web* delle amministrazioni pubbliche tenute al rispetto degli obblighi di pubblicazione sanciti dal d.lgs. n. 33/2013[97]. Tale piattaforma raccoglierà i dati di tutte le pubbliche amministrazioni in un unico *hub* digitale, offrendo la possibilità a cittadini, imprese e *stakeholders* di accedervi agevolmente. Nello specifico, la piattaforma è in grado di raccogliere e organizzare i dati di tutte le 23.663 pubbliche amministrazioni italiane, analizzando in meno di 20 ore le rispettive sezioni *web*. Grazie a strumenti avanzati di *web crawling* e *web scraping*, la piattaforma "TrasparenzAI" verifica la conformità della struttura e la presenza delle sezioni previste dal d.lgs. 33/2013, individuando in maniera oggettiva e standardizzata eventuali mancanze o difformità[98].

L'obiettivo è quello di andare oltre una trasparenza puramente formale, promuovendo un accesso ai dati che sia effettivo, intuitivo ed utile. In tal modo, la Piattaforma diventa uno strumento non solo per informare, ma anche per coinvolgere la società civile nell'attività di vigilanza sull'operato delle istituzioni.

4. I possibili impatti del Web3

Il *Web3* rappresenta una nuova evoluzione di Internet, basata su tecnologie innovative come la *Blockchain*, i contratti intelligenti (*smart contracts*) e i registri distribuiti (*Distributed Ledger Technology*). Questa rivoluzione

[97] Decreto legislativo 14 marzo 2013, n. 33, "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" (G.U. n. 80 del 05 aprile 2013).

[98] La piattaforma "TrasparenzAI", frutto della collaborazione tra ANAC e il Consiglio Nazionale delle Ricerche nell'ambito del protocollo d'intesa stipulato nel 2023, consente l'analisi e il monitoraggio delle sezioni "Amministrazione Trasparente" dei siti *web* istituzionali delle singole amministrazioni, verificandone la conformità alle regole previste per i singoli nodi della sezione.

tecnologica mira a creare un ambiente digitale più trasparente, sicuro e decentralizzato, consentendo scambi di dati e transazioni affidabili senza la necessità di intermediari. Nel contesto della pubblica amministrazione, il *Web3* offre strumenti capaci di trasformare profondamente i processi burocratici, aumentando l'efficienza, la tracciabilità e la fiducia nei sistemi.

L'introduzione della tecnologia *Blockchain* negli appalti pubblici, sancita per la prima volta dall'art. 106 del Codice dei contratti pubblici, rappresenta una tappa fondamentale di tale percorso di digitalizzazione e di costruzione della "legittimazione democratica" dell'azione amministrativa digitale.

La norma, al comma 3, disciplina le garanzie che le imprese devono fornire alla stazione appaltante per partecipare alla gara, stabilendo che la garanzia fideiussoria debba essere emessa e firmata digitalmente, oltre a essere verificabile telematicamente presso l'emittente o gestita in tutte le sue fasi tramite piattaforme basate su tecnologie a registri distribuiti (*Distributed Ledger Technology*), al fine di garantire la trasparenza e la certezza del processo.

In aggiunta, il comma 8 dell'art. 106, Cod. contratti pubblici introduce un incentivo per l'adozione della *Blockchain*, prevedendo una riduzione del 10% della garanzia per quegli operatori economici che presentino una fideiussione emessa e firmata digitalmente, gestita tramite piattaforme a registri distribuiti o attraverso verifica telematica sul sito dell'emittente.

Nell'intento del legislatore codicistico, infatti, la riduzione del 10% prevista per la garanzia gestita mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti "*è volta a incentivare il ricorso alle piattaforme già previste dall'art. 25 del Codice. A compimento del progetto di digitalizzazione si dovranno realizzare l'interoperabilità e l'integrazione tra i sistemi dei diversi attori, la digitalizzazione e l'automazione del processo di garanzia dall'emissione allo svincolo, la condivisione e l'attestazione all'interno della filiera di dati e processi. A regime, la soluzione potrà consentire di conseguire maggiore efficienza, trasparenza e certezza informativa lungo tutto il ciclo di vita delle fideiussioni e ridurre potenziali fenomeni di frodi*".

Sulla scorta di tale previsione, iniziano ad essere sperimentate piattaforme basate su DLT per la gestione digitale di fideiussioni bancarie e cauzioni assicurative negli appalti pubblici, segnando un passo concreto verso la smaterializzazione della garanzia e la trasparenza verificabile. Tali piattaforme, consentono, infatti, la c.d. "notarizzazione" della polizza, ossia la registrazione di un documento in modo univoco e immutabile su una rete condivisa, rappresentata, appunto, dalla *Blockchain*[99]. Una volta inserito

[99] Cfr. F. Bassan, M. Rabitti, *From smart legal contracts to contracts on blockchain: An empirical investigation* in *Computer Law & Security Review,* vol. 55, November 2024. F. Bassan, M. Ra-

in piattaforma, quindi, il documento contenente la garanzia non può più essere alterato o duplicato in maniera fraudolenta, per cui in sede di gara la stazione appaltante potrà agevolmente verificarne l'autenticità e svincolare la garanzia in funzione del livello di esecuzione dell'appalto.

Ciò indubbiamente consente alla stazione appaltante di velocizzare le fasi di controllo dell'autenticità della garanzia e di svincolo della stessa, alleggerendo gli oneri burocratici che ingessano queste fasi della procedura di evidenza pubblica e dilatano molto spesso i tempi di aggiudicazione e di gestione dell'appalto.

In futuro, si potrebbe immaginare l'applicazione di tecnologie *Web3* anche alla fase della stipula del contratto di appalto, per il tramite dell'introduzione di *smart contract* sostitutivi del contratto di appalto pubblico. Infatti, anche per la firma del contratto tra l'operatore economico e il rappresentante della stazione appaltante potrebbe essere utile la "notarizzazione" del documento, così da garantire la decentralizzazione, l'immutabilità e l'integrità dello stesso, nonché la provenienza della firma.

Parimenti, anche la fase dell'esecuzione del contratto di appalto potrebbe trovare beneficio dalle tecnologie *Web3*; pensiamo ad esempio all'attività di gestione delle riserve iscritte dall'impresa o delle varianti in corso d'opera oppure all'emissione dei SAL, così come pure alla fase di emissione dei pagamenti.

Sarebbero, dunque, innumerevoli le opportunità di impiego delle tecnologie *Web3* all'interno degli appalti pubblici; tuttavia, attualmente la creazione di siffatte piattaforme è rimessa all'iniziativa dei privati, dal momento che non sono state ancora costituite piattaforme pubbliche che consentono di offrire gli stessi servizi.

Pertanto, l'utilizzo di tali piattaforme private potrebbe rivelarsi fonte di costi per le stazioni appaltanti che volessero usufruire di tutti i servizi messi a disposizione.

Un altro aspetto critico riguarderebbe, poi, l'interoperabilità con le infrastrutture IT già esistenti, come la BDNCP e il FVOE e la necessità di standardizzazione a livello tecnico e normativo, per garantire che i diversi sistemi possano scambiarsi dati in modo efficiente e sicuro.

Non meno importanti da evidenziare sarebbero, poi, le esigenze di

---

BITTI, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain',* in *Rivista di diritto bancario,* 2023(III), 561-639. A. CORRADO, *I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro, in Federalismi.it,* 2023, pp. 128 ss. G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione,* in *Dir. econ.,* 2019, pp. 187 ss.

tutela della *privacy* e di protezione dei dati personali, soprattutto in presenza di dati sensibili trattati nelle procedure di appalto, che mal si concilierebbero con la trasparenza e la tracciabilità proprie della *Blockchain*.

5. Conclusioni

Le piattaforme digitali, con le loro potenzialità di semplificazione e ottimizzazione dei processi amministrativi, offrono una risposta concreta a molti problemi atavici dell'amministrazione pubblica italiana, come la lentezza burocratica e il rischio di corruzione. Il percorso verso la digitalizzazione delle pubbliche amministrazioni italiane, guidato dall'adozione di piattaforme digitali sempre più avanzate, non è solo una sfida tecnologica, ma un'occasione per ridefinire le relazioni tra istituzioni e cittadini, ponendo al centro valori fondamentali come la trasparenza, la fiducia e l'inclusività.

Ma cosa vuol dire davvero affidarsi alla tecnologia? Significa probabilmente immaginare un futuro in cui i cittadini non siano spettatori passivi, ma coprotagonisti del cambiamento: un futuro in cui un operatore economico può confidare su procedure di appalto eque e trasparenti, un cittadino può monitorare l'uso delle risorse pubbliche e, in generale l'operato della pubblica amministrazione e un funzionario pubblico può contare su strumenti che lo liberino da attività burocratiche ripetitive che ingessano il proprio lavoro, distogliendolo dal perseguimento dell'interesse pubblico. Per realizzare tale obiettivo, però, c'è bisogno di fiducia nel digitale. Sotto questo profilo, le piattaforme digitali, integrate con tecnologie come la *Blockchain* e inquadrate nel più ampio ecosistema del *Web3*, rappresentano oggi un'opportunità senza precedenti. Esse non solo rendono i procedimenti amministrativi più efficienti e tracciabili, ma assicurano quella trasparenza effettiva da sempre auspicata.

Tuttavia, le piattaforme digitali, processando una enorme quantità di informazioni e abilitando l'accesso remoto e distribuito, diventano bersagli privilegiati per attacchi informatici: *malware*, *ransomware*, *data breach* e azioni di sabotaggio possono compromettere la disponibilità, integrità e riservatezza di dati e processi decisionali. La concentrazione di dati e funzioni su sistemi interconnessi richiede dunque forti presidi di sicurezza, come crittografia, autenticazione forte degli accessi, aggiornamento costante dei sistemi e protocolli di gestione degli incidenti informatici.

La sicurezza informatica della pubblica amministrazione non può essere concepita come un mero adempimento tecnico, ma come un obiettivo strategico di *governance* pubblica, che integra tecnologia, diritto e cultura

amministrativa. Solo costruendo ecosistemi resilienti, interoperabili e costantemente aggiornati sarà possibile garantire la fiducia dei cittadini nell'amministrazione digitale[100].

[100] In materia di appalti pubblici, il legislatore italiano prevede la necessità di soluzioni tecniche adeguate a garantire la sicurezza delle piattaforme negli artt. 19, comma 5 del Codice dei contratti pubblici e 12 del Codice dell'amministrazione digitale e impone la certificazione delle stesse da parte dell'AGID, ma resta elevato il rischio di vulnerabilità strutturali o di compromissione per errori umani o difetti progettuali, che non sono a monte prevedibili.

Le piattaforme digitali di pagamento tra Web2 e Web3: le sfide evolutive nella prospettiva della Banca d'Italia

Armando Di Cello

Il presente scritto offre una panoramica essenziale circa i comportamenti e gli sviluppi attuali nel panorama finanziario e delle loro potenziali ricadute sul consumatore. Il suo scopo principale è analizzare le tendenze emergenti che influenzano i servizi bancari e di pagamento a livello nazionale ed europeo, fornendo un quadro critico per regolatori e operatori del settore.

1. Premessa

Il settore dei sistemi di pagamento sta attraversando una fase di profondo fermento, sospinto da un'intricata convergenza di fattori normativi, tecnologici e geopolitici che, nel loro insieme, ne stanno ridefinendo l'architettura e le dinamiche di funzionamento.

Negli ultimi anni, il legislatore europeo ha progressivamente abbandonato il modello della regolazione per direttive – connotata da margini di discrezionalità nel recepimento da parte degli Stati membri – per adottare un approccio legislativo di sostanziale autonomia europea, che privilegia lo strumento del regolamento. Tale scelta segna il culmine del processo di armonizzazione e si pone come condizione essenziale per garantire uniformità interpretativa, scongiurando il rischio di frammentazione giuridica e di conseguente incertezza per gli operatori economici e per i consumatori. Resta una discrezionalità in sede di applicazione dei regolamenti, in capo però alle autorità indipendenti nazionali più che agli stati membri.

Le tematiche al centro del nuovo quadro normativo europeo sui servizi di pagamento riflettono le sfide evolutive a cui il settore è chiamato a rispondere, con particolare riferimento ai modelli tecnologici consolidatisi nell'era del Web2. In primo luogo, l'innalzamento del livello di sicurezza e, per l'effetto, della fiducia riposta nell'utilizzo delle piattaforme digitali di

pagamento, perseguito attraverso un più efficace contenimento delle frodi. In secondo luogo, una riflessione circa il perimetro applicativo della disciplina, finalizzata, sia a promuovere una leale concorrenza nel settore sia a considerare rilevanti ai fini della regolamentazione anche i servizi che abilitano e/o coadiuvano la prestazione di servizi di pagamento, sempre più offerta da nuovi operatori del mercato.

Parallelamente, la diffusione delle tecnologie riconducibili al cosiddetto Web3 evidenzia divergenze profonde tra l'approccio prudenziale europeo, improntato alla tutela della stabilità finanziaria e della sovranità monetaria, e quello statunitense, orientato a favorire lo sviluppo di valute e piattaforme private per garantire indirettamente il mantenimento della supremazia globale del dollaro. Questa diversità di impostazione accentua il rischio di arbitraggio regolatorio e di vulnerabilità sistemiche, con ricadute dirette sui consumatori e sugli utenti finali.

Sintetizziamo quindi le trasformazioni in atto nelle piattaforme digitali di pagamento, distinguendo tra i modelli riconducibili al Web2 e i modelli emergenti del Web3, ove l'attenzione si concentra sulle *stablecoins* e sulle implicazioni derivanti dalla loro adozione diffusa. L'euro digitale, nella prospettiva dell'Eurosistema, si configura come elemento di cerniera, concepito per operare come ponte tra le due dimensioni e favorire un'evoluzione graduale, ordinata e coerente del mercato europeo dei pagamenti.

2. Le piattaforme di pagamento nel Web2: rischi e mutamenti del mercato

L'ecosistema dei pagamenti digitali riconducibile al Web2 è oggi teatro di un'intensa trasformazione, i cui contorni sono in parte delineati dalla recente relazione biennale dell'*European Banking Authority* (EBA) sulle tendenze dei consumatori[101]. In particolare, il *Consumer Trends Report 2024/25* ha identificato tre aree di criticità preminenti per i consumatori dell'Unione: le frodi nei pagamenti, il crescente indebitamento e il fenomeno del *de-risking* ingiustificato. Sebbene tutte e tre le tematiche meritino attenzione, è indubbio che la lotta alle frodi mantenga una centralità assoluta in relazione all'utilizzo delle piattaforme digitali di pagamento, come peraltro confermato dall'impianto normativo e dalle finalità del nuovo pacchetto legislativo europeo composto dalla proposta di Direttiva sui Servizi di

[101] *EBA CONSUMER TRENDS REPORT* 2024/25, 26 March 2025.

Pagamento (PSD3) e dalla proposta di Regolamento sui Servizi di Pagamento (PSR)[102].

La rilevanza del fenomeno fraudolento è suffragata dai dati. Il "Rapporto sulle operazioni di pagamento fraudolente in Italia" evidenzia come, nel primo semestre del 2024, il valore dei bonifici fraudolenti ammontasse a circa 50 milioni di euro, segnando un incremento del 67% su base annua, mentre il valore delle transazioni fraudolente con carte di pagamento si attestava a 33 milioni di euro. È interessante notare, inoltre, come la principale tipologia di frode vari a seconda dello strumento: per i bonifici, la manipolazione del pagatore ha rappresentato il 74% del valore totale delle frodi, mentre per le carte, l'emissione del pagamento da parte del frodatore (ad esempio tramite *phishing* o furto di dati) ha costituito la quasi totalità dei casi[103]. Questi dati non solo quantificano l'entità del problema, ma sottolineano anche la natura multiforme e la continua evoluzione delle tecniche utilizzate.

La diffusione e l'utilizzo dei sistemi digitali di pagamento è intrinsecamente connessa alla fiducia che gli utenti vi ripongono, e tale fiducia è, a sua volta, garantita dalla percezione di sicurezza[104]. Il contenimento delle frodi assume pertanto un ruolo cardine che impone un adeguato livello di educazione finanziaria diffusa. Su questo tema, lo stato dell'arte del dibattito dottrinale e istituzionale ha raggiunto alcuni punti fermi: in primo luogo, si è consolidata la consapevolezza che il rischio di frode è tecnologicamente ineliminabile; l'idea utopica di un sistema invulnerabile ha ceduto il passo a un approccio più pragmatico, basato sulla gestione e mitigazione del rischio. In secondo luogo, è ormai acclarato che la quasi totalità delle frodi si realizza con una compartecipazione, seppur inconsapevole, dell'utente. Tale concorso ha innescato una profonda riflessione sulla ripartizione delle responsabilità tra utenti e prestatori di servizi di pagamento, conducendo alla progressiva affermazione di un modello basato sulla responsabilità oggettiva "relativa" del PSP.

Invero, pur essendo economicamente più efficiente allocare il rischio sul PSP – in quanto soggetto meglio posizionato, in un rapporto

[102] Proposta di Regolamento sui Servizi di Pagamento del mercato interno (PSR), Considerando 3.

[103] Per ulteriori dettagli, si rinvia al Rapporto sulle operazioni di pagamento fraudolente in Italia - Febbraio 2025.

[104] The level of perceived security of payment instruments affects consumer's payment choices: C. Arango, V. Taylor, *The Role of Convenience and Risk in Consumers' Means of Payment* (Bank of Canada, Discussion Papers, 2009).

strutturalmente asimmetrico, per gestire i costi delle frodi e ribaltarli poi sulla clientela sotto forma di costi del servizio – la compartecipazione dell'utente non può essere ignorata. Il regime di responsabilità che ne deriva si presenta dunque ambivalente: da un lato, si assiste a un progressivo ampliamento degli obblighi e delle responsabilità in capo ai PSP, come testimoniato dalle nuove disposizioni del PSR in materia di frodi con furto d'identità[105] e di verifica della corrispondenza IBAN/beneficiario[106]. Dall'altro lato, si richiede all'utente un livello di diligenza che varia in funzione delle condizioni in cui il soggetto versa[107]: maggiore sarà il livello di vulnerabilità digitale dell'utente, minore sarà il grado di diligenza richiesto e più complesso sarà integrare lo stato della colpa grave[108].

Proprio la nozione di colpa grave rappresenta uno dei nodi più delicati e controversi dell'intero impianto normativo. Trattandosi di *open-ended clause*, la sua concretizzazione è volutamente demandata all'interprete per evitare di cristallizzare in una formula rigida una casistica in perenne evoluzione e per consentire una valutazione parametrata sulle condizioni soggettive dell'utente (età, grado di alfabetizzazione digitale, vulnerabilità particolari). La scelta di optare per regole a carattere aperto – una tendenza che pare accentuarsi nel PSR – funzionale a garantire l'adattabilità del quadro normativo ai rapidi mutamenti del mercato, accresce l'esigenza di coerenza applicativa e impone di prevenire criticità specifiche: la difficoltà di assicurare l'uniformità delle decisioni a livello nazionale ed europeo; l'incertezza su quali condotte integrino la colpa grave con conseguente rischio di deresponsabilizzazione dell'utente; l'opinabilità del "fatto notorio" e l'efficacia esimente della *Strong Customer Authentication* (SCA)[109].

L'applicazione di norme generali rischia di condurre a un inevitabile aumento dell'incertezza e un conseguente incremento del contenzioso che, data la difficoltà dei giudici togati a tenere il passo con la

[105] *Payment Services Regulation (PSR)*, art. 59.

[106] *Payment Services Regulation (PSR)*, artt. 50 e 57.

[107] O. Ben-Shahar, A. Porat, *Personalized Law. Different Rules for Different People* (New York: Oxford University Press, 2021).

[108] Paglietti, M. Cecilia, & Rabitti, M., *"A Matter of Time. Digital-Financial Consumers' Vulnerability in the Retail Payments Market"*, European Business Law Review, vol. 33, no. Issue 4, 2022, pp. 581-606.

[109] L'esperienza ha infatti dimostrato come la SCA, pur avendo drasticamente ridotto le frodi basate sul furto di credenziali, sia inefficace contro tecniche di *social engineering* più sofisticate, come lo *spoofing*, in cui è l'utente stesso ad autorizzare, con tutti i crismi della sicurezza, un'operazione fraudolenta.

rapida obsolescenza normativa e tecnologica in materia, si riverserà in misura crescente sugli organismi di risoluzione alternativa delle controversie (ADR), come l'Arbitro Bancario Finanziario, aumentando il carico istruttorio e decisionale per le stesse autorità di vigilanza. Invero, l'assenza di indirizzi condivisi consolidati su queste tematiche e l'ampliamento della discrezionalità interpretativa di autorità, giudici e ADR può tradursi in decisioni non allineate, con effetti di frammentazione, incertezza e possibili distorsioni del *level playing field*. Al fine di mitigare tale rischio, il pacchetto di riforma attribuisce un ruolo centrale agli atti di regolazione secondaria e di *soft law* (*RTS*, linee guida)[110] nonché a meccanismi stragiudiziali, spostando l'attenzione sulla governance e sull'uniformità dell'*enforcement*[111].

Accanto alla sfida della sicurezza, il mercato del Web2 delle piattaforme digitali di pagamento è caratterizzato dalla crescente presenza di nuovi operatori e servizi[112]. La proposta di revisione della PSD2 mira a perfezionare il quadro esistente per rispondere alle nuove dinamiche competitive, tentando di perseguire un miglioramento del funzionamento dell'*open banking* e garantendo l'accesso ai sistemi di pagamento anche a PSP non bancari, al fine di promuovere una concorrenza equa[113].

La trasformazione del perimetro competitivo è resa inoltre ulteriormente evidente dal crescente ruolo nel settore delle grandi imprese tecnologiche (*BigTech*), che agiscono non solo come fornitori di tecnologie ma sempre più come erogatori diretti di soluzioni di pagamento. Peraltro, l'imprescindibilità dei servizi tecnici a supporto delle piattaforme determina oramai un rapporto di integrazione talmente pervasivo da rendere complesso tracciare una netta linea di confine tra servizio di pagamento in senso stretto e servizio tecnico a supporto. Tale circostanza, ha reso necessario procedere ad un inquadramento specifico dei servizi tecnici al fine di valutare se e quando sia adeguato estendere l'applicazione della disciplina anche alle *BigTech*[114].

---

[110] Proposta di Regolamento sui Servizi di Pagamento del mercato interno (PSR), Considerando 139.

[111] Sul punto si veda PAGLIETTI, M. CECILIA, *"Towards a European Retail Payment Law. The Role of Private Law",* European Business Law Review, vol. 36, no. Issue 5, 2025, pp. 675-694.

[112] Proposta di Regolamento sui Servizi di Pagamento del mercato interno (PSR), Considerando 1.

[113] Proposta di Regolamento sui Servizi di Pagamento del mercato interno (PSR), Considerando 31, 32, 34.

[114] SUARDI, M., *"Revisione della PSD2 e coordinamento con il MiCAR: evoluzione o rivoluzione della*

Un esempio concreto è offerto dalla diffusione dei portafogli digitali (o *digital wallet)* e dei servizi connessi alla tokenizzazione degli strumenti di pagamento su dispositivi mobili, impiegati nei pagamenti online e *contactless* presso il *Point of Interaction (POI)*. La distinzione più comune è tra *wallet pass-through*, che si limitano a tokenizzare uno strumento di pagamento esistente (es. una carta), e *wallet staged,* nei quali l'utente detiene fondi per operazioni future. I primi sono considerati servizi tecnici e quindi, in linea di principio, esclusi dalla regolamentazione (pur vedendosi applicare specifiche disposizioni)[115]; i secondi, invece, rientrando all'interno della definizione di "strumento di pagamento" e "servizio di pagamento"[116], sono soggetti all'applicazione integrale della disciplina.

L'analisi dell'assetto applicativo dei servizi di pagamento nel quadro di revisione della PSD2 mostra pertanto come la frontiera regolatoria si stia spostando verso l'intersezione tra funzioni di pagamento e servizi tecnologici abilitanti. In questo snodo, i *technical service provider* rappresentano uno dei banchi di prova principali: a fronte di un'opzione che ne conferma l'estraneità al perimetro dei servizi di pagamento, pur assoggettandoli selettivamente ad alcune regole, si è affacciata una soluzione più incisiva che, senza "finanziarizzare" i *TSP*, li ricomprende entro specifici obblighi del pacchetto PSD3/PSR. Quest'ultima prospettiva, ampliando l'orizzonte soggettivo della disciplina, ha un maggiore coefficiente innovativo, perché riconosce la rilevanza sistemica di attori non finanziari nella catena del valore dei pagamenti[117].

In termini più generali, emerge con evidenza come la principale sfida per il legislatore europeo risieda proprio nella capacità di intercettare le nuove dimensioni tecnologiche e le molteplici tipologie di servizi che gravitano attorno al settore dei pagamenti. L'efficacia della futura disciplina dipenderà dall'abilità nel definire categorie giuridiche sufficientemente precise da garantire un ambiente competitivo privo di distorsioni, ma al contempo abbastanza flessibili da non essere superate dall'evoluzione del mercato.

---

disciplina sui servizi di pagamento?" in Mercati, infrastrutture, sistemi di pagamento della Banca D'Italia, n. 54, ottobre 2024.

[115] Proposta di Regolamento sui Servizi di Pagamento del mercato interno (PSR), art. 2(2)(i).

[116] PSD2, art. 4.

[117] Sul tema si veda Consiglio dell'Unione europea (2021), p. 11.

3. L'Euro digitale, un ponte tra Web2 e Web3

Alle profonde trasformazioni che stanno ridefinendo il panorama delle piattaforme digitali di pagamento si aggiunge, quale elemento di mediazione tra Web2 e Web3, il progetto dell'euro digitale. La Banca Centrale Europea, al pari di altre autorità monetarie a livello globale, sta concretamente esplorando la possibilità di emettere una propria valuta digitale (*Central Bank Digital Currency* - CBDC), sia in una forma destinata al grande pubblico (*retail*), sia in una variante per le transazioni interbancarie (*wholesale*). La finalità principale è dotare l'Eurosistema di un'àncora monetaria pubblica nell'era digitale, capace di preservare le garanzie connesse all'uso della moneta di banca centrale e, al contempo, di fungere da veicolo per l'innovazione, estendendo in modo graduale e ordinato l'uso di tecnologie a registro distribuito alle infrastrutture di pagamento.

La componente *wholesale* dell'euro digitale, in particolare, si pone come il terreno di sperimentazione più avanzato per l'integrazione delle tecnologie DLT nelle infrastrutture di pagamento critiche. Nei pagamenti all'ingrosso i meccanismi di integrazione tra DLT e moneta di banca centrale mirano a preservare l'unico ancoraggio che il diritto riconosce come *risk-free* per il *settlement*. È in questo ambito che si collocano le soluzioni esplorative avanzate da diverse banche centrali nazionali dell'Eurosistema. La Banca d'Italia, ad esempio, ha sperimentato l'interoperabilità tra l'infrastruttura di regolamento istantaneo TIPS *(TARGET Instant Payment Settlement)* e piattaforme DLT esterne, attraverso soluzioni in grado di far comunicare i sistemi su cui vengono scambiati gli asset digitali e i sistemi che forniscono servizi di regolamento in moneta di banca centrale[118]. In tal modo verrebbe garantito a queste operazioni di confluire nelle infrastrutture dei mercati tradizionali mantenendo la moneta "ufficiale" al centro del processo di regolamento di attività finanziariamente sempre più rilevanti.

Le architetture sperimentate nell'ambito dell'Eurosistema – in cui un evento su registro distribuito condiziona o attiva un regolamento in moneta di banca centrale nello strato *legacy* – segnalano un approccio di continuità regolatoria e di sperimentazione controllata, volto a evitare rotture brusche nel presidio dei rischi. In particolare, queste soluzioni concepiscono la DLT come strato di coordinamento e condizionalità,

[118] Per un approfondimento sul tema: paper n. 26 del 2022, *"Integration of DLTs with market infrastructures: analysis and proof of concept for a secure DvP between TIPS and DLT platforms"*, in Mercati, infrastrutture, sistemi di pagamento della Banca D'Italia.

lasciando che la finalità finanziaria risieda comunque in ambiente sorvegliato e governato dall'autorità monetaria. Tale impostazione consente di testare benefici come la riduzione del *time-to-settle* per operazioni complesse, la possibilità di *delivery-versus-payment (DvP)* e *payment-versus-payment (PvP)* programmabili, nonché il miglioramento della trasparenza sugli stati di avanzamento delle transazioni, preservando al contempo l'integrità del perimetro prudenziale.

L'orizzonte di lungo periodo prospetta, invece, soluzioni ancora più radicali che superano la logica del "ponte" tra mondi distinti. L'ipotesi sarebbe quella di approdare a un registro condiviso e unificato in cui moneta di banca centrale, depositi commerciali e altri attivi finanziari coesistono nativamente. L'obiettivo ultimo è abbattere le frizioni strutturali del sistema finanziario e abilitare un'innovazione *end-to-end*, dal momento dell'emissione a quello del regolamento finale[119].

Parallelamente all'innovazione nel comparto *wholesale*, una riflessione non meno cruciale investe il futuro dei pagamenti al dettaglio e il ruolo della moneta pubblica in un contesto di crescente digitalizzazione. Storicamente, la fiducia nel sistema monetario si basa sulla disponibilità del contante, emesso dalle banche centrali quale bene pubblico esente da rischio di credito e di liquidità. Tale funzione, che garantisce la convertibilità e la stabilità di valore anche delle valute private, è oggi messa in discussione dalla progressiva contrazione dell'uso di banconote e monete nelle transazioni quotidiane e dalla contestuale diffusione di mezzi di pagamento alternativi emessi da soggetti privati. Ciò ha maturato tra le istituzioni bancarie europee la profonda convinzione che l'assenza di una forma digitale di moneta di banca centrale al dettaglio rischi, in prospettiva, di marginalizzarne il ruolo, alterando il delicato equilibrio tra moneta pubblica e moneta privata che ha finora sostenuto la stabilità e la sovranità monetaria dell'Eurosistema.

Anche in questo caso, il progetto di un euro digitale, concepito non come mera innovazione tecnologica ma come l'evoluzione necessaria del contante per l'era digitale, si propone come possibile risposta di sistema finalizzata a mantenere la moneta di banca centrale quale *medium* di estinzione delle obbligazioni pecuniarie. L'obiettivo è quello di preservare l'accesso diretto dei cittadini a un mezzo di pagamento pubblico, sicuro e

[119] La strategia dualistica dell'Eurosistema è stata delineata nel corso dei lavori esplorativi sulle nuove tecnologie per il regolamento all'ingrosso della moneta della banca centrale, di cui al report: <https://www.ecb.europa.eu/press/pubbydate/2025/html/ecb.exploratoryworknewtechnologies202506.it.html>.

garante della privacy, assicurando che la moneta di banca centrale continui a svolgere la sua funzione essenziale di stabilizzazione e di unità di conto, anche in un ecosistema dominato da soluzioni di pagamento private.

4. *Stablecoins*: opportunità o minaccia?

L'urgenza di un intervento pubblico europeo assume una connotazione ancor più strategica in ragione della rapida ascesa di iniziative private, in particolare delle cosiddette *stablecoins*. Questi strumenti, concepiti per mantenere un valore stabile ancorato a un asset di riferimento come una valuta fiat, si propongono quale chiave di accesso all'ecosistema decentralizzato del Web3.

A livello globale, la capitalizzazione di mercato delle *stablecoins* è cresciuta esponenzialmente, rappresentando una quota sempre più rilevante dell'intero mercato delle cripto-attività. Tuttavia, pur essendo tra i principali mezzi di regolamento in protocolli di finanza decentralizzata, il loro utilizzo con funzione di pagamento è ancora molto limitato[120].

La risposta regolamentare alla diffusione di questo fenomeno ha seguito percorsi marcatamente divergenti, scavando un solco profondo tra l'approccio europeo e quello statunitense. Da un lato, l'UE si trova a dover giocare un ruolo da mediatore privilegiando un'internalizzazione *ex ante* dei rischi, attraverso la regolamentazione del mercato e il controllo della moneta (*MiCAr*[121]*,* sorveglianza e integrazione dei sistemi di pagamento, euro digitale). Il regolamento *MiCA,* in particolare, riconosce che l'adozione diffusa delle *stablecoins* può generare criticità per il regolare funzionamento dei sistemi di pagamento e per la stessa sovranità monetaria[122]. Per questo, impone agli emittenti stringenti requisiti autorizzativi, patrimoniali e di governance, nonché l'obbligo di costituire e mantenere riserve di attività liquide e a basso rischio per garantire il diritto di rimborso dei possessori.

[120] Alcune stime circa l'utilizzo di *stablecoins* con funzione di pagamento sono riportate in: Boston Consulting Group, *"Stablecoins, five killer tests to gauge their potential"*, 2024; nonché in *"Report on the payment attitudes of consumers in Italy: results from ECB SPACE 2024 survey",* in Mercati, infrastrutture, sistemi di pagamento della Banca D'Italia, n. 68 del 2025.

[121] Regolamento (UE) 2023/1114

[122] Atti del Convegno *"Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento"* in Quaderni di Ricerca Giuridica della consulenza legale, Banca d'Italia, 29 settembre 2023.

Dall'altro lato, gli Stati Uniti appaiono favorire un approccio prevalentemente *market driven*, dove la diffusione di *stablecoins* emesse da soggetti privati, e ancorate al dollaro statunitense, viene vista non come una minaccia, ma come un veicolo per perpetuare la centralità del dollaro nell'ecosistema finanziario digitale globale (così il *Genius Act*). Questa strategia, di fatto, esternalizza l'innovazione monetaria al settore privato, puntando a mantenerne il controllo attraverso il ruolo egemonico della propria valuta.

Tuttavia, anche all'interno delle istituzioni UE emergono tensioni riguardo alcuni aspetti applicativi della regolamentazione in materia. Ne sono un esempio le recenti posizioni dell'*EBA* in seguito alle modifiche introdotte dalla Commissione sui requisiti di liquidità e composizione delle riserve. Anche in questo caso, il conflitto nasce dalla contrapposizione tra un approccio più flessibile e orientato al mercato e uno maggiormente prudenziale[123].

Questa frammentazione regolamentare a livello internazionale solleva significative preoccupazioni[124]. In primo luogo, l'esistenza di regimi normativi con livelli di rigore differenti crea un evidente rischio di arbitraggio regolamentare, spingendo gli operatori a localizzare le proprie attività nelle giurisdizioni con la vigilanza meno stringente; in secondo luogo, emergono vulnerabilità sistemiche legate a modelli operativi transfrontalieri complessi, come nel caso di *multi-issuance stablecoins*. In questi paradigmi, i token sono emessi da entità uniche con sedi in giurisdizioni differenti, creando un disallineamento tra le passività di un emittente (che potrebbe essere chiamato a rimborsare token emessi all'estero) e le attività di riserva detenute localmente, esponendo i possessori europei a rischi legali, operativi e di liquidità che originano al di fuori dell'Unione[125].

[123] Il riferimento è ai due Opinions – EBA/Op/2025/13 e EBA/Op/2025/14 – pubblicati il 9 ottobre 2025, in cui l'EBA critica la proposta (introdotta dalla Commissione nei drafts delle RTS) di riduzione dei vincoli di liquidità sulle riserve. Nello specifico, l'EBA sostiene che consentire agli emittenti di investire le riserve anche in asset non altamente liquidi equivarrebbe a ridurre il livello minimo di solidità imposto da MiCA, a creare incoerenze normative e rischi di arbitraggio regolamentare con il settore bancario, nonché potenziali vulnerabilità sistemiche.

[124] Per un confronto tra l'approccio regolamentare europeo e quello statunitense: Odinet, C., Tosato, A., (forthcoming, 2026), *"Regulating Stablecoins: Comparing MiCAR and GENIUS Act"*, Notre Dame Law Review Reflection.

[125] Sul tema vedi, Chiara Scotti *"Stablecoins in the Payments Ecosystem: Reflections on Responsible Innovation"*, welcome address for Economics of Payments XIV Conference, Rome, 18

Le *stablecoins* promettono di aumentare l'efficienza dei pagamenti attraverso la creazione di un'infrastruttura finanziaria più aperta, capace di consentire transazioni quasi istantanee e atomiche, dove lo scambio di un bene o servizio e il relativo pagamento avvengono simultaneamente e in maniera indissolubile, annullando il rischio di controparte. L'attrattività dei sistemi di pagamento tradizionali, pertanto, viene messa in discussione dall'emergere di tali architetture tecnologiche, caratterizzate da meccanismi di consenso e di programmazione del trasferimento di valore che si propongono come alternativi o complementari alle piattaforme digitali del Web2.

Tuttavia, è opportuno mantenere un approccio regolamentare prudente e coordinato a livello globale che consenta di evitare forme di arbitraggio regolamentare, prevenire rischi di sostituzione valutaria e tutelare la stabilità finanziaria.

5. Conclusioni

L'esperienza della PSD2 ha palesato come, persino in regime di armonizzazione massima, interpretazioni e applicazioni divergenti a livello nazionale possano generare frammentazione, incertezza, rischi di *forum shopping* e alterazioni del *level playing field*.

Il passaggio ad una legislazione per regolamenti è una risposta diretta a questa criticità. Tale dinamica segna il culmine del processo di armonizzazione e sposta inevitabilmente il baricentro del dibattito sull'uniformità dell'*enforcement*. L'efficacia del nuovo quadro normativo, articolato e multilivello, dipenderà non tanto dal tenore letterale della norma, quanto da una sua coerente applicazione nei mercati di ciascuno Stato membro.

Le autorità di vigilanza sono pertanto chiamate ad un'assunzione di responsabilità di cruciale importanza, che possono perseguire attraverso due direttrici concorrenti: una prima, "verticale", che consiste nell'aderire con rigore alle indicazioni interpretative fornite dalle agenzie di regolazione europee. Sebbene tali atti rientrino nella categoria della *soft law*, la loro autorevolezza tecnica e la capacità di promuovere un'applicazione uniforme li rendono un riferimento imprescindibile. Ignorarli equivarrebbe a rinunciare all'opportunità di contribuire a un mercato unico dei pagamenti

September 2025; o, General Secretariat of the Council of the European Union (2025), *"Non-paper on EU and third country stablecoin multi-issuance"*; o ancora, Arnal J. (2025), *"Multi-issuance stablecoins and MiCA's first real credibility test"*.

realmente integrato. Una seconda, "orizzontale", attiene alla necessità di coordinare le diverse autorità di controllo, per dirimere preventivamente eventuali conflitti di competenze. Accordi di collaborazione e una chiara delimitazione dei rispettivi ambiti di intervento sono essenziali per non disorientare né gli operatori di mercato né i consumatori.

L'incertezza sull'effettività della tutela e sulla portata dei propri diritti rappresenta un potente disincentivo all'utilizzo di nuovi servizi, con un conseguente impatto negativo sulla domanda di innovazione e sulla gestione dei contenziosi. In un contesto in cui la rapidità dei cambiamenti tecnologici e regolamentari rende arduo per la giustizia ordinaria consolidare orientamenti giurisprudenziali stabili, il contenzioso si riverserà inevitabilmente e in misura crescente sui meccanismi di risoluzione alternativa delle controversie, come l'Arbitro Bancario Finanziario. La sfida principale, dunque, non è più solo comprendere cosa dice la norma, ma definire con chiarezza e coerenza come essa debba essere applicata, per bilanciare innovazione e stabilità, e per garantire che la transizione digitale avvenga all'insegna della certezza del diritto.

Consob e piattaforme digitali: fra *robo-advisory*, *gamification* e *blockchain*

Matteo Ghezzi

Il contributo analizza il ruolo della Commissione Nazionale per le Società e la Borsa nell'affrontare le sfide poste dall'innovazione tecnologica nei mercati finanziari, con particolare riferimento alla robo-advisory, alla gamification degli investimenti e alla diffusione di cripto-attività nel contesto del Web 3.0. L'analisi evidenzia le criticità per la tutela degli investitori e la necessità di un quadro di vigilanza coerente, capace di armonizzare regolazione e innovazione tecnologica, evitando rischi sistemici e garantendo trasparenza, fiducia e protezione dei consumatori.

1. Premessa

La disamina dei profili di interesse e delle criticità connesse, da un lato, all'operatività delle piattaforme digitali nel contesto del Web 2.0 e, dall'altro lato, allo sviluppo della tecnologia *blockchain* e del mercato dei *cripto-assets*, presuppone alcuni cenni introduttivi in merito alla nozione di Web 3.0 e al suo rapporto evolutivo con il Web 2.0, anche nell'ottica di comprendere il cruciale ruolo che le autorità di vigilanza assumono nel suddetto ambito.

Il Web 2.0 si riferisce a piattaforme digitali caratterizzate da interoperabilità, usabilità e condivisione di informazioni tra gli utenti e da un modello di *business* centralizzato che opera tramite l'acquisizione, aggregazione e monetizzazione dei dati, con *governance* accentrata e distribuzione dei profitti a *manager* e *shareholders*[126].

[126] F. BASSAN, *Web 3 in Transition and participatory regulation*, in *CPI-Tech Cronicle*, 2023, 3; D. W. WILSON, X. LIN, P. LONGSTREET, S. SARKER, *Web 2.0: A Definition, Literature Review, and*

Diversamente, il Web 3.0, anche definito *web semantico* o *web decentralizzato*, è costituito da una tecnologia di registro distribuito (*Distributed Ledger Technology*) le cui implementazioni includono, *inter alia*, la tecnologia *blockchain* che consente la creazione di modelli di *business* decentralizzati, idonei a garantire agli utenti un maggiore controllo sui propri dati. L'operatività del Web 3.0 risulta contrassegnata dall'implementazione di *smart contracts* (algoritmi che rendono automatizzata l'esecuzione delle transazioni), da meccanismi di *governance* (condivisi dalla comunità di utenti) e di distribuzione dei profitti a utenti e creatori[127].

Lo sviluppo del Web 3.0 è connesso anche all'utilizzo di sistemi di intelligenza artificiale che consentono alle macchine di comprendere il linguaggio naturale, rendendo i contenuti in linea con le preferenze individuali e assicurando risultati di ricerca più accurati[128]. Anche nel Web 2.0, invero, si è assistito a un'evoluzione in termini di utilizzo di sistemi IA che, in primo luogo, ha permesso alle piattaforme digitali, attraverso analisi predittive, di ottimizzare la profilazione degli utenti, lo sviluppo di meccanismi di pubblicità mirata e di raccomandazione[129]; in secondo luogo, l'IA ha consentito l'efficientamento delle attività connesse alla moderazione automatica dei contenuti[130]. In sostanza, l'intelligenza artificiale assume un ruolo trasversale rispetto a Web 2.0 e Web 3.0.

Il passaggio qualitativo[131] da Web 2.0 a Web 3.0 ha origine dall'aumento dei dati generati da utenti e dispositivi e dalla conseguente esigenza di una gestione più efficiente delle informazioni nonché di maggiori livelli di *privacy* e sicurezza[132]. In tale contesto, la grande sfida del legislatore, anche con il supporto delle autorità di vigilanza (si pensi alla Consob e alla Banca

Directions for Future Research, in AMCIS, 2011, 1 ss.

[127] F. Bassan, *Web 3 in Transition and participatory regulation*, cit.; Sul punto anche, M. Nasar, *Web 3.0: A Review and its Future*, in *International Journal of Computer Applications*, 2023, 41 ss.

[128] Nasar, *Web 3.0: A Review and its Future*, cit., 41.

[129] Nei *social media*, tali meccanismi generano i noti fenomeni di *echo chamber* e *filter bubbles*. Per approfondimenti, v. E. Longo, *The Risks of Social Media Platforms for Democracy: A Call for a New Regulation*, in B. Custers, E. Fosch-Villaronga (a cura di), *Law and Artificial Intelligence, Regulating AI and Applying AI in Legal Practice*, in *Information Technology and Law Series*, 35, 2022, 76 ss.

[130] Per approfondimenti v. A. Loreggia, G. Sartor, *L'intelligenza artificiale nella moderazione del digitale*, in *Sistemi intelligenti*, 1, 2022, 53 ss.

[131] Bassan, *Web 3 in Transition and participatory regulation*, cit., 3.

[132] Nasar, *Web 3.0: A Review and its Future*, cit., 41.

d'Italia), è quella di compiere vere e proprie scelte di valore[133] per assicurare coerenza, e, al contempo, coesistenza tra i due modelli, nonché mitigare gli effetti distorsivi da un non corretto utilizzo del Web.

Nel prosieguo si tratteranno i profili di interesse e le criticità oggetto di maggior attenzione da parte delle competenti autorità di vigilanza – in particolare, della Consob – relativi al Web 2.0 e al Web 3.0 e ai fenomeni che in concreto si innestano in dette infrastrutture.

2. La *robo-advisory* nell'infrastruttura Web 2.0

In primo luogo, per cogliere appieno le recenti sfide delle autorità di vigilanza nell'ambito del Web 2.0, appare opportuno analizzare la *robo-advisory*. Trattasi di un fenomeno ampiamente dibattuto in letteratura, in quanto emblematico della trasformazione dei mercati finanziari attraverso l'innovazione tecnologica.

I *robo-advisor* sono piattaforme digitali di consulenza finanziaria che, mediante l'elaborazione di ingenti quantità di dati e l'impiego di sistemi IA, forniscono raccomandazioni d'investimento con un livello minimo, se non del tutto assente, di intervento umano. L'evoluzione dei *robo-advisor* è stata profondamente influenzata dall'introduzione di tecnologie basate sull'intelligenza artificiale. Se, originariamente, le piattaforme si fondavano su modelli standard di ottimizzazione del portafoglio, quelle più recenti si caratterizzano per l'impiego crescente di strumenti sofisticati, quali algoritmi di *machine learning*, sistemi di *natural language processing* e meccanismi avanzati di raccomandazione personalizzata. È ormai noto come la *robo-advisory* offra continuità e immediatezza, sia in grado di ridurre alcuni *bias* derivanti da scelte discrezionali e favorisca previsioni tempestive sugli andamenti di mercato. Onde, una significativa riduzione dei costi di distribuzione dei servizi di consulenza e, al contempo, una maggiore redditività per gli intermediari[134].

Tuttavia, emergono alcuni profili di rischio; in Italia, la Consob ha

[133] F. Bassan, *Web 3 in Transition and participatory regulation*, cit., 3; F. Bassan, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain'*, in *Rivista di Diritto Bancario*, 2023, 563.

[134] Basti pensare che secondo le statistiche da circa 300 miliardi di dollari di *asset under management* stimati nel 2017, avrà luogo un potenziale incremento fino a oltre 4.500 miliardi entro il 2027; v. G. Cardillo, H. Chiappini, *Robo-advisors: A systematic literature review,* in *Finance Research Letters*, 62, 2024, 1.

più volte segnalato come l'adozione di modelli di consulenza automatizzata debba essere accompagnata da adeguati presìdi di trasparenza affinché l'utilizzo di algoritmi non comprometta il *best interest of the client*[135]. Si intende garantire un servizio conforme ai principi di adeguatezza e correttezza, evitando che l'opacità tecnologica provochi lacune di tutela.

Più nel dettaglio, risultano problematici i confini interpretativi della nozione di "consulenza personalizzata"; con tale espressione, la disciplina europea e nazionale di riferimento – la MiFID II e il TUF – si riferisce al servizio diretto al pubblico attraverso piattaforme digitali. Ciò sembra dunque escludere alcuni servizi offerti dai *robo-advisor*, quali le raccomandazioni di *asset allocation* del portafoglio, le informazioni generali e specifiche per l'esecuzione di transazioni nonché il supporto dell'attività del personale dell'intermediario[136].

Sotto altro profilo, rilevano talune criticità relative ai questionari online. Come noto, l'identificazione dei profili degli investitori è centrale nella prestazione del servizio; tuttavia, l'assenza di un operatore umano[137] genera il rischio, per gli utenti meno esperti, di fraintendere le domande, fornire dati inesatti o interpretare in modo distorto i suggerimenti ricevuti[138]. Analogamente, ci si interroga se i *robo-advisor* siano in grado di svolgere una valutazione realmente esaustiva della situazione complessiva del cliente in circostanze atipiche, di adattarsi a risposte non previste dal modello o di cogliere anomalie nei comportamenti e nelle attitudini indivi-

[135] 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, art. 24.

[136] Gruppo di lavoro CONSOB, Scuola Superiore Sant'Anna di Pisa, Università Bocconi, Università di Pavia, Università di Roma 'Tor Vergata', Università di Verona, *La digitalizzazione della consulenza in materia di investimenti finanziari*, Quaderni FinTech, 3, 2019, 8.

[137] Il grado di automazione nei servizi di consulenza finanziaria può variare, consentendo di distinguere tra *robo-advisor* con algoritmo e interfaccia fisica, soluzioni "ibride", e modelli completamente automatizzati; v. P. Pia, *La consulenza finanziaria automatizzata,* Franco Angeli, Banca Finanza e PMI, Milano, 2017, 112.

[138] R. Feng, H. Li, M. Liu, *Robo-Advisors Beyond Automation: Principles and Roadmap for AI-Driven Financial Planning,* September 12, 2025, 7 ss. reperibile su SSRN al seguente link: <https://ssrn.com/abstract=5473746>.

[138] Concetto delineato da F. Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Ex-plainability in an Algorithmic Society,* in *Ohio State Law Journal*, 78, 5, 2017, 1243 ss.

duali[139]. Proprio la mancanza di sensibilità rispetto alle sfumature comunicative e agli aspetti emotivi del rapporto fiduciario con l'investitore rappresenta, in questa prospettiva, uno dei principali limiti strutturali della consulenza automatizzata[140].

A ciò si aggiunga che l'operatività dei *robo-advisor* rimane talvolta limitata alla consulenza sugli investimenti, con particolare riferimento alla costruzione e gestione dei portafogli, all'allocazione degli *asset*, al ribilanciamento periodico e all'ottimizzazione fiscale. Tale impostazione deriva dal loro *design*, ideato per offrire soluzioni di investimento efficienti e a basso costo, ma non per soddisfare in *toto* le esigenze di pianificazione finanziaria di lungo periodo[141].

Un ulteriore limite significativo riguarda l'opacità algoritmica e l'affidabilità delle raccomandazioni. Gran parte delle piattaforme si fonda su modelli di valutazione di proprietà e su motori di raccomandazione il cui funzionamento interno non è sempre accessibile in larga misura ai clienti (cd. *black box*)[142]. Ciò impedisce ai clienti di comprendere le logiche sottostanti alle proposte ricevute e di verificare se esse colgano appieno le loro necessità.

La letteratura ha inoltre rilevato che le raccomandazioni algoritmiche non risultano sempre coerenti tra loro, considerando che investitori con profili simili possono ricevere indicazioni divergenti in funzione della frequenza di aggiornamento dei dati o della diversa ponderazione attribuita a variabili marginali nei questionari di profilazione[143]. Sorgono, dunque, dubbi sull'effettiva origine di tali divergenze che potrebbero dipendere non tanto da mutamenti sostanziali delle condizioni di mercato, bensì da modifiche e/o aggiornamenti arbitrari del modello. Al riguardo, alcune autorità

---

[139] Feng, Li, Liu, *Robo-Advisors Beyond Automation: Principles and Roadmap for AI-Driven Financial Planning,* cit.

[140] Ed invero, la dimensione fiduciaria e relazionale costituisce un fattore decisivo nell'accettazione della consulenza automatizzata. Sul punto v. C. Cruciani, G. Gardenal, L. Tonon, *Fiducia e accettazione del consiglio di investimento: consulenza tradizionale e automatizzata a confronto*, in *Bancaria*, 4, 2024, 10 ss.

[141] Feng, Li, Liu, *Robo-Advisors Beyond Automation: Principles and Roadmap for AI-Driven Financial Planning,* cit.

[142] Concetto delineato da F. Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Ex-plainability in an Algorithmic Society,* in *Ohio State Law Journal*, 78, 5, 2017, 1243 ss.

[143] P. Kofman, *Scoring the Ethics of AI Robo-Advice: Why We Need Gateways and Ratings*, in *Journal of Business Ethics,* 198, 2025, 21 ss.

di vigilanza hanno evidenziato come l'utilizzo di strumenti di *machine learning* poco trasparenti renda più complessa l'attività di supervisione e, di conseguenza, la tutela dell'investitore[144].

Pertanto, la sfida delle autorità non si limita ad assicurare l'osservanza del principio di adeguatezza, ma si estende all'esigenza di tracciabilità delle logiche decisionali sottostanti ai servizi di consulenza automatizzata e alla presenza di un adeguato controllo umano. In prospettiva, sarà necessario valutare l'eventuale impatto dell'*Artificial Intelligence Act*[145] che, pur non menzionando espressamente i *robo-advisor* tra i sistemi IA "ad alto rischio", introduce principi di trasparenza e *accountability* che potrebbero trovare applicazione anche in questo settore, soprattutto laddove tali sistemi incidano in modo significativo sulle decisioni di investimento dei clienti[146].

[144] *Ex multis*, P. Deriu, S. Racioppi, con presentazione a cura di A. Lalli, *Riflessioni in tema di intelligenza artificiale e attività di vigilanza*, Quaderni FinTech, Consob, 15, 2025; Speech by L.F. Signorini, *Artificial Intelligence in Finance,* Durban, South Africa, 17 luglio 2025, reperibile al seguente link: <https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2025/20250717-signorini/Signorini-17.07.2025.pdf>; ESMA, *Public Statement On the use of Artificial Intelligence (AI) in the provision of retail investment services,* 30 maggio 2024, reperibile al seguente link: <https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924_Public_Statement_on_AI_and_investment_services.pdf>; EBA, *Risk assessment report of The European Banking Authority,* novembre 2024, 86 ss., reperibile al seguente link: <https://www.eba.europa.eu/sites/default/files/2024-11/f03ee0c1-7258-4391-8bf1-578924956049/EBA%20Risk%20Assessment%20Report%20-%20Autumn%202024.pdf>.

[145] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[146] Per alcune riflessioni in merito alla potenziale applicabilità dell'*Artificial Intelligence Act* sui servizi di *robo-advisor* v. T. Myklebust, F.M. Mancioppi, *Financial literacy: still a priority for the well-functioning of financial markets*, in *Law and Economics Yearly Review*, in corso di pubblicazione, 2025, 14; A. Sciarrone Alibrandi, M. Rabitti, G. Schneider, *The European AI Act's Impact on Financial Markets: From Governance to Co-Regulation,* in *EBI Working Paper Series*, 138, 2023, 22 ss.

3. La maggiore esposizione al rischio di investimento alla luce del fenomeno "gamification"

Un'ulteriore area di interesse concerne la *gamification,* intesa come l'utilizzo di meccanismi propri del gioco in ambiti estranei al contesto ludico[147].

Il fenomeno, coniato nel 2011, si è diffuso in molteplici ambiti fra cui la finanza digitale[148] con l'adozione di interfacce "gamificate" nelle piattaforme di *trading* e investimento.

La *gamification*, da un lato, appare uno strumento utile ad avvicinare i consumatori, soprattutto più giovani, a tematiche finanziarie di rilievo, favorendo al contempo una maggiore inclusione attraverso la semplificazione di concetti complessi. Dall'altro lato, tuttavia, l'accesso diretto degli investitori *retail* ai mercati finanziari mediante piattaforme digitali di tal genere ha introdotto molteplici rischi comportamentali considerando che, spesso, le decisioni di investimento sono assunte con la stessa leggerezza con cui si partecipa ad un videogioco. Tale pericolo ha spinto le autorità di vigilanza, fra cui la Consob[149], a estendere la propria attività di supervisione sul mercato nei confronti delle piattaforme finanziarie che integrano modelli di *gamification*, con l'obiettivo ultimo di valutarne l'impatto sulla tutela degli investitori.

Ed invero, nelle piattaforme di investimento gamificate i consumatori ottengono – oltre al risultato finanziario derivante dalla decisione di investimento stessa – un valore aggiunto attraverso il conseguimento di un obiettivo prestabilito[150] (come accumulare più punti rispetto agli altri, raggiungere per primi un traguardo o sconfiggere gli avversari secondo parametri quantificabili). Onde, un ambiente stimolante e competitivo per l'utente che induce i consumatori a impegnarsi con l'intento di "vincere"

---

[147] S. Detering, D. Dixon, R. Khaled, L. Nacke, *From Game Design Elements to Gamefulness: Defining "Gamification"*, in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environment*, 2011, 9 ss.

[148] Basti pensare che la base di clienti della nota piattaforma Robinhood è aumentata fino a 25,2 milioni del 2024; sul punto v. <https://investors.robinhood.com/news-releases/news-release-details/robinhood-reports-fourth-quarter-and-full-year-2024-results>.

[149] Sul punto, v. Comunicato stampa Consob, *Gamification: l'investimento finanziario non è un "videogioco",* 20 gennaio 2025, reperibile al seguente link: <https://www.consob.it/documents/d/asset-library-1912910/cs_20250120>.

[150] C. Hüller, M. Reimann, C. Warren, *When Financial Platforms Become Gamified, Consumers' Risk Preferences Change*, in *Journal of the Association for Consumer Research*, 2023, 3.

all'interno dell'ambiente gamificato[151].

Ne deriva che la *gamification* nelle piattaforme di investimento può indurre gli utenti, attraverso tecniche di *nudge*, ad assumere comportamenti più rischiosi considerando, in aggiunta, l'utilizzo di sistemi IA che agevolano, mediante meccanismi di *machine learning* e *data analytics*, la personalizzazione del servizio e la profilazione dell'utente. In tale contesto, dunque, l'obiettivo non è solo l'ottimizzazione del rendimento finanziario, ma altresì il raggiungimento del traguardo competitivo fissato dal gioco[152]. Al riguardo, l'ESMA ha evidenziato come il ricorso a tecniche di *gamification* possa generare dinamiche di dipendenza nei clienti *retail* idonee ad innalzare i rischi di investimento assunti (come emerso a seguito del caso *GameStop*), potenzialmente in contrasto con il miglior interesse dell'investitore e con i requisiti previsti dalla MiFID II[153].

Appare evidente che i rischi sinora esaminati si manifestino anche, e in misura potenzialmente amplificata, nelle piattaforme di *trading* online che integrano meccanismi di *gamification*. Ed invero, il breve periodo operativo tipico del *trading* accresce la frequenza delle operazioni e la propen-

[151] K.P.Y. Lai, P. Langley, *Playful finance: Gamification and intermediation in FinTech economies*, in *Geoforum,* 151, 2024, 3.

[152] Se tale ipotesi è vera, è altrettanto ragionevole considerare che i suddetti obiettivi esercitano una forza motivante sugli utenti finché non risultano conseguiti; una volta raggiunti, tale effetto tende infatti ad attenuarsi. In questa prospettiva, è plausibile ipotizzare che la gamification incrementi l'assunzione di rischi finanziari principalmente nei casi in cui i consumatori non abbiano ancora accumulato guadagni sufficienti a soddisfare l'obiettivo competitivo imposto dal gioco. Viceversa, laddove tale obiettivo sia già stato raggiunto, è verosimile che gli investitori mostrino una propensione al rischio analoga, o persino inferiore, rispetto a quella che manifesterebbero in un contesto privo di elementi gamificati. Sul punto, v. Hüller, Reimann and Warren, *When Financial Platforms Become Gamified, Consumers' Risk Preferences Change*, cit.

[153] La potenziale applicabilità della MiFID II alle piattaforme che utilizzano tecniche di *gamification* e di *nudging* dipende dal grado di personalizzazione della comunicazione rivolta al cliente. Se, ad esempio, una piattaforma invia pop-up, notifiche o e-mail che spingono l'utente a effettuare una transazione su uno specifico strumento finanziario, tenendo conto delle sue caratteristiche personali o del suo profilo, tale sollecitazione può essere qualificata come una raccomandazione di investimento personalizzata. In questo caso, l'impresa è tenuta a raccogliere dal cliente tutte le informazioni necessarie per svolgere una valutazione di adeguatezza e a utilizzarle nel formulare la raccomandazione, in linea con gli obblighi MiFID II. Sul punto, v. C. Brescia Morra, D. Colonnello, M. Gargantini, G. Sandrelli e G. Trovatore, *La gamification degli investimenti finanziari*, Quaderno giuridico Consob, 32, 2025, 13.

sione al rischio, in particolare fra utenti privi di un'adeguata educazione finanziaria[154]. Recenti studi empirici hanno rilevato che nonostante tale dinamica aumenti il volume degli scambi al dettaglio, la stessa può altresì pregiudicare la posizione dell'investitore *retail*. La *gamification* tende a ridurre la qualità delle strategie di *trading* provocando, di conseguenza, una riduzione dei rendimenti giornalieri e una maggiore volatilità dei rendimenti individuali. In sostanza, gli investitori *retail* devono sostenere i costi della *gamification*; *gamification* di cui, invece, beneficiano i fornitori di liquidità e gli intermediari finanziari in quanto il fenomeno in esame riduce la tossicità del flusso di ordini al dettaglio. Questa divergenza solleva questioni rilevanti per l'attività di vigilanza in merito al ruolo prorompente dell'innovazione digitale nell'orientare il comportamento del mercato[155].

4. Web 3.0, *blockchain* e *cripto-assets* tra innovazione, regolazione e vigilanza

Come anticipato in premessa, il paradigma Web 3.0 – diversamente dal Web 2.0 – è fondato sulla decentralizzazione dei processi, sulla tecnologia *blockchain* e sull'operatività degli *smart contracts* che consentono l'esecuzione automatizzata di transazioni[156]. Sotto altro profilo, il Web 3.0 condivide invece con l'ecosistema Web 2.0 l'integrazione di sistemi di intelligenza artificiale capaci di incrementare le rispettive potenzialità.

Nell'ambito di tale architettura, gli operatori danno luogo a trasferimenti di valore (*i.e. cripto assets*)[157] in assenza di interventi di autorità centrali

[154] Sul punto, v. lo studio di D. Şenol, C. Onay, *Impact of gamification on mitigating behavioral biases of investors,* in *Journal of Behavioral and Experimental Finance,* 37, 2023.

[155] E. Yelagin, *Gamification of Stock Trading: Losers and Winners*, in *Proceedings of the EUROFIDAI-ESSEC Paris December Finance Meeting*, 2024, 3 ss.

[156] Sull'evoluzione, anche sul piano concettuale della *blockchain*, quale strumento funzionale alla circolazione non solo di un unico *asset*, ma di un numero indefinito degli stessi, v. Bassan, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain'*, cit., 562.

[157] In particolare, secondo quanto si evince, tra l'altro, nelle *Updated Joint ESAs Factsheet on crypto-assets* pubblicate dalle autorità di vigilanza europee EIOPA, EBA ed ESMA in data 6 ottobre 2025, per cripto-attività si intende "*una rappresentazione digitale di un valore o di un diritto che può essere trasferita e memorizzata elettronicamente, utilizzando un registro distribuito1 o altra tecnologia simile*." Esempi ormai noti sono BTC (Bitcoin) ed ETH (Ethereum), nonché le stablecoins, le "meme coins" e i token non fungibili (NFT), per un approfondimento

che verifichino la validità dei passaggi di titolarità[158].

Tra i rischi connessi all'investimento in cripto-attività, pare opportuno segnalare la volatilità estrema delle stesse, la carenza di trasparenza e adeguata *disclosure* nei bilanci delle società di informazioni in merito a tali strumenti[159], nonché, sotto altro profilo, la potenziale configurazione di fattispecie criminose di esercizio abusivo dell'attività finanziaria nel caso in cui le cripto-attività vengano proposte come investimento[160].

È proprio per far fronte a tali rischi che il legislatore europeo è intervenuto con il Regolamento (UE) 2023/1114 (c.d. MiCAR), che intende fornire un quadro armonizzato per i mercati delle cripto-attività e la cui finalità è quella di tutelare il consumatore garantendogli, ad esempio, l'accesso a informazioni complete e innestando nell'ordinamento europeo procedure trasparenti per la gestione dei reclami. Ne ha fatto seguito l'adozione nell'ordinamento italiano del d.lgs. 5 settembre 2024, n. 129, in ottica di recepimento delle predette previsioni europee[161].

---

delle quali, si rinvia al predetto documento.

[158] M. Lembo, *Il Regolamento UE 2023/1114 (MiCA) sul mercato delle cripto valute*, in *i Contratti*, 2025, I, 70 ss.

[159] Di rilevanza, in tal senso, il richiamo di attenzione da parte delle competenti autorità di vigilanza agli emittenti detentori di cripto-attività sul ruolo cruciale di una corretta informativa delle stesse nella documentazione finanziaria annuale, idonea a consentire una corretta analisi e valutazione in merito all'esposizione e al rischio associato a significative posizioni in cripto-attività (cfr. Banca d'Italia-Consob, *Comunicazione Banca d'Italia/Consob*, 6 marzo 2025 avente a oggetto "*Cripto-attività e informativa di bilancio - Comunicazione congiunta agli emittenti1 e alle società di revisione legale e ai revisori legali con incarichi sui bilanci degli enti di interesse pubblico (EIP) e degli enti sottoposti a regime intermedio (ESRI)*, reperibile al seguente link: <https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/20250306-bi-consob/comunicazione_consob_bi_20250306.pdf>.

[160] Sul punto la Consob è intervenuta ordinando l'oscuramento di una serie di siti web tramite cui vengono abusivamente offerti servizi per le cripto-attività (cfr. Consob, comunicato stampa del 10 ottobre 2025, reperibile al seguente link: <https://www.consob.it/documents/d/asset-library-1912910/cs_20251010>).

[161] Sul punto v. Consob-Banca d'Italia, *Nota di sintesi "Riparto di competenze tra Banca d'Italia e Consob nell'applicazione di MiCAR"*, cit.
Le disposizioni nazionali attuative del MiCAR hanno designato Banca d'Italia e Consob quali autorità nazionali competenti, attribuendo loro poteri di vigilanza e di natura autorizzativa, nonché prevedendo sanzioni di natura amministrativa e penale in caso di violazione delle disposizioni ivi contenute. In tale quadro, alla Consob vengono attribuite funzioni di vigilanza in materia di trasparenza, correttezza dei comportamenti, ordinato

In tale quadro, il Regolamento MiCAR e le correlate disposizioni nazionali attuative non sono in grado, autonomamente, di far fronte a tutte le problematiche connesse alla circolazione di tali rappresentazioni di valore, rendendo necessario un costante monitoraggio da parte delle autorità nazionali e sovranazionali e ulteriori interventi regolatori.

In primo luogo, preme segnalare la sopracitata "volatilità" dei prezzi che può determinare repentine perdite di valore, fino all'azzeramento dell'investimento. A ciò si aggiungono i rischi di liquidità, che incidono sulla possibilità di dismettere le cripto-attività al momento o al prezzo desiderato. Ulteriori criticità derivano dalla circolazione di informazioni fuorvianti e dalla promozione aggressiva, soprattutto attraverso talune piattaforme digitali, quali i *social media*[162]. Il settore è inoltre terreno fertile per frodi, truffe e attacchi informatici, anche per il tramite di tecniche sofisticate quali *phishing*, ingegneria sociale e *link* ingannevoli[163].

In tale contesto, la *blockchain* potrebbe servirsi dell'intelligenza artificiale per incrementare potenzialmente le possibilità di sventare pericolosi attacchi informatici. Difatti, secondo alcuni studi è possibile incrementare la sicurezza degli *smart contracts* attraverso sistemi di IA (ad es. *LLM*), i quali possono intercettare problematiche riguardanti il codice alla base dell'operatività degli *smart contracts*, riducendone la vulnerabilità informatica e incrementando la fiducia e sicurezza degli operatori[164].

Altro elemento che le autorità di vigilanza europee non hanno mancato di valutare è costituito dall'interconnessione tra la circolazione delle

---

svolgimento delle negoziazioni e tutela dei possessori di cripto-attività/clienti nonché di conservare l'integrità dei mercati delle cripto-attività nonché competenze in tema di prevenzione e divieto degli abusi di mercato relativi alle cripto-attività.

[162] EBA, EIOPA, ESMA, *Joint ESAs warning on crypto-assets*, 6 ottobre 2025, reperibile al seguente link: <https://www.esma.europa.eu/sites/default/files/2025-10/Updated_Joint_ESAs_revised_warning_on_crypto-assets_IT.pdf>.

[163] EBA, EIOPA AND ESMA, *Joint ESAs warning on crypto-assets*, cit.; inoltre, quale generale lacuna di tutela in tale materia, il MiCAR assicura protezioni più limitate rispetto ai prodotti finanziari tradizionali: mancano, ad esempio, regimi di compensazione, e le garanzie si riducono ulteriormente qualora i servizi siano offerti da operatori extra-UE non regolamentati. Infine, la complessità intrinseca delle cripto-attività rende spesso opaca la comprensione del loro funzionamento e dei rischi sottostanti, con conseguente vulnerabilità per l'investitore *retail*

[164] Lo studio a cui si fa riferimento è quello di N.P. KUPPA,V. K. MADISETTI, *Robust Detection and Analysis of Smart Contract Vulnerabilities with Large Language Model Agents*, in *Journal of Information Security*, 2025 197 ss.

cripto-attività e gli abusi di mercato e la conseguente necessità di offrire presidi per prevenire questi ultimi. Con gli Orientamenti adottati dall'ESMA lo scorso 9 luglio 2025 relativi alle prassi di vigilanza in materia di prevenzione e individuazione degli abusi di mercato connessi alle cripto-attività – a cui la Consob si è conformata con proprio avviso nel settembre 2025 – si è inteso estendere al predetto settore presidi già noti nei mercati finanziari regolamentati (*insider trading*, manipolazioni, abusi informativi).

Si evidenzia inoltre l'importanza di costruire una cultura comune della vigilanza sulle cripto-attività e lo sviluppo di un dialogo costante con il settore, garantendo, per un verso, coerenza nell'approccio regolatorio e nelle prassi di vigilanza, e, per altro verso, che le singole autorità nazionali possano tenere in debita considerazione le peculiarità connesse al concreto manifestarsi del *trading* di cripto-attività nella specifica giurisdizione[165].

Da ultimo, sono ben note le potenzialità connesse all'architettura Web 3.0 e alla tecnologia *blockchain* in termini di rapidità ed economicità delle transazioni – e, potenzialmente anche di sicurezza della stessa grazie all'integrazione nel Web 3.0 di sistemi sempre più avanzati di IA – ma ciò deve essere accompagnato da un quadro istituzionale dotato di strumenti di vigilanza e trasparenza. Solo in tal modo la decentralizzazione della fiducia può divenire, grazie alla cornice regolatoria europea, un meccanismo capace di garantire credibilità, stabilità e protezione dei consumatori[166].

5. Considerazioni conclusive

All'esito delle riflessioni di cui sopra, emerge che tanto il Web 2.0, dominato da piattaforme centralizzate, quanto il Web 3.0, fondato su *blockchain* e decentralizzazione dei processi, possono generare, oltre a significa-

[165] ESMA, *Guidelines On supervisory practices for competent authorities to prevent and detect market abuse under the Markets in Crypto Assets Regulation (MiCA)*, del 9 luglio 2025; sul punto v. anche Avviso Consob del 4 settembre 2025. Nell'ottica di rafforzare la trasparenza e affidabilità degli operatori e la fiducia degli investitori, lo spettro soggettivo di vigilanza di Consob e Banca d'Italia si è ampliato con le *Disposizioni di vigilanza in materia di cripto-attività* del 1° ottobre 2025. Tali misure completano l'attuazione del MiCAR e delle disposizioni nazionali attuative, introducendo requisiti su *governance* e assetti organizzativi amministrativi, contabili e di controllo, includendo anche emittenti di *stablecoin* e prestatori di servizi cripto tra i soggetti vigilati.

[166] F. Burlando, *I vantaggi dell'approccio europeo alla blockchain*, su Il Sole 24Ore, 8 ottobre 2025.

tive e virtuose innovazioni tecnologiche, anche criticità rilevanti per la tutela dei consumatori e, in generale, dei mercati. Basti pensare, come è stato ampiamente evidenziato, alla potenziale non affidabilità delle raccomandazioni fornite dai *robo advisors* (e al conseguente pregiudizio per il *best interest of the client*), all'eccessivo incremento del rischio di investimento assunto dagli utenti su piattaforme di *gamification*, alle repentine perdite di valore degli investimenti in cripto-attività, e, in generale, all'incertezza di transazioni tramite *smart contracts*.

In tale quadro, l'intelligenza artificiale, operando trasversalmente in entrambi gli ecosistemi, consente, da un lato, di incrementare le potenzialità del Web 2.0 e del Web 3.0, ma, dall'altro lato, necessita di adeguata regolazione e vigilanza da parte del legislatore e delle competenti autorità di vigilanza nazionali, tenuto conto dei potenziali effetti distorsivi derivanti da un non corretto utilizzo della stessa.

Come autorevolmente osservato[167], le piattaforme digitali, la *blockchain* e l'IA costituiscono ecosistemi a sé, ciascuno dotato di un proprio quadro normativo di riferimento ma, ogni qualvolta le piattaforme digitali si servono della *blockchain* e/o di sistemi di IA, i predetti blocchi normativi vengono a intersecarsi tra di loro ed è in tal contesto che diviene cruciale il ruolo dell'autorità, ivi inclusa la Consob, nell'assicurare la coerenza e l'armonizzazione dei predetti ecosistemi normativi, evitando fughe regolatorie da parte degli operatori e assicurando la coesistenza tra i due modelli (Web 2.0 e Web 3.0), con conseguente sviluppo dei mercati e maggior protezione per i consumatori.

[167] F. Bassan, *Digital Platforms and Blockchains: The Age of Participated Regulation*, in *European Business Law Review*, 2022, 18, reperibile su SSRN al seguente link: <https://ssrn.com/abstract=4244139>.

IVASS

Piattaforme, dati e regole: distribuzione assicurativa digitale e stratificazione regolatoria europea

Vincenzo Orsini

Il contributo analizza la trasformazione della distribuzione assicurativa nell'era digitale, esaminando l'emergere di nuove piattaforme e tecnologie data-driven che ridefiniscono ruoli e dinamiche concorrenziali. Dopo aver ricostruito le principali direttrici di cambiamento e le diverse tipologie di piattaforme operative nel mercato, l'analisi si concentra sull'intreccio tra disciplina settoriale e disciplina orizzontale. In particolare, vengono messi a confronto il quadro regolatorio derivante dalla Insurance Distribution Directive (IDD) e quello introdotto dal Digital Services Act (DSA), evidenziando ambiti di sovrapposizione e divergenza in termini di finalità e intensità degli obblighi. Successivamente, il contributo esamina le tensioni tra le regole cross-sectoral i nuovi atti legislativi europei in materia di data governance e data protection (Data Act, FIDA, GDPR, AI Act e DORA), che incidono in modo significativo sulla profilazione assicurativa. Infine, si discutono le implicazioni istituzionali e sistemiche di questa stratificazione normativa, richiamando anche le considerazioni critiche del Rapporto Draghi.

1. La digitalizzazione della distribuzione assicurativa

La distribuzione assicurativa sta attraversando un processo di trasformazione strutturale, determinato dalla progressiva digitalizzazione dei canali di offerta e dall'impiego crescente di nuove tecnologie come l'intelligenza artificiale[168]. Questi mutamenti, che si inseriscono nel più ampio processo di innovazione che interessa i mercati finanziari europei, stanno ridefinendo i rapporti tra imprese, intermediari e consumatori. A partire

[168] Si v. EIOPA, *Consumers Trends Report 2024*, 19 dicembre 2024, disponibile su *eiopa.europa.eu*.

da un modello storicamente fondato su reti di agenti e sulla bancassicurazione, la distribuzione assicurativa sta gradualmente evolvendo verso forme più articolate, in cui canali fisici e digitali coesistono e si integrano. Accanto agli intermediari tradizionali si affermano nuove piattaforme *online*, mentre le nuove tecnologie come l'intelligenza artificiale assumono un ruolo crescente lungo l'intera catena distributiva, che si sviluppa dalla profilazione degli utenti alla gestione dei sinistri, passando naturalmente per la determinazione dei premi.

La prima direttrice di cambiamento riguarda la transizione dai canali distributivi tradizionali verso piattaforme e strumenti digitali. Seppur in misura inferiore rispetto agli altri segmenti del settore finanziario (bancario e mobiliare), dove l'uso dei canali digitali per la stipula e la gestione dei rapporti contrattuali è ormai prevalente, anche nel segmento assicurativo si registra una crescente digitalizzazione dei canali distributivi. A livello europeo, le vendite online rappresentano ormai una quota significativa dei premi complessivi – mediamente il 9% nei rami vita e il 19% nei rami danni – con prospettive di ulteriore espansione nel breve periodo[169]. Anche nel contesto italiano, tradizionalmente caratterizzato da una forte centralità dei canali fisici, si osserva una tendenza consolidata all'integrazione di modalità distributive digitali[170]. Tra i canali di collocamento digitale, un ruolo centrale è svolto dai siti *web* delle imprese di assicurazione, che sovente consentono di elaborare preventivi personalizzati, e dai comparatori *online* di polizze, in particolare per la distribuzione di prodotti standardizzati (come la RC auto). Emerge insomma un modello ibrido, nel quale i canali digitali non sostituiscono ma completano e ampliano le modalità tradizionali di distribuzione.

Un'ulteriore linea di sviluppo riguarda la progressiva penetrazione delle *BigTech* all'interno delle catene distributive assicurative[171]. Queste imprese, grazie al controllo di grandi piattaforme digitali e all'accesso privilegiato a ingenti flussi di utenti e dati, si collocano in una posizione strategica per il procacciamento di nuovi affari. Tramite piattaforme non assicurative – in particolare quelle attive nei settori dei viaggi e dell'e-commerce, come Booking o Amazon – offrono polizze accessorie direttamente integrate nei propri processi di vendita, proponendole al cliente contestualmente all'acquisto del bene o del servizio principale. Si tratta di forme di

[169] Cfr. EIOPA, *Report on the Digitalisation of the European Insurance Sector*, 30 aprile 2024, p. 11 ss., disponibile su *eiopa.europa.eu*.

[170] *Ibid.*

[171] Sul punto si v. P. Marano, *Regulating Digital Insurance Platforms in the EU: Legal Frameworks and Future Directions*, in *Riv. dir. banc.*, IV, 2024, p. 1017 ss.

distribuzione riconducibili ai modelli di *embedded insurance*, che affiancano i canali tradizionali e ampliano i punti di contatto con i consumatori, rendendo più permeabile il confine tra attività assicurativa e altri settori economici. Ne deriva una ridefinizione delle dinamiche concorrenziali e dei ruoli intermediativi, con potenziali effetti significativi sulla struttura del mercato e sull'effettività della disciplina di settore.

La terza direttrice è rappresentata dalla diffusione pervasiva delle tecnologie di intelligenza artificiale, che investe l'intero ciclo distributivo[172]. Le imprese di assicurazione utilizzano già da tempo sistemi di *machine learning* per profilare e segmentare la clientela, analizzando grandi moli di dati al fine di personalizzare l'offerta e ottimizzare i processi di acquisizione di nuovi clienti. L'IA è impiegata inoltre nella definizione dinamica dei prezzi, consentendo tariffe più granulari e flessibili, anche grazie alla diffusione di dispositivi *wearable* e di dispositivi dell'*Internet-of-Things* (IoT), che raccolgono dati sulla salute e sugli stili di vita degli utenti. Infine, i *large language models* sono sempre più utilizzati nelle relazioni con la clientela (chatbot, *robo-advisory*, assistenti virtuali) e nella gestione dei sinistri, attraverso strumenti automatizzati per l'analisi documentale, la video-perizia e la rilevazione antifrode. Tali strumenti attribuiscono un vantaggio competitivo agli operatori tecnologicamente più avanzati (in grado di raccogliere, elaborare e utilizzare in modo efficiente i dati), contribuendo a ridefinire gli equilibri tra imprese assicurative e tecnologiche.

2. Le diverse tipologie di piattaforme

La digitalizzazione non elimina l'attività di intermediazione, ma ne **trasforma radicalmente le modalità**, ridefinendo ruoli, processi e punti di contatto lungo l'intera catena distributiva. Le attività di incontro tra domanda e offerta si spostano progressivamente verso **piattaforme digitali** che, fungendo al tempo stesso da infrastrutture tecnologiche e da spazi di interazione economica, diventano nodi centrali nei rapporti tra imprese di assicurazione, intermediari e consumatori. Questa evoluzione si colloca all'interno di un più ampio mutamento strutturale che riguarda l'intero sistema finanziario e che ha portato la dottrina a elaborare una distinzione tra diverse tipologie di *digital finance platforms* (DFP), in base alle funzioni

[172] In arg. si v. D. CAPONE, *La governance dell'Artificial Intelligence nel settore assicurativo tra principi etici, responsabilità del board e cultura aziendale*, in *Quaderni* IVASS, febbraio 2021, pp. 5-13, disponibile su *ivass.it*.

svolte, ai soggetti coinvolti e al grado di interazione con l'utenza finale[173].

Una prima categoria è costituita dalle **piattaforme destinate ai distributori**, che operano nel *back-end* fornendo infrastrutture tecnologiche e servizi operativi a imprese e intermediari, senza interfacciarsi direttamente con i consumatori. Rientrano in questa tipologia gli strumenti utilizzati per attività di *back-office*, comparazione interna dei prezzi, gestione dei rapporti tra intermediari e compagnie o interconnessione di sistemi. Tali piattaforme, pur non incidendo direttamente sul rapporto impresa–consumatore, svolgono un ruolo rilevante nella raccolta, gestione e circolazione dei dati, contribuendo così a modellare l'offerta assicurativa nel suo complesso. Le informazioni acquisite e trattate a livello infrastrutturale incidono infatti sulle strategie di *pricing*, sulla segmentazione della clientela e sulla strutturazione dei prodotti, influenzando indirettamente le condizioni finali proposte ai consumatori.

Una seconda categoria comprende le piattaforme *front-end*, che dispongono di un'interfaccia diretta con il pubblico. In questa categoria rientrano i siti e le piattaforme proprietarie delle compagnie assicurative, attraverso i quali i consumatori possono ottenere preventivi personalizzati, consultare la documentazione informativa e sottoscrivere *online* i contratti, nonché i siti di comparazione, che consentono di confrontare in tempo reale prezzi, condizioni contrattuali e livelli di copertura e, in molti casi, di completare interamente la transazione in via telematica.

Una terza categoria è costituita dalle piattaforme non assicurative, operanti in altri settori economici (come Amazon o Booking) che offrono coperture assicurative accessorie direttamente integrate nei propri processi di vendita, secondo logiche di *embedded insurance*. In questi casi, la piattaforma non svolge un'attività assicurativa in senso proprio, ma si appoggia a compagnie *partner*, sfruttando il proprio bacino di utenza e la capacità di profilazione per proporre prodotti assicurativi complementari al bene o al servizio principale.

Una simile strutturazione del mercato canalizza una quota crescente dei flussi informativi e transattivi attraverso un numero limitato di punti di accesso digitali. Questa concentrazione attiva economie di scala, legate alla possibilità di servire un numero crescente di utenti a costi marginali decrescenti, ed economie di rete, per cui l'utilità della piattaforma aumenta con l'ampliarsi della base di imprese e consumatori, rafforzandone

[173] Cfr. D.A. Zetsche, W.A. Birdthistle, D.W. Arner, R.P. Buckley, *Digital Finance Platforms: Toward a New Regulatory Paradigm*, in *U. of Pennsylvania Journal of Business Law*, I, 2020, p. 273 ss.

progressivamente l'attrattività. L'interazione di questi fattori può però determinare, nel medio periodo, fenomeni di forte concentrazione del mercato, con l'emersione di pochi operatori in grado di controllare i principali canali distributivi e incidere sulle condizioni di accesso ai prodotti assicurativi. A questi fenomeni si sommano gli effetti di *lock-in* tecnologico, che vincolano utenti e operatori all'interno dell'ecosistema della piattaforma e riducono ulteriormente la contendibilità del mercato, amplificando il rischio di posizioni dominanti difficilmente scalzabili.

3. Idd e Dsa nel governo delle piattaforme assicurative

Com'è noto, la direttiva 20 gennaio 2016, n. 97/UE (*Insurance Distribution Directive* – IDD) è stata recepita nell'ordinamento italiano con il **d.lgs. 21 maggio 2018, n. 68**, che ha modificato in modo significativo il titolo IX del Codice delle assicurazioni private (c. ass.). L'intervento ha segnato il passaggio dal sistema incentrato sull'intermediazione assicurativa a quello più ampio della **"distribuzione assicurativa"**, estendendo la disciplina a tutti i soggetti che intervengono professionalmente nel processo di collocamento di prodotti assicurativi, **inclusi quelli operanti attraverso canali digitali.** In questo modo, il recepimento della IDD ha fornito la base normativa per attrarre nel perimetro regolato le nuove forme di distribuzione digitale, assicurando l'applicazione uniforme delle regole sostanziali e comportamentali a tutti gli operatori che, anche tramite piattaforme, partecipano professionalmente alla distribuzione di prodotti assicurativi[174].

L'art. 106 c. ass., infatti, riproduce la definizione ampia contenuta nella IDD, includendo espressamente nella distribuzione anche «la fornitura di informazioni relativamente ad uno o più contratti di assicurazione sulla base di criteri scelti dal cliente tramite un sito internet o altri mezzi e la predisposizione di una classifica di prodotti assicurativi, compreso il confronto tra prezzi e tra prodotti o lo sconto sul premio di un contratto di assicurazione, se il cliente è in grado di stipulare direttamente o indirettamente un contratto di assicurazione tramite un sito internet o altri mezzi». Ne consegue che i gestori di piattaforme online che svolgono tali attività devono rientrare tra i **soggetti abilitati** ai sensi dell'art. 107-*bis* c. ass., vale a dire imprese e intermediari iscritti nelle relative sezioni del **Registro unico**

[174] Sul punto si v. S. Balsamo Tognani, *Il fenomeno dei "siti comparativi" alla luce della recente* Insurance Distribution Directive: a new consumer trend?, in *Assicurazioni*, I, 2017, p. 71 ss.

degli intermediari (RUI). Nella prassi, questi operatori agiscono prevalentemente come ***broker*** **assicurativi**, risultando iscritti alla sezione B del RUI: stipulano convenzioni con più imprese e mettono a disposizione degli utenti strumenti di preventivazione e confronto, che consentono anche la **conclusione diretta del contratto *online*.**

Tra gli aspetti più significativi del recepimento italiano della direttiva si colloca l'introduzione di un *corpus* organico di regole di comportamento, volte ad assicurare che l'attività distributiva, indipendentemente dal canale utilizzato, assicuri il medesimo livello di tutela per gli assicurati[175]. A tal fine, l'art. 119-*bis* c. ass. enuncia il principio generale secondo cui i distributori devono operare «con equità, onestà, professionalità, correttezza e trasparenza nel miglior interesse dei contraenti», fornendo informazioni «corrette, chiare e non fuorvianti, imparziali e complete». Alla c.d. *best interest rule* si collega la disciplina delle pratiche di remunerazione e degli incentivi. Il legislatore vieta, infatti, politiche commerciali e sistemi di incentivazione che possano indurre i distributori a raccomandare o collocare prodotti non coerenti con le esigenze del cliente al solo fine di massimizzare la provvigione o altri benefici (cc.dd. *inducements*).

Parallelamente, gli artt. 120-*bis* e 120-*ter* prevedono obblighi stringenti di trasparenza sulle remunerazioni e di presidio dei conflitti di interesse, imponendo di rendere note al cliente la natura e la fonte dei compensi percepiti e di comunicare i conflitti non eliminabili mediante misure organizzative. Il legislatore, d'altronde, non trascura di disciplinare con attenzione anche la trasparenza informativa, imponendo al distributore di fornire al cliente tutte le informazioni necessarie per compiere scelte consapevoli. L'art. 120-*quater* regola le modalità dell'informazione, imponendo che essa sia resa in forma chiara, corretta e comprensibile, su supporto durevole o tramite mezzi elettronici idonei, mentre gli artt. 120-*quinquies* e 121 introducono specifici presidi per le vendite abbinate e a distanza.

Il sistema, inoltre, attribuisce un ruolo primario all'indagine sulle esigenze del cliente, anche qualora il distributore non offra una consulenza personalizzata: il distributore deve acquisire dal contraente ogni informazione utile a identificare le sue richieste ed esigenze, al fine di valutare l'adeguatezza del contratto offerto (art. 119-*ter*). La prospettiva è completata dalle norme in materia di *product oversight and governance* (POG), che delineano un quadro di responsabilità condivise tra produttori e distributori in tutte le fasi del ciclo di vita del prodotto. Tali disposizioni impongono l'indivi-

[175] Cfr. P. Corrias, *La direttiva UE 2016/97 sulla distribuzione assicurativa: profili di tutela dell'assicurando*, ivi, p. 11 s.

duazione di un mercato di riferimento positivo e negativo (*target market*) per ciascun prodotto, la definizione di strategie distributive coerenti con le caratteristiche e le esigenze della clientela individuata, e un monitoraggio costante della performance e dell'adeguatezza dei prodotti offerti (artt. 30-*decies*, 121-*bis* e 121-*ter* c. ass., reg. IVASS 4 agosto 2020, n. 45).

Dal quadro normativo descritto emerge un sistema articolato e coerente, che supera la tradizionale logica della mera trasparenza informativa per attribuire ai distributori un ruolo proattivo nella tutela dell'assicurato. Le regole non si limitano, infatti, a prescrivere obblighi di *disclosure*, ma impongono ai distributori di intervenire attivamente nella selezione, presentazione e distribuzione dei prodotti, assicurandone la coerenza con le caratteristiche e le esigenze della clientela.

L'assetto delineato dalla IDD e dalla disciplina di recepimento di rango primario e secondario si intreccia oggi con la disciplina *cross-sectoral* contenuta nel reg. 19 ottobre 2022, n. 2065 (*Digital Services Act* – DSA), entrato pienamente in vigore il 17 febbraio 2024. Sebbene il DSA non sia specificamente rivolto al settore assicurativo o finanziario, esso si applica a una vasta gamma di servizi della società dell'informazione, incluse molte piattaforme che operano nel settore assicurativo (tra cui certamente i siti di comparazione polizze)[176].

Il perno concettuale della disciplina delineata dal DSA è rappresentato dalla nozione di "servizi intermediari", nella quale rientrano, ai sensi dell'art. 3, lett. g, tre tipologie di servizi della società dell'informazione: le attività di mero trasporto (*mere conduit*), la memorizzazione temporanea (*caching*) e la memorizzazione di informazioni (*hosting*). All'interno della categoria dei servizi di *hosting*, il DSA individua una sottocategoria specifica, quella delle "piattaforme online", definita dall'art. 3, lett. i, come «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico». Si tratta, dunque, di servizi di *hosting* che non si limitano a conservare dati, ma che svolgono un ruolo attivo nella diffusione al pubblico delle informazioni fornite dagli utenti, consentendo di raggiungere una platea potenzialmente illimitata di destinatari.

All'interno di questo quadro, le piattaforme operanti in ambito assicurativo possono essere collocate con relativa precisione. Tali operatori, nella misura in cui ospitano e diffondono al pubblico informazioni relative a prodotti assicurativi forniti da terzi, rientrano nella definizione di piatta-

[176] Sul punto si v. MARANO, *Regulating Digital Insurance Platforms in the EU: Legal Frameworks and Future Directions*, cit., p. 1030 s.

forme online ai sensi dell'art. 3, lett. i, e sono pertanto soggetti sia agli obblighi generali applicabili ai servizi intermediari sia a quelli specifici per le piattaforme *online*. Ciò comporta che i gestori di piattaforme assicurative sono di fatto soggetti a un duplice regime regolatorio: da un lato, quello settoriale che disciplina in modo specifico la distribuzione assicurativa; dall'altro, quello orizzontale del DSA, che regola gli obblighi generali di funzionamento dei servizi intermediari e delle piattaforme *online*.

Dall'analisi delle disposizioni contenute nel regolamento emerge una parziale sovrapposizione tra gli obblighi del DSA e quelli imposti dalla normativa settoriale assicurativa. Alcune disposizioni del DSA, infatti, presentano evidenti analogie con le regole di comportamento dei distributori previste dal Codice delle assicurazioni.

Un primo gruppo di disposizioni applicabili è costituito da quelle che il DSA prevede, in via generale, per tutti i prestatori di servizi intermediari. Tra queste, assumono rilievo per le piattaforme assicurative gli obblighi di trasparenza sanciti dall'art. 14, relativi ai recapiti e alle condizioni d'uso del servizio. Tali obblighi sono funzionali a garantire la chiara identificabilità del prestatore e la piena intelligibilità delle regole che disciplinano l'utilizzo della piattaforma da parte degli utenti, rafforzando così la fiducia e la tracciabilità degli operatori coinvolti. A questi si affianca l'obbligo di cooperazione con le autorità competenti (art. 19), che consente un controllo pubblico effettivo sull'operato delle piattaforme digitali.

Ai gestori di piattaforme online, inoltre, il DSA impone un gruppo di obblighi specifici, contenuti nel Capo III, Sezione 4 (artt. 24-30), che si affiancano a quelli previsti per i prestatori di servizi intermediari in generale. In particolare, l'art. 24 introduce obblighi di trasparenza relativi ai sistemi di raccomandazione e di presentazione dei contenuti: i gestori devono rendere pubblici i parametri principali utilizzati per la classificazione o la presentazione delle offerte e fornire agli utenti una spiegazione chiara delle modalità con cui tali parametri incidono sull'ordine e sulla visibilità delle informazioni. La norma non impone la divulgazione integrale degli algoritmi, ma richiede la comunicazione di elementi sufficienti a consentire agli utenti di comprendere i criteri fondamentali che orientano la presentazione dei contenuti e, di conseguenza, le dinamiche di scelta.

A tali obblighi si affiancano quelli previsti dagli artt. 25, 26 e 27, che delineano un ulteriore quadro di garanzie volto ad assicurare trasparenza commerciale e corretto funzionamento delle piattaforme. L'art. 25 impone ai gestori di informare chiaramente gli utenti qualora la visualizzazione di specifici contenuti o offerte sia influenzata da pubblicità o accordi a fini commerciali, distinguendo tali contenuti da quelli organici. L'art. 26

disciplina i requisiti di trasparenza della pubblicità online, prevedendo che le inserzioni siano chiaramente identificabili e che vengano fornite informazioni sui principali parametri utilizzati per determinarne il destinatario. L'art. 27, infine, introduce divieti e limiti specifici in materia di pubblicità mirata, in particolare nei confronti dei minori e in relazione all'utilizzo di categorie particolari di dati personali, rafforzando così la tutela degli utenti contro pratiche manipolative o opache. L'art. 30 completa il quadro disciplinando gli obblighi di tracciabilità degli operatori commerciali, imponendo ai gestori di piattaforme *online* di raccogliere e verificare informazioni essenziali sull'identità dei soggetti che utilizzano la piattaforma per offrire beni o servizi.

Il DSA prevede inoltre una disciplina specifica in materia di reclami. L'art. 20 impone ai prestatori di piattaforme online di istituire meccanismi interni di gestione dei reclami che siano facilmente accessibili, gratuiti e strutturati, consentendo agli utenti di contestare decisioni o comportamenti della piattaforma in modo tracciabile e trasparente. Tale procedura deve essere accompagnata dalla possibilità di ricorrere a sistemi di risoluzione extragiudiziale delle controversie riconosciuti, al fine di assicurare un rimedio effettivo e proporzionato. Una previsione analoga è contenuta nel diritto assicurativo nazionale. Gli intermediari e le imprese sono infatti tenuti, ai sensi dell'art. 10-*bis* del reg. ISVAP 19 maggio 2008, n, 24 e dell'art. 79 del reg. IVASS 2 agosto 2018, n. 40, ad adottare procedure efficaci e trasparenti di gestione dei reclami, che garantiscano tempi certi di risposta, la tracciabilità delle comunicazioni e la possibilità per il contraente di rivolgersi all'Autorità in caso di insoddisfazione.

Il raffronto tra i due regimi evidenzia, da un lato, punti di contatto strutturali, dall'altro, una diversa intensità e finalità degli obblighi imposti. Le disposizioni del DSA e quelle del Codice delle assicurazioni presentano infatti alcune aree di sovrapposizione, in particolare nei profili legati alla trasparenza e alla responsabilizzazione degli operatori, che si riflettono sia nelle modalità di presentazione delle offerte sia nella gestione dei rapporti con gli utenti.

Questa sovrapposizione resta tuttavia circoscritta ad aspetti prevalentemente informativi e procedurali. Gli obblighi previsti dal DSA hanno natura orizzontale e standardizzata: si applicano a tutte le piattaforme digitali, indipendentemente dal settore di attività, e mirano a garantire la trasparenza e il corretto funzionamento dell'ambiente digitale. Non incidono invece sulla sostanza dei rapporti contrattuali, né impongono un intervento attivo nella valutazione dell'adeguatezza delle offerte rispetto alle esigenze individuali degli utenti. La disciplina derivante dalla IDD opera invece su

un piano settoriale e presenta un grado di penetrazione ben più ampio. Essa non si limita a prescrivere obblighi formali, ma richiede ai distributori di assumere un ruolo proattivo nella tutela dell'assicurato, imponendo valutazioni individualizzate e l'adozione di procedure interne volte ad assicurare la coerenza tra il prodotto offerto e il profilo del cliente. Ne sono espressione la regola del miglior interesse, l'indagine sulle richieste ed esigenze, la verifica di adeguatezza e appropriatezza per i prodotti di investimento assicurativo e la disciplina di *product oversight and governance*, che incide anche sulla fase di ideazione e selezione dei prodotti.

La diversa intensità degli obblighi riflette la diversità degli interessi tutelati. La IDD è orientata alla protezione dell'assicurato come parte debole, intervenendo sul contenuto sostanziale della distribuzione e sulla condotta del distributore. Il DSA, al contrario, ha una finalità sistemica: regola il contesto digitale nel quale le piattaforme operano, ponendo obblighi di trasparenza e tracciabilità volti a garantire il buon funzionamento del mercato, senza incidere direttamente sul rapporto contrattuale.

4. Il rapporto tra disciplina di settore e regole *cross-sectoral* in materia di *data governance* e *data protection*

La rapida affermazione di modelli distributivi e produttivi *data-driven* nel settore assicurativo rende particolarmente evidente la progressiva sovrapposizione tra discipline di natura orizzontale e discipline settoriali[177]. Il recente quadro regolatorio europeo si caratterizza, infatti, per l'intreccio di atti normativi diversi per finalità, *ratio* e tecniche di regolazione, che incidono sul trattamento, sulla condivisione e sull'utilizzo dei dati a fini economici: il reg. 13 dicembre 2023, n. 2854 (*Data Act*), la proposta di regolamento sul *Financial Data Access* (FIDA), il reg. 27 aprile 2016, n. 679 (*General Data Protection Regulation* o GDPR), il reg. 13 giugno 2024, n. 1689 (*AI Act*) e il reg. 14 dicembre 2022, n. 2554 (*Digital Operational Resilience Act* o DORA), incidono tutti – con un differente livello di intensità – sull'attività assicurativa per come viene esercitata oggi.

Una simile ipertrofia normativa produce una stratificazione di obblighi che, pur muovendo da finalità diverse, possono risultare tra loro difficilmente conciliabili nella prassi applicativa. Tale fenomeno emerge con particolare nettezza nell'ambito della profilazione assicurativa, dove con-

[177] Parla in termini di opportunità, P. Franchini, *Innovazione e competitività: l'ecosistema assicurativo e fintech per il sistema paese*, 18 settembre 2025, disponibile su *ivass.it*.

vergono obblighi di apertura e condivisione dei dati ispirati a finalità pro-concorrenziali, prescrizioni in materia di protezione dei dati personali, vincoli di trasparenza e spiegabilità degli algoritmi, nonché requisiti di sicurezza e resilienza delle infrastrutture digitali. Si tratta di piani regolatori distinti ma strettamente intrecciati, che incidono simultaneamente sulle modalità di raccolta, trattamento e utilizzo dei dati a fini di *pricing* e personalizzazione dell'offerta, dando luogo a zone di frizione, incertezze interpretative e potenziali conflitti applicativi.

Il *Data Act* si inserisce nel quadro della strategia europea per i dati, con l'obiettivo di favorire la circolazione e la condivisione dei dati tra soggetti pubblici e privati, stimolare l'innovazione e correggere le asimmetrie informative nei mercati digitali. Esso si applica ai dati generati dall'uso di prodotti e servizi connessi e introduce obblighi di accesso e condivisione in capo ai detentori dei dati, sia nei confronti degli utenti sia di terzi designati dagli utenti stessi. In particolare, gli artt. 3-5 riconoscono all'utilizzatore il diritto di accedere ai dati generati dall'utilizzo dei prodotti e di condividerli con soggetti terzi; l'art. 8 prevede che tale accesso avvenga a condizioni eque, ragionevoli e non discriminatorie. Queste disposizioni, sebbene formulate in termini generali, si applicano anche al settore assicurativo, nel quale la diffusione di dispositivi IoT e *wearable* genera una mole crescente di dati rilevanti ai fini della valutazione del rischio e della determinazione del premio. Attraverso il *Data Act*, soggetti terzi – inclusi potenziali nuovi intermediari o piattaforme digitali – possono accedere a tali dati per sviluppare servizi innovativi e personalizzati, ridefinendo gli equilibri concorrenziali del mercato.

Su questa traiettoria si colloca la proposta di regolamento FIDA, che mira a estendere la logica dell'*open banking* all'intero settore finanziario, realizzando la c.d. *open finance*. Essa prevede l'introduzione di obblighi armonizzati di condivisione dei dati tra detentori e soggetti terzi autorizzati, previo consenso dell'utente, per stimolare lo sviluppo di nuovi servizi basati sull'analisi di dati finanziari e assicurativi. In ambito assicurativo, ciò implica la possibilità per operatori terzi di accedere a dati relativi a sinistrosità, storico dei premi, comportamenti assicurativi e profili di rischio, al fine di proporre coperture personalizzate, comparazioni dinamiche e servizi di consulenza basati su algoritmi predittivi. FIDA, dunque, rafforza la logica pro-concorrenziale già insita nel *Data Act*, favorendo l'ingresso di nuovi attori nell'ecosistema assicurativo e la creazione di modelli di offerta fondati sull'analisi di dati eterogenei e granulari.

L'approccio del *Data Act* e di FIDA – orientato alla massimizzazione dell'uso economico dei dati – si colloca però in potenziale tensione

con i principi e i vincoli del GDPR, che costituisce il pilastro della disciplina europea in materia di protezione dei dati personali. Il GDPR si fonda su logiche profondamente diverse: il trattamento dei dati deve rispettare i principi di liceità, correttezza e trasparenza (art. 5, par. 1, lett. a), essere limitato alle finalità per le quali i dati sono raccolti (art. 5, par. 1, lett. b), e deve avvenire nella misura adeguata, pertinente e limitata a quanto necessario rispetto alle finalità perseguite (principio di minimizzazione, art. 5, par. 1, lett. c). Inoltre, l'art. 22 riconosce all'interessato il diritto a non essere sottoposto a decisioni unicamente automatizzate che producano effetti giuridici o incidano significativamente sulla sua persona, salvo specifiche garanzie. Questi principi si applicano pienamente alle attività di profilazione assicurativa, che costituiscono una forma di trattamento automatizzato spesso basata su dati comportamentali, sanitari o relativi alla circolazione raccolti mediante dispositivi connessi.

L'utilizzo di dati ottenuti attraverso i meccanismi di accesso e condivisione previsti dal *Data Act* o da FIDA può entrare in conflitto con i vincoli di finalità e minimizzazione del GDPR, generando incertezze sulla base giuridica del trattamento da parte dei soggetti terzi che ricevono i dati. Inoltre, la combinazione di fonti informative eterogenee – come dati telematici, storici assicurativi e dati finanziari – accentua i rischi di profilazione invasiva e di trattamenti non proporzionati rispetto alle finalità originarie della raccolta.

A questo quadro si aggiunge la disciplina dell'*AI Act*, che interviene in modo trasversale per regolare l'uso dei sistemi di intelligenza artificiale. Il regolamento classifica come "ad alto rischio" (art. 6 e Allegato III) «i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie». Per tali sistemi sono previsti obblighi stringenti di gestione del rischio (art. 9), qualità dei dati di addestramento, trasparenza e tracciabilità (art. 10), sorveglianza umana (art. 14) e valutazione d'impatto (art. 27). Gli operatori assicurativi che utilizzano modelli di *pricing* algoritmico o strumenti di profilazione automatizzata sono dunque tenuti ad adeguare i propri sistemi alle prescrizioni del regolamento, garantendo la spiegabilità dei risultati e la possibilità di verifica *ex post* dei meccanismi decisionali. L'AI Act non si limita, quindi, a prescrivere obblighi informativi, ma incide direttamente sulla progettazione, addestramento e impiego dei modelli di IA, con conseguenze profonde sui processi assicurativi.

Infine, il DORA introduce un ulteriore complesso di obblighi, volto a garantire la sicurezza operativa e la resilienza digitale degli operatori finanziari, comprese imprese assicurative e intermediari. Esso prevede ob-

blighi di *governance* e gestione del rischio ICT (artt. 5-13), notificazione degli incidenti (artt. 17-20), test di resilienza operativa digitale (artt. 21-24) e regole per la gestione dei fornitori terzi critici (artt. 28-30). Anche se non riguarda direttamente la profilazione, DORA incide sull'ambiente tecnico-organizzativo in cui le attività algoritmiche si svolgono. I sistemi di IA e le infrastrutture che li supportano devono rispettare elevati *standard* di sicurezza, resilienza e tracciabilità, e le imprese sono tenute a predisporre adeguati piani di continuità e sistemi di monitoraggio. Questo aspetto assume particolare rilevanza per le compagnie che esternalizzano lo sviluppo e la gestione dei modelli di *pricing* a fornitori tecnologici non vigilati, i quali entrano così stabilmente nella catena del valore assicurativa.

Gli effetti concreti di questa stratificazione emergono nell'attività di profilazione assicurativa, fulcro dei modelli *data-driven*[178]. L'analisi di dati personali e comportamentali consente alle imprese di elaborare profili di rischio sempre più dettagliati e di personalizzare i prodotti. Ciò può generare benefici notevoli: una profilazione più granulare consente valutazioni attuariali più precise, riduce le asimmetrie informative e può favorire la creazione di prodotti personalizzati e dinamici. Ad esempio, i dati telematici sulla guida consentono di costruire classi di rischio più aderenti alla realtà; analogamente, nel ramo salute, i dati raccolti da dispositivi indossabili permettono programmi di prevenzione e premi dinamici.

Queste stesse tecniche, tuttavia, accentuano i rischi di discriminazione, opacità decisionale e uso improprio dei dati. Un esempio paradigmatico è il *price walking*, ossia l'applicazione di premi crescenti ai clienti fidelizzati nel tempo senza variazioni del rischio assicurato, basata su modelli predittivi del comportamento di rinnovo. Tali pratiche si collocano in un'area giuridica complessa: implicano trattamenti intensivi e spesso opachi, potenzialmente in contrasto con i principi del GDPR (artt. 5, 12-14, 22), sollevano dubbi sulla base giuridica per dati provenienti da terzi e richiedono, ai sensi dell'AI Act, spiegabilità e documentazione difficili da garantire per modelli di discriminazione di prezzo. Inoltre, DORA impone presidi di sicurezza e resilienza per le infrastrutture ICT che supportano tali processi, incidendo sulle modalità operative con cui la profilazione può essere svolta.

La complessità del quadro normativo europeo in materia di dati, intelligenza artificiale e resilienza digitale si riflette inevitabilmente anche sul piano istituzionale, poiché ciascuna disciplina attribuisce competenze

[178] Su benefici e rischi dell'impiego dell'IA nel segmento assicurativo, si v. CAPONE, *La governance dell'Artificial Intelligence nel settore assicurativo tra principi etici, responsabilità del board e cultura aziendale*, cit., p. 12 s.

di vigilanza e poteri regolatori a diverse autorità, spesso con mandati e strumenti eterogenei. Questa distribuzione policentrica delle competenze determina un sistema di vigilanza multilivello, nel quale coesistono autorità settoriali, autorità orizzontali e organismi di coordinamento europei. In assenza di chiari meccanismi di raccordo e di linee interpretative condivise, il rischio è quello di generare frammentazione applicativa, sovrapposizione di controlli e incertezza per gli operatori. Sarà pertanto necessario sviluppare forme stabili di cooperazione tra autorità – sia a livello nazionale sia europeo – per delineare quadri applicativi coerenti, capaci di conciliare le diverse finalità perseguite dalle discipline coinvolte e di fornire indicazioni uniformi ai soggetti vigilati.

Il recente Rapporto Draghi ha messo chiaramente in luce come l'ipertrofia normativa europea costituisca uno dei principali ostacoli alla capacità di innovazione e di investimento delle imprese[179]. La proliferazione di discipline parallele e l'assenza di coordinamento effettivo tra autorità producono costi di conformità elevati, incertezza giuridica e difficoltà nell'implementazione di nuovi modelli tecnologici. Il quadro regolatorio, pur animato dall'obiettivo di bilanciare la salvaguardia degli interessi individuali (protezione dei dati, trasparenza, sicurezza) con la promozione dell'innovazione tecnologica, rischia così di tradursi in un freno strutturale allo sviluppo competitivo del mercato unico digitale. Tale constatazione assume particolare rilievo nel settore assicurativo, dove la capacità di sfruttare in modo efficiente i dati è un elemento essenziale per la sostenibilità tecnica e l'innovazione di prodotto: un eccesso di stratificazione normativa, se non accompagnato da strategie di coordinamento e semplificazione, rischia di rendere più difficoltosa l'adozione di strumenti tecnologici avanzati e di scoraggiare nuovi.

[179] Cfr. M. Draghi, *The future of European competitiveness. Part A. A competitiveness strategy for Europe*, settembre 2024, p. 30, disponibile su *commission.europa.eu*.

ACN

Sicurezza digitale e governance nazionale: il ruolo dell'ACN tra *cyber threats*, disinformazione e intelligenza artificiale

Michela Mastrantonio

Il contributo analizza il ruolo dell'Agenzia per la Cybersicurezza Nazionale nella costruzione di un ecosistema di sicurezza digitale integrato, capace di affrontare minacce informatiche complesse, fenomeni di disinformazione e sfide poste dall'intelligenza artificiale. Viene approfondito l'approccio multilivello e partecipativo adottato dall'Agenzia, fondato sull'integrazione tra infrastrutture resilienti, cooperazione istituzionale e consapevolezza collettiva. L'analisi evidenzia la centralità della governance coordinata per garantire sicurezza, fiducia e sovranità digitale.

1. Premessa

Negli ultimi anni il panorama delle piattaforme digitali ha conosciuto una trasformazione profonda e radicale, sostenuta da un incremento esponenziale nella gestione dei dati, della fruizione di servizi digitali e dell'informatizzazione dei processi nelle Pubbliche Amministrazioni, nelle imprese e nelle abitazioni private. Questa evoluzione è stata largamente facilitata dalla convergenza di tecnologie innovative quali la dematerializzazione documentale, il *cloud computing*, l'*Internet of Things* (IoT). In altre parole, l'adozione di soluzioni digitali pervasive ha rimodellato in modo sostanziale il concetto stesso di sicurezza, con l'effetto di esporre il sistema-Paese a nuove e complesse minacce informatiche, non più efficacemente contenute da misure di protezione tradizionali basate su barriere perimetrali[180].

[180] Si sta consolidando sempre più diffusamente l'idea di *safety* come ambito che intende tutelare l'intera collettività dai rischi e dalle minacce capaci di compromettere o indebolire

La sicurezza digitale assume oggi una dimensione multidisciplinare e multifattoriale, ulteriore rispetto alla mera gestione informatica di criticità di natura tecnica. Diviene un vero e proprio pilastro imprescindibile per lo sviluppo economico, sociale e democratico del Paese. Da qui – a partire dal riconoscimento della natura strumentale e vitale per cittadini e imprese – reti informatiche, infrastrutture digitali e dati personali si manifestano al contempo come potenziali vettori di vulnerabilità e di rischio sistemico.

La frammentazione della *governance* della cybersicurezza, associata alla marcata dipendenza da tecnologie e *software* di provenienza estera, aggrava questo scenario – evidentemente già compromesso – generando fragilità significative. Ancora, il *digital divide* territoriale accentua disuguaglianze tra aree più o meno resilienti, con l'effetto di rendere più complicata la messa in sicurezza delle piattaforme considerate essenziali sul piano socio-economico globale.

La sofisticazione e la crescente frequenza degli attacchi informatici evidenziano l'urgenza di adottare misure proattive e integrate per la protezione di sistemi e dati sensibili. Nello specifico ambito delle piattaforme digitali, l'obiettivo di protezione si estende anche ad aspetti di natura sociale: lungi dall'essere meri strumenti neutrali, le piattaforme digitali si configurano come infrastrutture critiche che influenzano profondamente le dinamiche sociali, culturali e politiche. Si tratta piuttosto di strumenti che, interamente considerati in termini di funzionamento tecnico-operativo e delle conseguenti ricadute sulla collettività, hanno il potenziale di generare il c.d. fenomeno della "disinformazione digitale", che in alcuni contesti assume profili di *cybercrime*[181].

Le c.d. "*filter bubble*", così come la crescente diffusione degli attacchi mirati di natura *cyberpsicologica*, la manipolazione degli ecosistemi informativi e l'uso sempre più massiccio di tecniche quali *social engineering* e *phishing*, emergono come episodi chiave nei recenti studi specialistici e nelle analisi empiriche. Questi rilievi impongono la necessità di un approccio alla sicu-

il regolare funzionamento delle dinamiche democratiche. Questa accezione si distingue da quella di *security*, che assume invece un profilo ancillare, limitato al garantire l'affidabilità e la solidità dello spazio cibernetico.

[181] Le evidenze raccolte nel corso di indagini di questo tipo mettono in evidenza in modo sempre più chiaro la presenza e la diffusione pervasiva di modelli organizzativi di tipo "*as-a-service*". La criminalità informatica tende, infatti, a pianificare e a condurre operazioni illecite per conto di terzi, consentendo anche a soggetti con competenze limitate di eseguire attacchi grazie a strumenti e infrastrutture messe a disposizione da altri, con il risultato di rendere questo fenomeno ampiamente accessibile e strutturalmente consolidato.

rezza digitale che sia non solo tecnologico, ma multidimensionale, partecipativo e orientato al coinvolgimento attivo della cittadinanza.

È infatti la centralità delle infrastrutture nel contesto dello sviluppo socioeconomico a imporre una riflessione anche sui profili inerenti alla previsione, alla prevenzione e alla gestione del rischio informatico. Considerata la trasversalità della cybersicurezza, individui, imprese, istituzioni e Stati si trovano inevitabilmente a collaborare secondo un approccio per cui risulta fondamentale il coordinamento delle parti nella gestione e nel controllo del rischio che si pone in un'ottica di "bene comune" o "bene pubblico".

In questo scenario, l'Agenzia per la Cybersicurezza Nazionale (ACN) si afferma come attore strategico essenziale e propone un modello di *governance* che supera la tradizionale dicotomia tra tecnologia e diritto. La sua azione si fonda su una duplice prospettiva: da un lato, investimenti strutturali per rafforzare infrastrutture resilienti, sistemi automatici di difesa e capacità di risposta tempestiva; dall'altro, programmi di sensibilizzazione e formazione per innalzare il livello di consapevolezza collettiva sulle minacce digitali e sulle modalità di prevenzione. Questo modello integrato si riscontra nel quadro normativo e nelle politiche delineate dall'ACN che, come si dirà, intende realizzare un'azione coordinata su più livelli istituzionali e sociali, allineata ai migliori standard europei e internazionali.

2. *Governance* della cybersicurezza: quadro normativo e implicazioni strategiche

La *governance* della cybersicurezza si configura come un sistema complesso e multilivello che coinvolge una vasta gamma di attori pubblici e privati e si avvale di molteplici strumenti normativi, tecnici e organizzativi. La natura pervasiva e senza confini del cyberspazio rende inadeguata la tradizionale prospettiva statuale di sovranità su un territorio. Nel contesto cibernetico, garantire un adeguato livello di tutela richiede un approccio strategico capace di superare la sola dimensione regolatoria, orientandosi, invece, anche alla salvaguardia degli interessi pubblici essenziali mediante il coordinamento tra attori istituzionali, sul piano sia nazionale sia sovranazionale. Di conseguenza, in ambito *cyber* un idoneo livello di protezione impone un approccio non più basato solo sulla regolazione, bensì anche sulla difesa degli interessi pubblici rilevanti, attraverso un'interrelazione di soggetti all'uopo preposti. Due principi fondamentali guidano l'efficacia di questa impostazione: (i) la necessità di coinvolgere tutti i settori dell'ordinamento, privato e pubblico; (ii) l'importanza della cooperazione, della stan-

dardizzazione dei processi e della condivisione d'informazioni a più livelli.

Questo è il modello d'azione adottato dall'Unione europea, che si riverbera direttamente e in modo coordinato nei piani d'azione interni degli Stati membri. La Direttiva NIS[182] e il suo più recente aggiornamento[183] (Direttiva NIS 2)[184], ha rappresentato una svolta fondamentale in ambito *cyber*: a partire dalla constatazione della forte interdipendenza tra le reti e della necessità di un approccio coordinato sovranazionale, ha definito un quadro comune di misure relative alla sicurezza delle reti e dei sistemi informativi e ha consentito di creare un impianto normativo armonizzato per garantire un alto livello di protezione in tutto il territorio dell'Unione. Questa armonizzazione si è resa indispensabile date la natura transnazionale delle infrastrutture digitali e la forte interconnessione tra reti; diversamente, la sicurezza europea sarebbe stata insufficiente. A rafforzare questo sistema, il Cybersecurity Act[185] ha affidato all'ENISA un ruolo operativo centrale e ha instaurato un quadro di certificazione comune per prodotti e servizi digitali, con effetti concretamente apprezzabili tanto per la libera circolazione nel mercato unico, quanto per la fiducia degli operatori e degli utenti.

[182] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[183] La Direttiva NIS 2 rafforza e amplia il quadro introdotto dalla prima NIS, colmando le lacune precedenti e imponendo un sistema più rigoroso di gestione del rischio e di segnalazione degli incidenti. Estende il proprio ambito di applicazione a nuovi settori strategici e introduce la distinzione tra "soggetti essenziali" e "soggetti importanti", richiedendo livelli elevati di sicurezza lungo tutta la catena di fornitura. Sul piano strategico, consolida il modello europeo di cybersicurezza basato su cooperazione istituzionale, armonizzazione degli *standard* e cultura del rischio; rafforza l'approccio integrato e resiliente che sostiene la protezione dei diritti fondamentali e la stabilità del mercato digitale europeo. In questo modo, la Direttiva promuove una responsabilizzazione diffusa delle organizzazioni e impone obblighi di sicurezza proporzionati, ma stringenti anche sotto il profilo della catena di fornitura e della resilienza operativa.

[184] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[185] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013.

In coerenza con la strategia europea sopra descritta, il D.L. 82/2021[186] ha istituito l'Agenzia per la Cybersicurezza Nazionale. Questo intervento normativo ha segnato un passaggio epocale nella definizione di una tutela organica dello spazio cibernetico del Paese: ha definito un modello di *governance* che attribuisce al Presidente del Consiglio un ruolo di indirizzo politico e strategico e colloca l'ACN come soggetto di raccordo tra istituzioni pubbliche, imprese strategiche, centri di *intelligence* e operatori privati. L'ACN, infatti, assume un ruolo che si distingue per la sua duplice natura di autorità strategica da una parte[187] e di centro di coordinamento tecnico-operativo dall'altra[188]. Questo modello di *governance*, com'è evidente, si basa su un approccio ibrido che integra capacità normative e operative, spingendo verso un dialogo costante tra pubblico e privato e tra ambienti politici e tecnici.

L'istituzione dell'Agenzia rappresenta il punto di arrivo di un percorso di sistematizzazione delle esperienze maturate nel quinquennio precedente, in particolare nel quadro del DPCM 17 febbraio 2017[189], recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, nonché delle migliori prassi sviluppate in ambito internazionale. Con questo intervento normativo si è riconosciuta autonomia e centralità alla

[186] Decreto-Legge 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

[187] Dal punto di vista funzionale, l'Agenzia si configura quale centro di elaborazione della strategia nazionale di cybersicurezza.

[188] Oltre all'elaborazione della strategia nazionale di cybersicurezza, l'Agenzia si occupa anche dello sviluppo concreto di capacità operative di prevenzione, rilevazione e risposta agli incidenti. Essa svolge, inoltre, attività di supporto tecnico al CSIRT Italia (*Computer security Incident Team* – è il *team* nazionale di risposta agli incidenti informatici, istituito presso l'ACN che gestisce la sicurezza cibernetica del Paese) e promuove la crescita di un ecosistema di collaborazione pubblico-privato per rafforzare la resilienza del sistema Paese. In virtù dell'assetto normativo vigente, l'ACN ricopre anche il ruolo di Autorità nazionale competente per l'attuazione della direttiva NIS e delle sue successive evoluzioni (NIS2), fungendo da punto di contatto unico (PoC) per la sicurezza delle reti e dei sistemi informativi, da Autorità nazionale di certificazione della cybersicurezza e da Centro Nazionale di Coordinamento (NCC) in relazione al Centro europeo per la cybersicurezza industriale, tecnologica e di ricerca.

[189] Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".

dimensione della sicurezza e della resilienza cibernetica, ricondotta alla diretta responsabilità del Presidente del Consiglio dei ministri quale componente essenziale del processo di digitalizzazione del Paese. Questa scelta sottolinea la volontà di garantire una *governance* più unitaria e strategica della cybersicurezza, basata su una stretta sinergia e un coordinamento operativo tra tutte le Amministrazioni competenti per assicurare coerenza e tempestività d'intervento[190]. Si è così voluto costruire un pilastro ulteriore – affidato a un unico soggetto governativo – complementare alle strutture già esistenti in materia di sicurezza nazionale. Concretamente, l'ACN opera quale interfaccia unitaria, nel rispetto delle competenze specificamente attribuite dalla normativa vigente alle altre amministrazioni, per il coordinamento dei soggetti pubblici coinvolti nella sicurezza e nella resilienza cibernetica, nonché per la rappresentanza univoca del Paese nei contesti internazionali, assicurando una postura nazionale coerente con le linee strategiche definite dalla Presidenza del Consiglio dei ministri. Sembra che in questo modo sia stata superata la frammentazione istituzionale inizialmente determinata dalla dispersione di competenze tra più soggetti.

Alla luce del carattere multidimensionale delle sfide affidate all'ACN, l'intelligenza artificiale assume una posizione strategica: l'Agenzia è investita del compito di garantire un impiego sicuro e affidabile delle tecnologie di AI nei sistemi critici, vigilando sulla coerenza tra innovazione tecnologica, sicurezza cibernetica e tutela dei diritti fondamentali. L'integrazione dell'AI nei processi informatici di analisi, prevenzione e risposta consente infatti di anticipare le minacce attraverso modelli predittivi e apprendimento automatico, migliorando la capacità di rilevamento in tempo reale e la resilienza del sistema Paese. Parallelamente, l'Agenzia agisce quale autorità di riferimento nazionale per l'attuazione del quadro regolatorio europeo in materia di AI – in particolare dell'AI Act[191] – assicurando che lo sviluppo e l'adozione di queste tecnologie avvengano nel rispetto dei principi di trasparenza, tracciabilità e *accountability*. Questo ruolo attribuisce

[190] Di prevenzione e repressione dei reati informatici si occupano le Forze di Polizia; la difesa e la sicurezza militare dello Stato nello spazio cibernetico è di spettanza del Ministero della Difesa; la ricerca e l'elaborazione informativa è di competenza degli organismi di informazione per la sicurezza.

[191] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

all'ACN una funzione di collegamento tra cybersicurezza e *governance* algoritmica, ponendola al centro di un nuovo paradigma strategico in cui innovazione e sicurezza diventano pilastri sinergici della sovranità digitale italiana ed europea.

3. Disinformazione digitale: *filter bubble*, attacchi mirati e vulnerabilità sociale

"La complessità e l'interdipendenza dei sistemi è cresciuta fino a sfumare la dualità tra la dimensione digitale e il mondo reale, rendendo spesso problematica l'identificazione di confini e rispettive caratteristiche"[192]. In questo contesto la disinformazione digitale assume un ruolo cruciale, tanto da comparire come uno dei tre rischi sistemici individuati dall'Agenzia stessa[193].

La proliferazione della disinformazione digitale e delle minacce *cyber* collegate alle piattaforme e ai motori di ricerca costituisce oggi uno dei problemi più sofisticati e complessi affrontati nel campo della sicurezza informatica nazionale e internazionale. La loro intrinseca natura ibrida, che combina aspetti tecnologici, sociali e politici, amplifica le vulnerabilità dell'intero ecosistema digitale, compromettendo la credibilità e l'affidabilità dell'informazione pubblica.

Alle fondamenta di questi preoccupanti effetti si trovano le c.d. *filter bubble* (letteralmente "bolle di filtraggio"), ambienti informativi polarizzati, generati da algoritmi che profilano gli utenti sulla base delle loro preferenze e comportamenti digitali. Gli algoritmi che operano nell'ambito dell'offerta dei principali servizi digitali, quali *social network*, motori di ricerca e piattaforme *streaming*, selezionano automaticamente i contenuti mostrati, in funzione dei dati preesistenti raccolti sugli utenti stessi. La costruzione di queste *filter bubble*, oggetto di discussione scientifica fin dal 2011[194], av-

[192] "Strategia nazionale di cybersicurezza 2022-2026" dell'ACN, p. 4.

[193] Gli altri due rischi riguardano gli "attacchi cyber dovuti a cybercriminali, attivisti o a campagne statuali coordinate" e le "tecnologie impiegate, le quali sono sviluppate e prodotte da grandi realtà aziendali, talvolta controllate o, comunque influenzate nel loro operato dai Governi in cui hanno sede" ("Strategia nazionale di cybersicurezza 2022-2026" dell'ACN, p. 10).

[194] L'elaborazione teorica è frutto del lavoro di Eli Pariser, che nel volume "The Filter Bubble", pubblicato dal Saggiatore nel 2011, descrive il fenomeno come una sorta di spazio digitale costruito su misura in base agli interessi e ai comportamenti online dell'utente:

viene attraverso sistemi di *machine learning* e algoritmi predittivi che analizzano costantemente le interazioni digitali: *click*, *like*, condivisioni, commenti e tempo trascorso su singole pagine, vengono impiegati per prevedere interessi futuri e proporre contenuti che rafforzano le preferenze già manifestate, creando una spirale di selezione e restringimento dell'orizzonte informativo. Questo meccanismo genera l'illusione che ciò che osserviamo *online* rappresenti un quadro completo della realtà, mentre di fatto si tratta di una selezione parziale e costruita esclusivamente in base ai nostri comportamenti e alle nostre precedenti interazioni.

L'urgenza di affrontare la questione non attiene solo alla pubblicità mirata né influisce unicamente sulle nostre abitudini di consumo. Per una quota sempre più consistente di utenti, infatti, piattaforme di notizie personalizzate, come Facebook, stanno assumendo un ruolo centrale come fonti informative principali[195].

Se da un lato questo meccanismo mira a massimizzare il coinvolgimento e la permanenza sulle piattaforme, dall'altro favorisce la formazione di comunità digitali omogenee, che ricevono informazioni convergenti e incrementano il rischio di diffusione di *fake news* e di campagne manipolative. Questi fenomeni alimentano una crisi democratica profonda, attraverso l'influenza che esercitano sulle scelte politiche degli individui e la creazione di divisioni sociali, con conseguenze che si manifestano con-

dalle pagine consultate ai link selezionati, fino alla traccia dei clic compiuti nella navigazione quotidiana. Quanto più ci si muove all'interno della rete, tanto più quest'ultima tende a riflettere e replicare le nostre preferenze, modellandosi su di esse. Si tratta di una "bolla" proprio perché invisibile e inconsapevole: nessuno vi accede intenzionalmente e la maggior parte degli utenti ignora di esserne immersa.

Il fenomeno della *filter bubble*, concettualizzato nel 2011 deve essere tenuto bene distinto da quello dell'*echo chamber*. Quest'ultima rappresenta una dinamica di natura principalmente psicologica e sociale, in cui gli individui scelgono consapevolmente di esporre sé stessi esclusivamente a contenuti, idee e opinioni affini alle proprie convinzioni, isolandosi da prospettive divergenti e rigettando sistematicamente punti di vista alternativi.

[195] L'Osservatorio annuale sul sistema dell'informazione 2025 di Agcom rappresenta come "Tra i più giovani è prevalente, più che nel resto della popolazione, la propensione ad utilizzare un solo mezzo per informarsi che, come facilmente intuibile, può essere identificato in internet." (p. 3). Nello specifico "In Italia la ricerca di notizie in rete avviene prevalentemente tramite i social network (19,8%). Il loro utilizzo anche quale strumento di informazione si caratterizza e distingue per la spiccata pervasività del mezzo, e per la possibilità di condividere e commentare in tempo reale una notizia. " (p. 10). Alle stesse conclusioni giunge anche la ricerca condotta da Pew Research Center "Social Media and News Fact Sheet", pubblicata a settembre 2025.

cretamente nella polarizzazione e nel rafforzamento delle ideologie estreme[196].

Oltre al fenomeno della polarizzazione, assume crescente rilevanza il problema dell'isolamento informativo. Le analisi condotte sui comportamenti degli utenti assidui di *social network* mostrano una tendenza marcata a fidarsi esclusivamente di fonti e notizie che confermano le proprie convinzioni pregresse, evitando o addirittura rifiutando attivamente contenuti che presentano punti di vista divergenti. Questo comportamento genera una rappresentazione parziale e distorta della realtà, aumentando la vulnerabilità degli individui alla diffusione di *fake news* e fenomeni di disinformazione sistematica. Le ripercussioni psicologiche derivate da queste "bolle informative" sono altrettanto significative: studi recenti mettono in luce come l'isolamento informativo favorisca l'incremento di stati emotivi negativi quali ansia e frustrazione, oltre a stimolare processi di radicalizzazione cognitiva. Questi stati contribuiscono a un aumento dell'aggressività nelle comunicazioni *online*, trasformando i dibattiti in confronti ostili e rendendo sempre più difficile la costruzione di dialoghi costruttivi. Seppur il senso di *comfort* e rassicurazione derivante dalla conferma continua delle proprie posizioni appaia immediatamente gratificante, questa dinamica comporta rischi concreti e rilevanti per il tessuto sociale complessivo: limita fortemente la capacità critica e analitica degli individui, concorre a diffondere e radicare la disinformazione e ostacola il confronto dialogico, determinando fratture sociali profonde e difficilmente sanabili. In sintesi, non solo si assiste a un indebolimento della capacità critica, ma paradossalmente si manifesta una crescente ostilità verso quanti si collocano al di fuori della propria bolla informativa.

Dinamiche dello stesso tipo hanno interessato e riguardano tuttora anche contesti bellici e rendono ancora più preoccupante il fenomeno e urgente l'intervento per contenerlo[197].

---

[196] Uno studio dell'Università di Oxford del 2022, focalizzato sulle piattaforme Twitter e Facebook, ha evidenziato che gli utenti esposti in modo continuativo a contenuti polarizzati tendono a rafforzare progressivamente le proprie convinzioni iniziali.

[197] Un'indagine della BBC ha svelato una campagna di propaganda russa condotta attraverso migliaia di account falsi su TikTok, creata per diffondere disinformazione sulla guerra in Ucraina e indebolire il sostegno europeo a Kiev. I video, che hanno raggiunto milioni di visualizzazioni, accusavano falsamente funzionari e familiari di alti ufficiali ucraini di arricchirsi durante il conflitto, diffondendo immagini e voci generate dall'intelligenza artificiale. BBC Verify ha individuato circa 800 profili legati a questo network, mentre TikTok ha dichiarato di aver già eliminato oltre 12.000 account creati in Russia,

Sul fronte specifico delle piattaforme digitali, queste vulnerabilità aumentano in ragione delle logiche di progettazione orientate alla viralità e all'interazione, accompagnate dalla proliferazione di *bot*, *troll farms* e campagne di amplificazione automatizzata. La diffusione di contenuti *deepfake*, ormai difficilmente distinguibili dalla realtà, mette in discussione le regole della moderazione e la responsabilità delle piattaforme nel garantire un ambiente informativo sicuro e affidabile. Il fenomeno interessa intensamente anche i motori di ricerca, ora tutt'altro che neutri. Numerose attività malevole, mirate al furto di dati, alla distribuzione di *malware* di tipo information *stealer* e alle violazioni delle identità digitali, sfruttano infatti la navigazione *online* e i risultati delle ricerche per veicolare sofisticate campagne di phishing e frodi digitali. I dati forniti dall'Agenzia[198] indicano un incremento dell'8,6% nel 2025 degli attacchi basati su URL malevoli, confermando la persistente evoluzione delle minacce. Il phishing continua a rappresentare la tecnica più diffusa poiché coinvolge oltre il 70% degli incidenti registrati.

Quanto alla sicurezza delle reti, gli attacchi di *Distributed Denial of Service* (DDoS) registrano un costante incremento in termini sia di frequenza sia di complessità. Nel corso del 2025, l'Agenzia ha documentato episodi di particolare rilevanza, tra cui appunto una campagna DDoS che ha interessato infrastrutture strategiche italiane per un periodo continuativo di tredici giorni, durante i quali sono stati rilevati oltre 275 attacchi distinti. Questo fenomeno testimonia la crescente sofisticazione e capacità di persistenza delle minacce dirette alla disponibilità dei servizi critici.

Gli stessi risultati si riscontrano anche sul piano europeo. Il Rapporto ENISA Threat Landscape 2024 individua tra le minacce più rilevanti, oltre ai *ransomware* e agli attacchi che compromettono la disponibilità dei servizi (DoS e DDoS), anche le minacce rivolte ai dati, quali violazioni e fughe di informazioni sensibili. Particolare attenzione viene riservata agli attacchi di *social engineering*, che si avvalgono ormai di strumenti tecnologici

che avevano accumulato circa 850.000 follower e miravano a promuovere punti di vista favorevoli al Cremlino anche in Paesi come l'Italia. La strategia comprendeva anche l'uso coordinato di profili con immagini rubate di celebrità e la pubblicazione simultanea di video quasi identici per manipolare l'algoritmo della piattaforma.

Parallelamente, un'indagine del Threat Analysis Center di Microsoft ha riportato un'altra operazione di disinformazione iniziata a luglio 2023: alcuni video di attori noti, manipolati digitalmente, venivano diffusi per screditare il presidente ucraino Zelensky con la falsa accusa di tossicodipendenza.

[198] "Operational Summary 1° semestre 2025. Dati e indicatori della minaccia cyber in Italia" di ACN.

avanzati, in particolare l'intelligenza artificiale generativa, per rendere più efficaci tecniche quali *phishing*, *vishing*, *qishing* e *smishing*.

L'insieme di queste dinamiche solleva interrogativi sulla coesione sociale e sulla tenuta democratica della società. L'ACN riconosce l'urgenza di affrontare la disinformazione e le minacce correlate con un approccio sistemico e integrato, che vada oltre la mera componente tecnologica. È infatti necessario combinare strumenti automatizzati di rilevazione e intelligenza digitale con strategie formative ed educative rivolte alla cittadinanza (all'utenza in questo contesto) per accrescere il pensiero critico e la capacità di orientamento nell'ecosistema informativo complesso e spesso fuorviante.

Senza una consapevolezza attiva e critica da parte degli utenti, la modalità di consumo informativo basata sulle piattaforme digitali e sui risultati delle ricerche, così come l'esposizione quotidiana ad attacchi informatici anche di semplice natura, rischiano di minare o comunque di indebolire l'efficacia delle altre componenti strategiche dell'azione dell'ACN.

4. L'intelligenza artificiale nella cybersicurezza: prospettive per la sicurezza nazionale

In questo panorama, l'intelligenza artificiale, se correttamente progettata e implementata, rappresenta oggi uno degli strumenti più potenti e promettenti nel rafforzamento della sicurezza nazionale in ambito cybersicurezza. Le sue capacità di elaborare grandi quantità di dati in tempi brevissimi, riconoscere *pattern* complessi e adattarsi dinamicamente a contesti in rapido cambiamento la rendono fondamentale per la protezione delle infrastrutture critiche e la difesa degli interessi sovrani dell'intero sistema-Paese[199].

[199] Nel corso del dibattito sull'innovazione tecnologica e la sicurezza digitale in Italia, tenutosi l'8 ottobre scorso presso l'Università Federico II di Napoli nell'ambito del Disclaimer Tour – "AI e criminalità", iniziativa promossa dal Corriere della Sera in collaborazione con CINECA, il Direttore generale dell'ACN, Bruno Frattasi, ha chiarito che "L'intelligenza artificiale è un potente alleato della minaccia cibernetica. Ce ne siamo accorti già da qualche tempo. […] Il phishing è 'migliorato' per quanto riguarda la capacità di ingannare il destinatario. Così come le fake news e i deep fake. L'intelligenza artificiale sta aiutando gli 'attaccanti'. Però va anche aggiunto che l'intelligenza artificiale può rivelarsi una potente arma di difesa dalla stessa minaccia, come tutte le tecniche avanzate che hanno una doppia faccia: la Red e la Blu. La prima è quella nella quale identifichiamo gli attaccanti e gli aggressori informatici, quella Blu è quella con la quale identifichiamo la parte buona, quella che combatte i criminali".

L'IA consente un rilevamento precoce e una risposta tempestiva a minacce informatiche sofisticate, abbattendo i tempi di reazione e massimizzando la precisione nell'individuazione di attacchi potenziali come intrusioni, *malware* o campagne di disinformazione automatizzate. Attraverso sofisticati algoritmi di *machine learning* e *deep learning*, è possibile analizzare in modo proattivo flussi di dati complessi provenienti da fonti eterogenee e individuare anomalie che sfuggirebbero ai tradizionali sistemi manuali o basati su firme statiche.

Questa trasformazione tecnologica si traduce in un vantaggio strategico cruciale per la cybersicurezza nazionale, poiché rende possibile non solo la possibilità di difendersi efficacemente, ma anche di anticipare le mosse degli attori ostili, siano essi gruppi criminali, enti statali o attori ibridi. Inoltre, l'IA consente di automatizzare e ottimizzare le risorse umane e tecnologiche dedicate, incrementandone così l'efficienza e riducendo la possibilità di errore umano.

Naturalmente, un'adozione responsabile e consapevole dell'IA deve includere un rigoroso controllo sui profili di sicurezza, trasparenza, rispetto della *privacy* e limitazione dei *bias* algoritmici. L'ACN si pone come garante di queste condizioni, promuovendo l'uso delle tecnologie IA all'interno di un quadro normativo e deontologico rigoroso, che salvaguardi i diritti fondamentali e la sovranità digitale. Sul piano operativo, si sta investendo nel rafforzamento delle competenze tecniche, nella formazione di esperti di alto profilo e nella creazione di *partnership* pubblico-privato per lo sviluppo di soluzioni IA innovative. Questi sforzi consentono di integrare efficacemente l'IA nelle infrastrutture di monitoraggio, prevenzione e risposta agli incidenti *cyber*, migliorando la resilienza complessiva del sistema-paese.

In questo scenario, la dimensione internazionale gioca un ruolo altrettanto cruciale. La cooperazione con organismi europei e internazionali nella definizione di *standard* comuni e nella condivisione di conoscenze è fondamentale per contrastare minacce che, per loro natura, non possono essere contenute entro confini nazionali. L'IA emerge quindi come uno strumento di sicurezza nazionale non soltanto tecnico, ma anche geopolitico, in grado di migliorare la capacità di deterrenza e di risposta coordinata sul piano globale.

5. L'approccio integrato tra consapevolezza dei cittadini e investimenti strutturali per il Paese

Nell'attuale contesto caratterizzato da sfide informatiche sempre più pervasive e sofisticate, l'Agenzia per la Cybersicurezza Nazionale adotta un modello strategico che coniuga, in modo sinergico e integrato, il rafforzamento infrastrutturale con la promozione della consapevolezza e della formazione digitale tra la popolazione e gli operatori economici e istituzionali, secondo un approccio *whole-of-society*[200]. Questo approccio riconosce la cybersicurezza non solo come una questione tecnica, ma come una dimensione sociale che coinvolge attivamente cittadini, imprese, enti pubblici e privati nell'adozione di comportamenti responsabili e nella costruzione di una cultura condivisa della sicurezza digitale.

L'idea di fondo è che "l'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso"[201].

A partire da questo tipo di impostazione, l'ACN fonda il proprio piano di azione su un duplice fronte: quello tecnico e quello sociale. La Strategia nazionale di cybersicurezza 2022-2026 a questo proposito parla di "fattori abilitanti," che comprendono formazione tecnico-specialistica e diffusione della cultura del rischio, in un quadro sistemico e partecipativo.

Sul fronte tecnico-infrastrutturale, la strategia dell'ACN si orienta verso la realizzazione e il potenziamento di sistemi resilienti e interoperabili, capaci di assicurare la continuità operativa e di contrastare efficacemente minacce digitali di crescente complessità. Questo include, in particolare, lo sviluppo del Polo Strategico Nazionale (PSN), piattaforme di monitoraggio avanzato e reti di laboratori d'eccellenza, che fungono da pilastri tecnologici del sistema nazionale di difesa cyber. Essenziale è l'aderenza a standard internazionali ed europei, come quelli previsti dal Regolamento NIS2 e dal Cybersecurity Act, che garantiscono obblighi rigorosi di audit e certificazione, salvaguardando la sicurezza lungo l'intero ciclo di vita delle infrastrutture digitali.

Parallelamente a questa dimensione tecnica, l'ACN rivolge un'attenzione prioritaria allo sviluppo di competenze e alla diffusione di una cultura della sicurezza *cyber* che permei tutta la società. Operando in sinergia con istituti scolastici, università, aggregazioni industriali e centri di ricerca,

[200] Così viene definita la propria strategia dall'ACN nel documento "Strategia nazionale di cybersicurezza 2022-2026".

[201] Strategia nazionale di cybersicurezza 2022-2026", p. 8.

l'Agenzia promuove iniziative di alfabetizzazione digitale fin dalla scuola primaria, sensibilizzazione continua e formazione specialistica mirata. Progetti come "Repubblica Digitale" e "Punto Digitale Facile"[202] sono emblematici di questa strategia: offrono strumenti e risorse per l'inclusione digitale e per il rafforzamento delle capacità critiche degli utenti, in particolare tra le fasce più vulnerabili e meno esperte. La promozione di un programma capillare di educazione digitale, da attuare anche mediante strumenti online, mira a sensibilizzare la collettività sull'adozione di *best practices* e sulla capacità di riconoscere contenuti *fake* e manipolativi. Analogamente, si investe in campagne di sensibilizzazione all'interno delle organizzazioni pubbliche e private che intendono promuovere una "*cyber hygiene*" diffusa, l'incremento della consapevolezza sui rischi e sulle minacce presenti e la gestione attenta del rischio residuo anche attraverso strumenti di autovalutazione basati su indicatori specifici quali i "*cyber index"*.

L'integrazione tra gli investimenti strutturali e la formazione degli individui genera un ecosistema complesso di sicurezza in cui l'adozione di tecnologie avanzate si accompagna a comportamenti virtuosi e a una responsabilizzazione attiva dei cittadini. La piattaforma "Cybersicurezza Italia" costituisce un luogo privilegiato di confronto, formazione e diffusione delle *best practices*, rafforzando la fiducia collettiva e stimolando la partecipazione civica alla tutela della resilienza digitale nazionale.

L'integrazione di competenze e risorse tra attori istituzionali, aziende strategiche e operatori tecnologici consente di fronteggiare efficacemente eventi critici e minacce emergenti, assicurando un adeguato grado di preparazione e risposta nell'intero tessuto produttivo e infrastrutturale.

[202] "Punto Digitale Facile" rappresenta una rete capillare di sportelli e servizi dedicati a facilitare l'accesso digitale per i cittadini, distribuita su tutto il territorio nazionale. Al 2024, secondo i dati forniti dal Dipartimento per la Trasformazione Digitale (DTD) in collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), sono stati attivati all'incirca 2.220 punti di accesso digitali, che hanno fornito supporto diretto a oltre 264.000 utenti. Il profilo prevalente degli utenti assistiti comprende donne adulte con livello di istruzione che va dalla scuola primaria a quella secondaria, nonché persone disoccupate o lavoratori dipendenti. Il progetto ha prodotto un miglioramento significativo nella consapevolezza digitale di base, traducendosi in una riduzione stimata del 18% negli incidenti di phishing e nelle frodi online nelle aree servite, rispetto agli anni precedenti. Il progetto rappresenta un esempio concreto dell'impegno dell'ACN nell'estendere l'accesso alle competenze digitali e nell'abbattere il *digital divide*, con un impatto tangibile sulla riduzione di incidenti di phishing e frodi online nelle aree di intervento.

6. Conclusioni

L'esperienza quotidiana e le responsabilità istituzionali dell'Agenzia per la Cybersicurezza Nazionale orientano la consapevolezza sull'importanza cruciale di un approccio integrato e multilivello nella lotta alla disinformazione online e nella tutela della sicurezza nazionale digitale. La molteplicità e la complessità delle minacce, amplificate dalla rapida evoluzione tecnologica e dalla proliferazione di contenuti digitali manipolativi, impongono un impegno costante e articolato, che solo un'efficace *governance*, in cui l'ACN svolge un ruolo di coordinamento primario, può gestire con efficacia.

Guardando al futuro, è chiaro che l'innovazione tecnologica – in particolare l'adozione responsabile e avanzata dell'intelligenza artificiale – rappresenta una risorsa strategica imprescindibile per rafforzare la resilienza del sistema Paese. La capacità di anticipare, monitorare e rispondere alle minacce *cyber* va necessariamente accompagnata da un investimento continuo nella formazione, nella sensibilizzazione e nella costruzione di una cultura digitale diffusa, che coinvolga trasversalmente tutti i cittadini, le istituzioni e le imprese. Solo la partecipazione attiva e consapevole dell'intera comunità nazionale può trasformare la cybersicurezza da mero obiettivo tecnico a una dimensione condivisa di tutela collettiva di e sovranità digitale.

L'ACN è chiamata a rinnovare il proprio impegno non solo nel perfezionamento degli strumenti tecnologici e normativi, ma anche nell'ampliamento delle collaborazioni strategiche con il mondo accademico, industriale e internazionale, favorendo lo scambio di best practice e la ricerca di soluzioni innovative e sostenibili. In questa prospettiva, la costruzione di un ecosistema *cyber* nazionale integrato, capace di rispondere in modo tempestivo ed efficiente alle sfide future, si configura come la priorità assoluta per i prossimi anni. Sarà fondamentale sviluppare modelli di cooperazione internazionale ancora più efficaci, in quanto nessun Paese, da solo, può affrontare adeguatamente quel panorama globale di rischi e opportunità che caratterizza il cyberspazio contemporaneo.

Il ruolo dell'Agenzia, pertanto, si conferma centrale nel promuovere una cultura della prevenzione che unisca capacità tecnologiche, competenze umane e responsabilità pubblica, creando le condizioni perché il digitale resti uno spazio di partecipazione libera, sicura e affidabile.

Il volume Consumerism 2025 raccoglie contributi dedicati all'analisi del ruolo delle autorità indipendenti nella regolazione dell'economia delle piattaforme digitali, alla luce dei profondi mutamenti introdotti dalla digitalizzazione dei mercati e dalla diffusione dell'intelligenza artificiale. L'indagine attraversa i principali ambiti di intervento — privacy, comunicazioni, concorrenza, energia, trasporti, mercati finanziari e cybersicurezza — mettendo in evidenza le sfide poste da modelli economici fondati sulla raccolta e sull'uso dei dati personali e sull'intermediazione digitale. L'obiettivo è interrogarsi sulla capacità dell'attuale assetto normativo e istituzionale di coniugare innovazione, tutela dei diritti fondamentali e fiducia dei consumatori. Le riflessioni raccolte offrono una lettura trasversale della trasformazione in atto, proponendo chiavi interpretative utili per la definizione di un nuovo modello di vigilanza e di governance cooperativa tra Autorità.

FABIO BASSAN

è professore ordinario di diritto internazionale e diritto dell'Unione Europea presso l'Università di Roma Tre. Si occupa da molti anni dei temi del diritto dei consumatori e delle tecnologie.

Roma Tre