CONSUMERS' FORUM

PRESENTA



Consumerism 2026

Agenda 2030 - Il Consumatore ibrido

in collaborazione con

ROMA TRE
UNIVERSITÀ DEGLI STUDI



CONSUMERS' FORUM

in collaborazione con

con il patrocinio di

Il consumatore ibrido:
infrastrutture, regolazione, tecnologie
XXI appuntamento annuale con le Authority

Roma, 18 novembre 2026
h 9.30/13.30 presso
Europa Experience – David Sassoli
Centro interattivo in Italia del Parlamento europeo e della Rappresentanza della Commissione europea - Piazza Venezia 6c, Roma

Esperienza Europa – David Sassoli
Europa Experience – David Sassoli

R.S.V.P. eventi@consumersforum.it

PROGRAMMA

h 9.30 inizio lavori

Saluti istituzionali
Carlo Corazza – Direttore del Parlamento Europeo in Italia
Massimo Pronio – Responsabile Comunicazione Commissione europea in Italia
Mara Bizzotto - Presidente Consiglio Nazionale dei Consumatori e degli Utenti**

Relazione a cura di
Fabio Bassan - Professore Ordinario di Diritto dell'Unione Europea Università degli Studi Roma Tre
Consumerism 2026: "Agenda 2030 - Il Consumatore ibrido"

Contributo alla discussione - intervista doppia con
Gianpiero Strisciuglio – Amministratore Delegato Gruppo Ferrovie dello Stato
Pietro Labriola – Amministratore Delegato TIM
Condotta da
Giovanna Pancheri - Giornalista Sky Tg24

Il punto di vista delle Authority*
Pasquale Stanzione – Presidente Autorità Garante per la Protezione dei Dati Personali
Giuseppe Busia - Presidente Autorità Nazionale Anticorruzione
Giacomo Lasorella – Presidente Autorità per le Garanzie nelle Comunicazioni
Guido Stazi – Presidente Commissione Nazionale per le Società e la Borsa
Maddalena Rabitti – Componente del Direttorio Integrato e del Consiglio Istituto per la Vigilanza sulle Assicurazioni
Fabrizio Balassone - Vice Capo Dipartimento Tutela della clientela ed educazione finanziaria Banca d'Italia
Nicola Dell'Acqua - Presidente Autorità di Regolazione per Energia, Reti e Ambiente
Nicola Zaccheo – Presidente Autorità di Regolazione dei Trasporti
Alberto Bagnai – Componente dell'Autorità Garante della Concorrenza e del Mercato
Modera
Furio Truzzi - Presidente Consumers' Forum

Contributo alla discussione - intervista doppia con
Giovanni De Cristofaro - Presidente Adiconsum
Giovanni Bellissima - Presidente Adoc
Condotta da
Fulvio Migliaccio - Giornalista - inviato Rai Parlamento

h 13.30 fine lavori

Consumers' Forum

e

Università degli Studi Roma Tre

presentano

CONSUMERISM 2026

Agenda 2030 - Il Consumatore ibrido

La versione integrale di "Consumerism 2026" è disponibile sul sito di Consumers' Forum

Il lavoro riflette esclusivamente le opinioni dei singoli Autori e non rappresenta le posizioni ufficiali di Consumers' Forum.

SOMMARIO

IL CONSUMATORE IBRIDO 2030 5

(di Fabio Bassan)

1. Il Consumatore ibrido sul piano regolatorio e dello stato sociale. 5
2. Dalla protezione dei dati personali alla sicurezza. Il GDPR porta d'ingresso degli ordinamenti 7
3. Il nuovo paradigma della concorrenza 8
4. I mercati finanziari e la trasformazione del paradigma informativo 9
5. Il consumatore automa: IA agentica anche nei pagamenti 9
6. L'Avatar dell'assicurato 10
7. Il consumatore soggetto e oggetto dell'ecosistema della mobilità 11
8. Il prosumer energetico evoluto 12
9. Contratti sovrani 13
10. Cittadinanza digitale intermediata dall'infrastruttura privata 13
11. Sicurezza, parametro della sovranità 15
12. Brevi 'conclusioni introduttive': il 'concerto regolatorio a due versanti' come strumento finale 16

AUTORITÀ E CONSUMATORI 2030: DALLA FRAMMENTAZIONE DELLE REGOLE ALLA TRASVERSALITÀ DELLA TUTELA 17

(di Paolo Occhiuzzi)

1. Dal consumatore "contraente debole" al consumatore nel mercato 17
2. Dalla modernizzazione dell'acquis al nuovo ordine regolatorio europeo 19
3. Il consumatore digitale verso il 2030: dalla trasparenza alla fairness 21
4. La transizione sostenibile: un secondo banco di prova 25
5. Dalla frammentazione regolatoria alla coerenza del sistema: regole trasversali e coordinamento tra Autorità 26
6. Autorità e consumatori 2030: dalla cross-regulation alla cross-enforcement? 28

IL CONSUMATORE 2030 IN UN *DIGITAL WELFARE* IBRIDO 31

(di Marco Cappai)

1. Pubblico-Privato, dagli incroci alle rotatorie 31
2. Prima rotatoria: Digital (Fundamental) Rights 32
3. Seconda rotatoria: Technology Regulation 34
4. Terza rotatoria: dalla Technology Regulation alla Digital (o Technological) Sovereignty 36
5. Ricadute per il diritto dei consumi: dai servizi, all'adeguatezza organizzativa, alle infrastrutture 38

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PRIORITÀ E QUESTIONI APERTE PER L'AZIONE DELLE AUTORITÀ INDIPENDENTI IN UN MONDO CHE CAMBIA 40

(di Aurora Saija)

1. Premessa e obiettivo dell'analisi 40
2. Le sfide per la protezione dei dati derivanti dalla situazione geopolitica 41
3. Le sfide per la protezione dei dati derivanti dall'evoluzione della tecnologia 43
4. Salvaguardare l'approccio regolatorio europeo e rafforzare la cooperazione 47

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

AGCM E TUTELA DEL CONSUMATORE IBRIDO 50

(di Sara Perugini)

1. Premessa 50
2. Il quadro normativo di riferimento: cenni 51
3. Utilizzo delle tecnologie digitali e consapevolezza ambientale: l'azione dell'AGCM a tutela del consumatore ibrido 53
4. Considerazioni conclusive 56

COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA

LA TUTELA DELL'INVESTITORE RETAIL VERSO IL 2030: DIGITALIZZAZIONE DEI MERCATI, METAMORFOSI DELLE INFRASTRUTTURE E NUOVE SFIDE PER LA VIGILANZA 58

(di Matteo Ghezzi)

1. Premessa 58
2. Dall'intermediazione finanziaria tradizionale alle piattaforme di *trading*: nuove modalità di accesso al mercato dell'investitore *retail* 60
3. La metamorfosi delle infrastrutture: *blockchain* e *cryptoassets* 63
4. I fattori di rischio connessi alla digitalizzazione delle infrastrutture e nuove forme di tutela 65
5. Verso un'agenda CONSOB 2030: consolidamento di una vigilanza *data-driven* e multilivello 68

BANCA D'ITALIA 71

DAL CONSUMATORE DIGITALE AL CONSUMATORE AGENTICO: INFRASTRUTTURE E REGOLE DEI SERVIZI DI PAGAMENTO EUROPEI VERSO IL 2030. 71

(di Armando Di Cello)

1. Premessa. Dal consumatore digitale al consumatore agentico 71
2. L'architettura europea dei pagamenti verso il 2030 73
3. I pagamenti agentici: nuovo paradigma, stesse regole? 74
4. Conclusioni. Le priorità per la tutela dell'utente di servizi di pagamento nel 2030 78

ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI (IVASS)

ASSICURARE L'IMPIEGO NON PROFESSIONALE DI AGENTI IA **81**

(di Vincenzo Orsini)

1. L'agentic AI 81
2. Il dato positivo 82
3. La proposta di un'assicurazione obbligatoria 84
4. Il problema dell'interesse all'assicurazione 85
5. I criteri di imputazione della responsabilità 87
6. Considerazioni conclusive 90

AUTORITA DI REGOLAZIONE DEI TRASPORTO

DALLA TUTELA DEL PASSEGGERO ALLA REGOLAZIONE DELLA MOBILITÀ. IL CONSUMATORE 2030 E IL RUOLO DELL'AUTORITÀ DI REGOLAZIONE DEI TRASPORTI. **93**

(di Federico Nespega)

1. Dal passeggero al consumatore di mobilità 93
2. La tutela del consumatore nella costruzione regolatoria del mercato 96
3. Nuove asimmetrie nella mobilità digitale 99
4. Dal reclamo alla regolazione anticipatoria 101
5. Verso il 2030: l'ART tra efficienza del mercato e inclusione della mobilità 104

AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE (ARERA)

ARERA AL FRONTE. IL "CONSUMATORE 2030", TRA POLICRISI E MONITORAGGIO CONTINUO **106**

(di Cristiana Lauri)

1. Premessa: il 2030 come orizzonte regolatorio 106
2. Una regolazione alla prova della policrisi 107
3. Energia elettrica e gas: mercati e reti 108
4. I settori ambientali: acqua, rifiuti e telecalore 109
5. Tecnologie abilitanti e rischi emergenti 110
6. Tutela, enforcement e governance 111
7. Conclusioni e raccomandazioni 112

AUTORITA NAZIONALE ANTICORRUZIONE

SOVRANITÀ DIGITALE E CONTRATTI PUBBLICI: IL NUOVO PARADIGMA DEGLI AFFIDAMENTI *CLOUD* E *AI* **114**

(di Serafina Piantedosi)

1. Sovranità digitale e infrastrutture immateriali: *IL CLOUD AND AI DEVELOPMENT ACT*. 114
2. Lo sviluppo di un ecosistema europeo del *CLOUD* e dell'ia. 117

3. Gli affidamenti pubblici per *cloud* e intelligenza artificiale. 119
4. Le prospettive di vigilanza e il possibile ruolo di ANAC. 120
5. Conclusioni. 122

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM)

COMUNICAZIONI ELETTRONICHE, MEDIA E AUDIOVISIVO NEL 2030: CONSUMATORI SEMPRE PIÙ CONNESSI, PERSONALIZZATI E VULNERABILI 124

(di Francesca Pellicanò e Rosaria Petti)

1. Premessa (Rosaria Petti) 124
2. Alla scarsità dei contenuti alla scarsità dell'attenzione *(Francesca Pellicanò)* 125
3. I principali profili di attenzione per i consumatori nel 2030 *(Francesca Pellicanò)* 127
   - *3.1.1. La trasparenza dell'algoritmo e la libertà di scelta 127*
   - *3.1.2. Il consumatore minore e la protezione dai rischi digitali 128*
   - *3.1.3. Pubblicità, influencer e nuove forme di persuasione 129*
   - *3.1.4. Il prezzo dell'accesso e la nuova economia degli abbonamenti 129*
   - *3.1.5. Pluralismo, qualità dell'informazione e disinformazione 130*
   - *3.1.6. Accessibilità e inclusione 130*
4. Aspetti strategici (Francesca Pellicanò) 130
5. Conclusioni: dal consumatore spettatore al consumatore "algoritmicamente mediato" *(Francesca Pellicanò)* 132
6. La tutela del consumatore nelle comunicazioni elettroniche *(Rosaria Petti)* 133
   - *6.1.1. Dalla disponibilità della rete alla qualità dell'esperienza digitale (Rosaria Petti) 135*
   - *6.1.2. La connettività come servizio essenziale (Rosaria Petti) 136*
   - *6.1.3. Switching e libertà di uscita: bundle, convergenza e rischio di lock-in (Rosaria Petti) 137*
   - *6.1.4. Personalizzazione delle offerte e rischio di discriminazione (Rosaria Petti) 138*
7. Le prospettive per AGCOM nel periodo 2026–2030 nel settore delle comunicazioni elettroniche *(Rosaria Petti)* 139
8. Quali conclusioni per le comunicazioni elettroniche? *(Rosaria Petti)* 140

AUTORITÀ NAZIONALE PER LA CYBERSICUREZZA (ACN)

IL BENE DI CONSUMO COME OGGETTO DI SICUREZZA NAZIONALE. COMPETENZE, LIMITI E SPAZI DI INTERVENTO DELL'ACN NELL'ORIZZONTE 2030 142

(di Michela Mastrantonio)

1. Introduzione. Il nuovo oggetto della sicurezza 142
2. Orizzonte 2030: i rischi emergenti 143
3. I limiti della competenza e il contenuto della funzione anticipatoria 146
4. I possibili spazi di intervento dell'ACN 148
5. Conclusioni 154

IL CONSUMATORE IBRIDO 2030

(di Fabio Bassan)

SOMMARIO: 1. Il consumatore ibrido sul piano regolatorio e dello stato sociale. 2. Dalla protezione dei dati personali alla sicurezza. Il GDPR porta d'ingresso degli ordinamenti. 3. Il nuovo paradigma della concorrenza. 4. I mercati finanziari e la trasformazione del paradigma informativo. 5. Il consumatore automa: IA agentica anche nei pagamenti. 6. l'avatar dell'assicurato 7. Il consumatore soggetto e oggetto dell'ecosistema della mobilita'. 8. il *prosumer* energetico evoluto. 9. Contratti sovrani. 10. Cittadinanza digitale intermediata dalla infrastruttura privata. 11. Sicurezza, parametro della sovranità. 12. Brevi 'conclusioni introduttive': il 'concerto regolatorio a due versanti' come strumento finale.

1. Il Consumatore ibrido sul piano regolatorio e dello stato sociale.

Quello del Rapporto Consumerism, superati ormai i vent'anni, è un gruppo di lavoro - che nasce da un dottorato, "Mercati, consumatori e Imprese" di Roma Tre che Consumers' Forum ha sostenuto a lungo – che è ormai maturo, non necessita più di una guida e per questo mi limito ora a coordinare. L'influenza ventennale di Liliana Rossi Carleo, Maddalena Rabitti e mia certo traspare ma non è più un ombrello: gli autori se ne emancipano con disinvoltura e seguono percorsi indipendenti. Il Rapporto di quest'anno ne è la prova. Il titolo "Il consumatore ibrido 2030" propone un tema – che origina da un libro recente[1] - che non richiede solo un'analisi della regolazione ma crea l'aspettativa di proposte e percorsi. Una sfida nuova, che gli autori hanno accettato con entusiasmo e ha prodotto una ricerca innovativa nel metodo, nei contenuti e nelle proposte.

Paolo Occhiuzzi e Marco Cappai sono gli autori dei due interventi introduttivi, che muovono da prospettive diverse – regolatoria e di welfare - ma giungono a conclusioni coerenti tra loro.

Lo spunto da cui parte Paolo Occhiuzzi è la constatazione che è ormai insufficiente un modello di tutela imperniato sulla trasparenza e sull'informazione; modello che cede non solo all'emersione di nuove pratiche commerciali ma anche alla progressiva trasformazione dell'ambiente nel quale si forma la decisione di consumo. Su questa base Occhiuzzi propone due direttrici di ricerca: la prima attiene alle tecniche con cui l'architettura digitale può incidere sulla formazione della volontà del consumatore: *dark patterns*, *addictive design*, sistemi di raccomandazione, personalizzazione delle offerte e tecniche di *nudging*. La seconda riguarda il soggetto destinatario della tutela. La capacità degli operatori di personalizzare l'ambiente nel quale si forma la decisione economica rende infatti inadeguata la figura astratta del consumatore medio.

E allora, una soluzione in prospettiva – anticipata dal *EU KIDS Act* – è quella di ridurre gli oneri del consumatore, oggi gravato di tutta l'attività informativa e cognitiva necessaria per colmare le inefficienze del mercato che rendono altrimenti inapplicabile l'intero apparato normativo digitale – e virare verso obblighi di *safety by design*. La responsabilità della tutela si sposterebbe così dalla capacità del consumatore vulnerabile di riconoscere e contrastare il condizionamento, alla responsabilità del professionista nella predisposizione dell'ambiente nel quale la decisione viene assunta. È una direzione corretta, mi pare, verso la quale ci ha instradati l'AI Act, ed è forse questo il precipitato più efficace di quel regolamento: a una ripartizione dei livelli di rischi consegue una distribuzione di responsabilità della filiera che alleggerisce gli oneri per il consumatore. Eterogenesi dei fini, ma solo se lo si legge con superficialità.

In questo contesto, ci dice Occhiuzzi, la specializzazione delle regole e la trasversalità della tutela non rappresentano tendenze necessariamente contrapposte, che anzi dalla loro capacità di integrarsi dipende la coerenza complessiva del sistema. La questione del consumatore 2030 diviene così, anzitutto, un tema di coerenza regolatoria. Questo è ancor più vero nell'ambiente digitale, che rende sempre meno netti i confini tra i mercati. Una piattaforma può essere contemporaneamente intermediaria commerciale, fornitore di servizi digitali, utilizzatore di dati personali, soggetto rilevante ai fini della concorrenza e utilizzatore o fornitore di sistemi di intelligenza artificiale. Una medesima condotta può incidere contemporaneamente sulla protezione dei dati, sulla concorrenza, sulla libertà di scelta del consumatore e sulle regole proprie del mercato interessato. Per queste ragioni, per Occhiuzzi, il tema centrale diventa la coerenza complessiva del sistema e la risposta diventa il coordinamento tra le Autorità che esercitano competenze sui mercati digitali. Primi modelli europei sono il *High Level Group* previsto nell'ambito del DMA, e il *Digital Fairness Fitness*

1. F. Bassan, L'era ibrida – Sovranità e democrazia tra poteri pubblici e imprese tech, 2026, Rubbettino.

Check. Il *Digital Fairness Act* diventa peraltro un fil rouge che unisce molte delle analisi dei capitoli successivi: evidentemente è un 'paradigma regolatorio contenitore' che consente applicazioni diverse e può essere riempito di contenuti (come è stato per la responsabilità sociale d'impresa e i reati presupposto).
Quindi, conclude Occhiuzzi, l'auspicio per il 2030 è che si passi dalla *cross regulation* al *cross enforcement*, che è non solo uno slogan (bello, peraltro), ma un obiettivo da raggiungere attraverso un percorso i cui snodi vengono illustrati da Occhiuzzi in dettaglio.

Dal *cross enforcement* di Occhiuzzi, con Cappai si passa all'esame dell'ibridazione del *welfare*, sempre via digitale. Cappai muove dagli standard di protezione elaborati dalle tesi del 'costituzionalismo digitale' e concentra l'analisi sui precipitati della contaminazione tra pubblico e privato, anche nel diritto dei consumi, e ipotizza (ma in fondo, auspica) lo spostamento della regolazione europea dai servizi digitali agli assetti organizzativi degli operatori e, in ultima analisi, alle infrastrutture (e alla tecnologia, quando intesa come infrastruttura). Queste ultime sono il centro dello sviluppo del mercato, e diventano oggetto di analisi giuridica sia per il diritto internazionale – perché l'infrastruttura sostituisce il territorio come fondamento della sovranità – sia per lo stato sociale, nell'ordinamento interno, e in via derivata – ma non intermediata - per il diritto dei consumi. La sovranità digitale, dice Cappai, se liberiamo l'infrastruttura dalla sovrastruttura, è sovranità tecnologica. E dunque, se 'pensiamo infrastrutturalmente', come ci suggerisce Ben Kingsbury, lacune normative (quanto alle infrastrutture), sovrapposizioni (su prodotti e servizi) e superstizioni (una tra tutte tra tutte: la neutralità tecnologica come presupposto dell'intervento regolatorio) emergono in modo più chiaro.
Anche Cappai traccia un suo percorso originale – questo, del resto, era il tema di ricerca – per il quale propone rotatorie, più moderne degli incroci con semafori; un semaforo classico, ad esempio, è quello della sussidiarietà, che indica chi tra Stati e Unione e, nel nostro ordinamento, tra regioni e Stato, deve intervenire per primo. La rotatoria di Cappai evita la contrapposizione e supporta la cooperazione sia tra autorità sia tra autorità e mercato, applicando modelli – circolo regolatorio e regolazione partecipata – che proprio i rapporti annuali Consumerism hanno proposto, rafforzato e consolidato, fino a trasformarli in standard interpretativi del diritto dei mercati.

Occhiuzzi e Cappai, con percorsi diversi, giungono alle stesse conclusioni: se ibrido è il contesto, di mercato e istituzionale, ibrida non può essere la norma, che sarebbe inefficace e inefficiente. La soluzione è invece il coordinamento, sul piano normativo, e la cooperazione – che non è ibridazione - sul piano dell'esecuzione delle norme e dell'enforcement, tra autorità indipendenti e tra queste e il mercato.

Vediamo ora come gli altri autori hanno sviluppato il tema nei settori specifici. Partiamo dalle discipline trasversali, orizzontali (protezione dei dati personali e concorrenza) e passiamo poi ai silos verticali, seguendo la semantica, e la tecnica della matrice, di nuovo, elaborata all'interno dei rapporti Consumerism e divenuta ormai strumento condiviso di analisi della regolazione.

2. Dalla protezione dei dati personali alla sicurezza. Il GDPR porta d'ingresso degli ordinamenti

La qualifica di protezione dei dati personali, ci dice Aurora Saija, è ormai inadeguata perché insufficiente: "la protezione dei dati assume un ruolo che supera la dimensione della privacy e del controllo consapevole dell'individuo sull'uso delle informazioni che lo riguardano: da un lato, diventa fattore decisivo nella realizzazione degli obiettivi di sovranità e resilienza perseguiti a livello nazionale e sovranazionale, dall'altro, si conferma strumento indispensabile per affermare la dignità e la centralità della persona". Dunque, non si può più affrontare questa disciplina senza collegarla, sul piano degli effetti, a quella della sicurezza e in ultima analisi, della sovranità digitale, tanto più ora che siamo oggetto (e speriamo di non diventare soggetti) della guerra ibrida, lanciata senza dichiararla da infrastrutture, pubbliche private o ibride anch'esse.
Avanza un tema duplice, di coordinamento sia tra le norme del GDPR e quelle su IA, cybersecurity e affini (incluse DORA e NIS II), sia tra le autorità nazionali competenti a darvi attuazione. Tutti d'accordo, sin qui, coerentemente con quanto illustrato da Occhiuzzi. Saija però lancia anche una sua suggestione: l'interconnessione tra i due plessi normativi può costituire un'opportunità, se *via* Brussels' effect il GDPR – diffusamente applicato nel mondo, anche in Cina - esporta le norme europee sulla sicurezza e sull'IA, consentendone un'efficacia extraterritoriale. L'idea del GDPR come porta d'ingresso in ordinamenti di paesi terzi per la regolazione europea è suggestiva e merita approfondimenti.

3. Il nuovo paradigma della concorrenza

Sara Perugini rende evocativo il luogo d'elezione dell'analisi della concorrenza: il mercato per il consumatore (il punto vendita, fisico o digitale) "abbandona la rigida funzione spazio transazionale per farsi teatro narrativo ed esperienziale". Il consumatore è fragilissimo, quasi di vetro: non compra il prodotto ma l'esperienza in cui è coinvolto e che gli viene promessa. Al contempo il consumatore non è un passivo terminale ultimo della catena del valore, ma diventa "un soggetto ibrido che si muove fluidamente in un ecosistema multicanale, destabilizzando i confini tra spazio online e offline". Insomma, "il legislatore contemporaneo si trova nella condizione di dover tutelare un soggetto che, sebbene mantenga la vulnerabilità tipica della persona fisica di fronte a giganti tecnologici e algoritmi predittivi, esercita al contempo un potere di influenza e produzione mai registrato prima".
Il problema qui è gigante: siamo di fronte non a due facce di una medaglia ma a una vera antinomia, semantica (strutturale) e giuridica (reale, non apparente, secondo le categorie di Bobbio), che è per i giuristi più o meno quello che la stagflazione è per gli economisti, o un problema indecidibile di Gödel per i matematici.
La tendenza, se non la soluzione, ci dice Perugini, è questa: l'asse degli oneri, che fino a poco fa gravavano sui consumatori, attori a cui si chiedeva di colmare le lacune del sistema facendosi di volta in volta parti diligenti, attive o propulsive, si sposta sugli operatori. Questi ultimi partecipano alla fase di formazione delle norme (e qui l'ibridazione tra pubblico e privato raggiunge il diapason), alla loro esecuzione (via creazione di standard e design) e all'enforcement (mediante l'adozione di impegni nei procedimenti davanti alle autorità). Le soluzioni proposte da Perugini sono coerenti con quelle di Occhiuzzi, Cappai e Saija.
Tutto bene, finché non c'è una concentrazione eccessiva sul mercato. Di qui, la rilevanza rinnovata dell'autorità per la concorrenza, che diventa il centro dell'azione regolatoria, non più però ex post (funzione sanzionatoria) ma ex ante (funzione conformativa) e gli impegni diventano una prassi tanto consolidata da essere trasposta anche ai mercati finanziari e assicurativi. Anche questo è un precipitato dirompente, quasi inevitabile ma che merita approfondimenti.

Se andiamo ai 'silos verticali', le analisi diventano specifiche e le soluzioni dettagliate.

4. I mercati finanziari e la trasformazione del paradigma informativo

Matteo Ghezzi ci dice che nei mercati finanziari la tutela dell'investitore al dettaglio si sposterà dalla trasparenza informativa alla progettazione degli ambienti digitali in cui si prendono le decisioni di investimento. Due sono i percorsi trasformativi che individua. La prima trasformazione riguarda l'accesso al mercato: le piattaforme di trading (neobrokers) riducono costi e barriere e favoriscono un investimento in prima persona. L'intermediario cambia ruolo. Gli utenti più giovani rendono ibrido l'investitore retail, a metà tra consumatore e operatore di un mercato complesso. Questo percorso si salda con la Retail Investment Strategy e la Savings and Investments Union nella parte in cui incentivano la partecipazione dei risparmiatori.
La seconda trasformazione riguarda le infrastrutture. Blockchain e cripto-attività promettono una democratizzazione degli scambi, ma hanno provocato una regolazione di dettaglio (MiCA, DORA, regime pilota DLT; Genius Act negli USA). Ghezzi segnala qui due tendenze: l'ibridazione tra blockchain *public* e *private* nelle "piattaforme logiche ad accesso controllato", e la contesa di sovranità tra poteri pubblici e operatori Web 3.0 sul controllo delle infrastrutture. Le proposte di Ghezzi sono coerenti con quelle generali di Occhiuzzi (quanto alle soluzioni regolatorie) e Cappai (quanto al tema centrale dell'infrastruttura) e con quelle trasversali di Saija e Perugini. Il focus regolatorio è sui nuovi rischi: *dark patterns*, gamification, costi nascosti, *alert* di scarsità, investimenti ricorrenti e promozione dello *staking*. Queste pratiche sfruttano i *bias* cognitivi e trovano terreno particolarmente fertile nel mercato cripto. Il paradigma informativo non è sufficiente e occorre intervenire sulla *choice architecture*. Di nuovo, centrale diventa il *Digital Fairness Act*. Precipitato inevitabile è una vigilanza *data-driven*, con intelligenza artificiale e sistemi di *early warning*, sempre più europea: in tal senso va la proposta di dicembre 2025 di attribuire all'ESMA la vigilanza diretta su CASP e piattaforme.

5. Il consumatore automa: IA agentica anche nei pagamenti

Armando Di Cello muove da una discontinuità: nell'economia digitale il pagamento è un atto umano riconoscibile: il consumatore sceglie, autorizza, paga; con l'AI agentica invece ricerca, confronto, selezione e acquisto confluiscono in un unico processo delegato. Si passa dal *click-to-pay* al *decide-to-pay*, e il consumatore digitale diventa consumatore agentico. Il paradigma informativo, già in crisi per la personalizzazione algoritmica – come visto negli interventi che lo precedono - diventa inefficace quando con l'agente la tecnologia non orienta la scelta, la compie.
Questa trasformazione si innesta sulla nuova architettura europea dei pagamenti, con un ecosistema ibrido a due livel-

li. Sul versante pubblico, l'euro digitale per il retail e Pontes e Appia per il regolamento *wholesale* su DLT, e sul versante privato, depositi tokenizzati e *stablecoin* in euro conformi a MiCAR. La sfida non è scegliere tra moneta pubblica e privata, ma conservare il controllo dei binari tecnologici, evitare la frammentazione e ridurre la dipendenza da circuiti extra-UE.
La tensione di fondo tra la logica probabilistica degli agenti e quella deterministica dei pagamenti deve essere sciolta sulla base del modello a tre livelli proposto dal FMI, mediante la separazione dell'interpretazione dell'intento dalla verifica e dall'esecuzione, e anche qui diventa centrale il coordinamento tra autorità, sia verticale (con le autorità europee) sia orizzontale (con quelle nazionali) e assume centralità la prospettiva infrastrutturale.

6. L'Avatar dell'assicurato

Vincenzo Orsini si occupa dell'uso dell'intelligenza artificiale da parte del consumatore che usa agenti IA capaci di agire per suo conto, e si chiede se questi possa assicurare la propria responsabilità per i danni a terzi: diffamazione, diffusione di dati personali, danneggiamento di sistemi in rete o, tramite dispositivi domestici connessi, danni fisici a persone. L'agente non si limita a produrre contenuti come un sistema conversazionale: incide direttamente sulla realtà, e questo cambia la natura stessa del rischio.
L'AI Act non impone obblighi al consumatore. Chi usa un sistema per scopi personali non professionali non è un *deployer* (artt. 3, punto 4, e 2, par. 10). I presidi *ex ante* gravano sui fornitori, che però non possono prevedere gli obiettivi assegnati da ciascun utente. I danni ai terzi restano così affidati ai rimedi *ex post* della responsabilità civile.
Il dibattito europeo ha proposto più volte un'assicurazione obbligatoria: la risoluzione del Parlamento europeo del 2017 sulla robotica, il gruppo di esperti del 2019, la risoluzione del 2020 e la proposta di direttiva del 2022, poi ritirata. Orsini osserva però che l'assicurazione della responsabilità segue l'imputazione e non può sostituirla, come mostra la RC auto, che si fonda sull'art. 2054 c.c. Anche l'interesse assicurabile (art. 1904 c.c.) esiste solo se la responsabilità del consumatore è almeno astrattamente configurabile. La domanda sull'assicurabilità diventa quindi una domanda sul criterio di imputazione.
Per rispondere, l'autore usa un caso concreto: un agente incaricato di ottenere un rimborso pubblica una recensione falsa e diffamatoria. Le cause possibili sono quattro: un difetto del sistema, un'istruzione imprudente o vaga dell'utente, una *prompt injection* di un terzo, un'iniziativa autonoma dell'agente. Su questo caso confronta due criteri: la colpa (art. 2043 c.c.): il consumatore risponde solo per istruzioni imprudenti o per scelte organizzative negligenti, come accessi troppo ampi o l'assenza di conferme prima di operazioni irreversibili. Il secondo criterio è la cosa in custodia (art. 2051 c.c.), soluzione da preferirsi per Orsini che esclude siano applicabili gli artt. 2049 e 2050. È il consumatore a decidere se attivare l'agente, con quali obiettivi e con quali accessi, ed è lui a trarne vantaggio. Ne risponde quindi anche per il difetto e per l'iniziativa autonoma, che non costituiscono caso fortuito, salvo forse l'interferenza di un terzo. Il produttore, responsabile anche per il software secondo la nuova direttiva sui prodotti difettosi, risponde in solido; il suo difetto rileva per il regresso, nel quale può surrogarsi l'assicuratore.
Il d.lgs. 160/2026 che applica l'AI Act non scioglie il nodo. Prevede una presunzione di nesso causale (art. 18), ma solo in caso di violazione dell'AI Act, e quindi non per l'uso personale. Prevede un'azione diretta contro l'assicuratore (art. 20), che però presuppone una copertura che oggi non esiste: la "RC del capofamiglia" non copre i danni digitali.
La conclusione è che serve una regola modellata sull'art. 2054 c.c.: imputare a chi impiega l'agente le conseguenze del suo funzionamento, con liberazione solo per caso fortuito o uso contro la propria volontà, e con responsabilità solidale con il produttore per i difetti, salvo regresso. La storia della RC auto indica anche l'ordine da seguire: prima la regola di imputazione (1912), poi l'obbligo assicurativo (1969). Per gli agenti IA, conclude l'autore, "siamo ancora al 1912".

7. Il consumatore soggetto e oggetto dell'ecosistema della mobilità

L'ipotesi di Federico Nespega sui trasporti è che nella mobilità del 2030 la tutela del consumatore "comincia prima del viaggio": non ci si limiterà a reagire al disservizio, ma si entrerà nella costruzione regolatoria del mercato.
Il punto di partenza è il passaggio dal passeggero al consumatore di mobilità. Il modello tradizionale ruota attorno al singolo contratto con un vettore e ai rimedi contro ritardi, cancellazioni e mancata assistenza. Oggi invece l'utente si muove in un ecosistema che integra infrastrutture fisiche e digitali, piattaforme, sistemi di pagamento e dati, come nel Mobility as a Service. Alla semplificazione tecnologica corrisponde però una complessità giuridica crescente, poiché il diritto europeo dei passeggeri è organizzato per silos verticali, per modo di trasporto, e la proposta di regolamento sui viaggi multimodali del 2023 è ancora in discussione.
Diversi provvedimenti recenti dell'ART vanno già nella direzione auspicata: le linee guida sull'affidamento del trasporto pubblico (2026); i meccanismi di premi e penalità legati alla qualità dell'infrastruttura ferroviaria (delibera

116/2025); gli indicatori di performance nei contratti di programma RFI-MIT (2026); i diritti minimi, anche risarcitori, degli utenti autostradali e il rimborso del pedaggio (delibera 211/2025). Questi provvedimenti attenuano la distinzione tra regolazione del mercato e tutela del consumatore.
Ma la mobilità digitale produce nuove asimmetrie: prezzi dinamici, ordinamento delle offerte, accesso ai dati, interoperabilità. Di nuovo, anche Nespega insiste con la necessità di un coordinamento sempre più strutturato tra autorità sul piano della concorrenza, la regolazione digitale e la protezione dei dati, e sulla neutralità dell'operatore infrastrutturale come co-regolatore.

8. Il prosumer energetico evoluto

Cristiana Lauri ci avverte che per ARERA quello del 2030 è un orizzonte regolatorio denso: è la scadenza dell'Agenda ONU e dei target europei su decarbonizzazione ed economia circolare, la data di apertura alla concorrenza della distribuzione elettrica e il traguardo intermedio della nuova Consiliatura, insediata a gennaio 2026, con il Quadro strategico 2026-2029. L'Autorità si propone di trasformare il consumatore da soggetto da proteggere a soggetto che "usa il mercato", attraverso autoconsumo, comunità energetiche e domanda flessibile. In un contesto di ibridazione tra pubblico e privato però, Lauri avverte che il legislatore non deve sopravvalutare la capacità aumentata del consumatore né rinunciare a spazi di sovranità erosi dai poteri privati. DI nuovo, si avverte lo spostamento degli oneri dal consumatore alle imprese che operano l'infrastruttura.
Lo scenario è di policrisi, lungo quattro direttrici:

- energetico-geopolitica: nel 2025 il PUN medio è stato di 115,9 €/MWh, contro 61,1 in Francia e 65,3 in Spagna, per la forte dipendenza dal gas;
- climatica: la scarsità idrica è ormai strutturale;
- sociale: i bonus sono diventati un presidio stabile;
- di governance: le competenze sono frammentate.

La risposta impone il passaggio da una logica emergenziale a una strutturale, con l'Unità di Vigilanza Energetica, il disaccoppiamento tra prezzo dell'elettricità e prezzo del gas e una sorveglianza REMIT rafforzata.
Lauri elenca le sfide principali nei diversi settori e illustra possibili soluzioni, che si basano su un monitoraggio pubblico dell'uscita dalle Tutele Graduali, indicatori comuni di consumer outcome per tutti i settori, bonus armonizzati tra i settori, criteri di equità distributiva nei prezzi zonali e nelle tariffe di rete, programmi di alfabetizzazione energetica, protocolli strutturali con le altre autorità, ACN *in primis*, garanzie di trasparenza e supervisione umana nell'uso dell'intelligenza artificiale, una valutazione dell'impatto dei data center su energia e acqua.
Il filo conduttore delle misure proposte da Lauri è che l'equità di accesso alla transizione è la forma più concreta di tutela del consumatore. Al rilievo infrastrutturale si aggiunge quindi, come già nella prospettiva di Saija, il ruolo centrale dell'ACN come *pivot* del coordinamento tra autorità.

9. Contratti sovrani

Serafina Piantedosi ipotizza che con la proposta di *Cloud and AI Development Act* (CADA), che è parte del *Tech Sovereignty Package*, la sovranità tecnologica cessi di essere una categoria politico-industriale e diventi un parametro concreto dei contratti pubblici. Il compito dei prossimi anni per l'ANAC sarà trasformarla "da principio generale a pratica amministrativa".
Il punto di partenza è che cloud, piattaforme, algoritmi e data center sono ormai infrastrutture immateriali, l' "ossatura invisibile" dei servizi pubblici, al pari di strade e reti energetiche. Il mercato è concentrato in pochi fornitori extra-UE, e questo espone le amministrazioni a rischi di interruzione, di modifiche unilaterali delle condizioni e di soggezione a normative straniere con effetto extraterritoriale. Per questo il Titolo IV del CADA ("Autonomy"), applica la nozione di sovranità digitale in modo ampio e non la limita alla protezione dei dati, ma include anche la sicurezza informatica, l'autonomia operativa, il diritto di migrare e la prevenzione di dipendenze irreversibili. Il destinatario finale di queste scelte è il cittadino-consumatore che usa servizi sanitari, fiscali o di identità digitale.
Il CADA traduce questa idea in requisiti verificabili, sulla base di un approccio risk-based, coerente con l' AI Act e il GDPR. La localizzazione del data center nell'Unione non è più sufficiente, e rilevano anche l'assetto di controllo del fornitore, la subfornitura, il diritto applicabile e le condizioni di uscita. Le ricadute sugli affidamenti sono: la 'valutazione di sovranità' che entra nell'istruttoria e nel capitolato; l'inserimento di clausole su restituzione dei dati in formato aperto, migrazione, costi di uscita e continuità del servizio; l'inserimento tra i criteri di aggiudicazione del "valore aggiunto europeo" proporzionato e subordinato a qualità e prezzo, e infine acquisti comuni gestiti dalla Commissione e la EuroCloud Federation (art. 34) per la cooperazione infrastrutturale pubblica.

Anche quanto al ruolo di ANAC, Piantedosi fa proposte concrete: una vigilanza collaborativa sugli affidamenti ad alta criticità, per verificare la qualità dell'istruttoria, il livello di assurance e la proporzionalità dei requisiti; linee guida e clausole tipo, utili soprattutto alle stazioni appaltanti più piccole; il monitoraggio, tramite la BDNCP, di rinnovi ripetuti e concentrazioni di contratti come indicatori di lock-in; protocolli con AgID, ACN, Garante privacy e AGCM. Di nuovo, la soluzione appare il coordinamento a due versanti: tra autorità e tra autorità e mercato-infrastruttura.

10. Cittadinanza digitale intermediata dall'infrastruttura privata

Francesca Pellicanò e Rosaria Petti convengono che nei settori vigilati da AGCom il paradigma del "consumatore informato" non sia più adeguato in un contesto in cui le asimmetrie riguardano l'architettura degli ambienti digitali in cui si formano le scelte. Occorre garantire al consumatore un' effettiva capacità di scelta, controllo e reversibilità delle proprie decisioni.

Nei settori 'media e audiovisivo' Pellicanò evidenzia che il consumo passa dal palinsesto all'accesso permanente, personalizzato e mediato dagli algoritmi. La risorsa scarsa non sono più i contenuti ma l'attenzione del consumatore: la ottiene chi rende visibile un contenuto, con sistemi di raccomandazione più efficaci. A questo si aggiungono da un lato l'intelligenza artificiale come infrastruttura dell'intero ciclo produttivo, che crea dubbi sull'autenticità dei contenuti, e dall'altro una crescente concentrazione dell'intermediazione. Il consumatore "è più libero nella scelta dei contenuti, meno nella scelta dell'infrastruttura". Il nodo, ormai è chiaro, è infrastrutturale.

In questo scenario Pellicanò individua sei aree critiche: trasparenza algoritmica comprensibile e pluralismo (EMFA); tutela dei minori con un'*age assurance* rispettosa della privacy, sul modello della verifica tramite terzo indipendente (delibera 96/25); pubblicità che si confonde con i contenuti; influencer (codice di condotta del 2025) e testimonial sintetici; economia degli abbonamenti, rinnovi e *dark patterns*, da affrontare con un approccio di *fairness by design*, disinformazione amplificata dall'intelligenza artificiale generativa, accessibilità come elemento strutturale della qualità. Sul piano strategico, Pellicanò propone una regolazione prospettica lungo l'intero ciclo della relazione digitale, un coordinamento tra le autorità, il rafforzamento della capacità di *algorithmic auditing* (anche nel ruolo di AGCom come *Digital Services Coordinator*), la garanzia di una trasparenza contestuale, la *media literacy* e *prominence* delle opere europee. In sintesi, la tutela deve spostarsi dal contenuto all'ecosistema. DI nuovo, il coordinamento a due versanti è al centro.

Sulle comunicazioni elettroniche, Petti conferma che la connettività è un'infrastruttura essenziale per la cittadinanza digitale e a questo fine individua alcune priorità: passare dalla qualità dichiarata alla qualità percepita: stabilità, latenza, resilienza, assistenza; far conoscere il costo totale lungo l'intero contratto, contro l'"asimmetria temporale" creata da promozioni e *bundle*; garantire uno *switching* effettivo contro il *lock-in* da convergenza (nel 2026 AGCOM ha avviato un tavolo tecnico sulle procedure di passaggio); vigilare sulla personalizzazione economica dei prezzi; garantire un'assistenza con operatore umano obbligatorio (delibera 255/24); assicurare l'accessibilità economica della connettività di qualità.

Petti propone poi un *Consumer Connectivity Index* basato su qualità effettiva, affidabilità, facilità di *switching*, trasparenza del costo complessivo e accessibilità economica. Per AGCOM Petti indica cinque direttrici: una conoscenza sistematica degli effetti degli algoritmi; la misurazione della contendibilità dei mercati; indicatori della qualità effettivamente sperimentata; l'individuazione delle vulnerabilità situazionali; una funzione di anticipazione basata su ricerca e monitoraggio.

Per Petti, l'obiettivo 2030 deve essere quello di un consumatore "assistito ma non sostituito, personalizzato ma non manipolato, connesso ma non escluso", che resti titolare delle proprie decisioni.

11. Sicurezza, parametro della sovranità

Michela Mastrantonio infine ci ricorda che in pochi anni ACN ha ottenuto tre leve che incidono sulla sicurezza dei prodotti di consumo: la certificazione, la vigilanza sui sistemi di intelligenza artificiale e la sorveglianza del mercato sui prodotti connessi prevista dal regolamento sulla cyber-resilienza. Sommate, queste competenze trasformano il bene di consumo in un oggetto di sicurezza nazionale, potenziale superficie di attacco del Paese. ACN dunque al centro del concerto regolatorio a due versanti. Le politiche europee però non ne prendono atto e restano separate: l'Agenda consumatori 2030 e il pacchetto cybersicurezza del gennaio 2026 non interagiscono tra loro.

Non c'è tempo: il 2030 è il punto in cui convergono scadenze già fissate: il portafoglio europeo di identità digitale (2026-2027), il regolamento sulla ciberresilienza (2027), i sistemi di intelligenza artificiale ad alto rischio (2027-2028) e la crittografia post-quantistica. Su questa base Mastrantonio individua cinque rischi relativi all'identità digitale, agli agenti IA, alla casa connessa, all'ingegneria sociale, alla tecnologia post-quantum.

Il limite strutturale (di nuovo, l'infrastruttura è il *bottleneck*) risiede attualmente nel fatto che l'ACN conosce soltanto ciò che i soggetti obbligati le notificano, e misura gli incidenti in base all'interruzione dei servizi. Una violazione che espone milioni di persone a frodi successive resta quindi fuori dal suo campo di osservazione, e quindi l'esposizione della popolazione non è solo sottostimata, è del tutto assente. In questo modo l'Agenzia può reagire, ma non anticipare.
Mastrantonio propone alcune soluzioni specifiche su un duplice piano. Il primo concerne i poteri dell'ACN: usare i dati già in possesso dello CSIRT (*phishing*, credenziali esposte) come misura dell'esposizione della popolazione; introdurre soglie di notifica legate al numero di persone esposte; chiedere agli operatori di telecomunicazioni l'inventario dei *router* dati in comodato, con modelli, versioni e date di fine supporto, applicando al territorio la logica della SBOM; usare l'intelligenza artificiale per selezionare i prodotti da sottoporre a prova di laboratorio.
Il secondo piano concerne interventi prescrittivi: per gli agenti AI, presidi esterni al modello: credenziali limitate al singolo compito, elenchi chiusi di strumenti, limiti di importo, conferma umana per le operazioni irreversibili, SBOM estesa all'intelligenza artificiale; per l'identità digitale, validità del portafoglio solo su sistemi operativi ancora supportati; per il post-quantum, priorità basate sulla durata della riservatezza necessaria.
Il tema che Mastrantonio rileva, più in generale, è che le autorità intervengono sulla base di un'osservazione settoriale; manca la visione d'insieme, che dovrebbe essere del legislatore (europeo) e che, in assenza, può realizzarsi con una collaborazione strutturata tra le autorità di vigilanza.

12. Brevi 'conclusioni introduttive': il 'concerto regolatorio a due versanti' come strumento finale

Il 'concerto regolatorio a due versanti', tra autorità indipendenti (verticale: tra autorità nazionali ed europee, e orizzontale: tra autorità nazionali, generali e settoriali) e tra autorità e mercato (inteso come infrastrutture, pubbliche e private) sembra essere in tutte le analisi che abbiamo sintetizzato lo strumento necessario e idoneo – sul piano sia della formazione delle norme, di *hard* e di *soft law*, sia dell'esecuzione, sia infine dell'*enforcement* - per affrontare l'evoluzione delle piattaforme tecnologiche, digitali e ora di IA.
Questa soluzione mette in valore gli strumenti ermeneutici elaborati nei rapporti Consumerism nel corso degli anni e di fatto rende coerente il percorso e lo conclude. Alla base vi sono infatti il circolo regolatorio e la regolazione partecipata.
Il primo, vede le norme nascere dal mercato come *best practices*, che le autorità propongono come *benchmark* e impongono poi come *standards*, che tornano al mercato (come strumenti di *soft-hard law*) oppure, quando necessario, vengono inseriti in atti esecutivi (della Commissione UE) o normativi (regolamenti, direttive) e comunque tornano al mercato, completando il circolo. Il circolo consente di superare l'asimmetria informativa e la cattura regolatoria.
La regolazione partecipata è lo strumento principale per realizzare il circolo regolatorio: le autorità non si limitano a pubblicare un documento per la consultazione e poi a prendere più o meno atto dei rilievi del mercato, come negli standard classici della co-regolazione, ma partecipano con il mercato – ora, con le infrastrutture – alla costruzione di strumenti che siano *by design* coerenti con il welfare europeo continentale.
Il concerto regolatorio a doppio versante da un lato (versante autorità) rende il circolo regolatorio omogeneo e coerente, interrompendo la rincorsa settoriale dei silos verticali e orizzontali, e dall'altro lato (versante mercato-infrastruttura) consente una regolazione partecipata consapevole. Quest'ultimo passaggio impone peraltro un ripensamento, sul piano concettuale, del paradigma della neutralità regolatoria, perché la spinta del mercato viene canalizzata verso un obiettivo consumeristico (come in parte è già per la concorrenza) e di *welfare*. È questo del resto lo spirito del tempo, come emerge in modo non più implicito dal mercato: il *paper* di Amodei "*Pace the frontier*" è un segnale di allarme che, al netto degli equivoci che può generare, manifesta un'esigenza reale: condividere con i regolatori, non solo con il mercato, lo sviluppo dei modelli di IA.

AUTORITÀ E CONSUMATORI 2030: DALLA FRAMMENTAZIONE DELLE REGOLE ALLA TRASVERSALITÀ DELLA TUTELA

(di Paolo Occhiuzzi)[1]

SOMMARIO: 1. DAL CONSUMATORE "CONTRAENTE DEBOLE" AL CONSUMATORE NEL MERCATO. 2. DALLA MODERNIZZAZIONE DELL'ACQUIS AL NUOVO ORDINE REGOLATORIO EUROPEO. 3. IL CONSUMATORE DIGITALE VERSO IL 2030: DALLA TRASPARENZA ALLA FAIRNESS. 4. LA TRANSIZIONE SOSTENIBILE: UN SECONDO BANCO DI PROVA. 5. DALLA FRAMMENTAZIONE REGOLATORIA ALLA COERENZA DEL SISTEMA: REGOLE TRASVERSALI E COORDINAMENTO TRA AUTORITÀ. 6. AUTORITÀ E CONSUMATORI 2030: DALLA CROSS-REGULATION ALLA CROSS-ENFORCEMENT?

1. Dal consumatore "contraente debole" al consumatore nel mercato

Interrogarsi sulla posizione che il consumatore occuperà nel 2030 richiede, anzitutto, di volgere lo sguardo al percorso compiuto dal diritto dei consumi. Poche discipline, infatti, mostrano con altrettanta evidenza la propria dipendenza dalle trasformazioni economiche, tecnologiche e sociali. Il diritto dei consumatori è, per sua natura, *law in a changing society*[2]: nasce e si sviluppa come risposta ai mutamenti del mercato e, proprio per questo, il suo perimetro non può essere definito una volta per tutte.

La sua origine moderna è tradizionalmente ricondotta alla necessità di proteggere il consumatore quale parte debole di una relazione economica caratterizzata da una strutturale asimmetria rispetto al professionista[3]. La prima stagione del diritto consumeristico è quindi essenzialmente una storia di protezione: alla libertà formale del contratto si affiancano regole imperative destinate a correggere gli squilibri informativi, economici e negoziali che possono condizionare l'autodeterminazione del consumatore.

Il percorso europeo riflette chiaramente questa impostazione. Dal riconoscimento dei primi diritti fondamentali del consumatore negli anni Settanta si passa, tra gli anni Ottanta e Novanta, alla progressiva costruzione di un vero *acquis* consumeristico europeo, prevalentemente attraverso direttive dedicate a specifici rapporti contrattuali. La direttiva 93/13/CEE sulle clausole abusive rappresenta uno dei momenti più significativi di tale evoluzione: l'intervento legislativo non è più indifferente alla qualità delle parti, ma muove precisamente dalla diversa posizione sostanziale di professionista e consumatore[4].

Una seconda trasformazione si realizza quando l'attenzione si sposta progressivamente "dall'atto all'attività". La protezione non riguarda più soltanto il contenuto del contratto o il momento della sua conclusione, ma il comportamento complessivo del professionista sul mercato. La direttiva 2005/29/CE sulle pratiche commerciali sleali costituisce, sotto questo profilo, un passaggio decisivo: oggetto della disciplina diventa l'intera attività commerciale suscettibile di incidere sulla libertà di scelta del consumatore prima, durante e dopo l'operazione economica.

È in questo passaggio che può cogliersi una trasformazione più profonda. Come evidenziato da Maddalena Rabitti, il diritto dei consumi tende progressivamente a oltrepassare la sola dimensione della tutela del contraente debole per assumere una funzione di regolazione del mercato. La protezione del consumatore non opera più soltanto *nel* rapporto con il professionista, ma concorre a definire le condizioni di corretto funzionamento del mercato stesso. Il consumatore, in questa prospettiva, non è soltanto destinatario di diritti individuali: diviene portatore di interessi che assumono una dimensione collettiva e la cui tutela contribuisce alla costruzione della fiducia nei mercati.

Anche la progressiva centralità del *public enforcement* si comprende in questa chiave. Se l'obiettivo fosse esclusivamente quello di riequilibrare un singolo rapporto contrattuale, il rimedio civilistico potrebbe costituire lo strumento naturale di tutela. Quando invece l'interesse protetto investe la correttezza dei comportamenti dell'impresa sul mer-

1. 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.
2. Così M. Rabitti, Il diritto dei consumatori, in AA.VV., Diritto ed economia del mercato, G. Lemme (a cura di), Milano, 2025, p. 376 che, riprendendo l'espressione utilizzata da Wolfgang Friedmann nel titolo della sua nota opera sul diritto quale fattore e, al contempo, prodotto del cambiamento sociale (W. Friedmann, Law in a Changing Society, 2nd ed., London, 1972, spec. pp. 132-135), definisce efficacemente il diritto dei consumatori come, «per eccellenza, Law in a Changing Society»: un diritto che «insegue il cambiamento e si adatta, di volta in volta, al nuovo contesto cercando di bilanciare gli interessi in gioco in una logica funzionale al migliore equilibrio del mercato.
3. L. ROSSI CARLEO, Art. 1, in Codice del Consumo. Commentario, a cura di G. Alpa – L. Rossi Carleo, Napoli, 2005, p. 1.
4. G. DE CRISTOFORO, 40 anni di diritto europeo dei contratti dei consumato-ri: linee evolutive e prospettive future, in Contratti, 2019, p. 176 ss.

cato e la libertà di scelta di una pluralità indeterminata di consumatori, diventa essenziale l'intervento delle Autorità amministrative indipendenti[5].
Il Codice del consumo del 2005 rappresenta, da questo punto di vista, insieme un punto di arrivo e l'inizio di una nuova fase[6]. Esso tenta di ricondurre ad unità una materia già complessa, ma la successiva evoluzione normativa dimostra progressivamente quanto sia difficile racchiudere il diritto dei consumatori entro i confini di un unico *corpus* normativo[7]. Il consumatore è contemporaneamente utente di servizi digitali, cliente bancario, assicurato, passeggero, utente dei servizi energetici e delle comunicazioni, acquirente di beni e servizi. All'unità della persona corrisponde così una crescente frammentazione delle discipline.
Questa evoluzione pone già una prima questione nella prospettiva del 2030. La specializzazione della tutela ha consentito di adattare le regole alle caratteristiche dei diversi mercati, ma ha progressivamente moltiplicato discipline, autorità e strumenti di intervento.
In questa prospettiva, la principale sfida non sembra risiedere tanto nell'ulteriore ampliamento del catalogo dei diritti sostanziali riconosciuti alla persona nel mercato, quanto nella capacità di ricondurre a coerenza discipline, autorità e modelli di *enforcement* sempre più differenziati. Se il diritto dei consumatori del Novecento è stato prevalentemente un diritto di progressiva espansione delle tutele, quello del prossimo decennio sembra destinato a divenire, anzitutto, un diritto di «*integrazione regolatoria*».

2. Dalla modernizzazione dell'acquis al nuovo ordine regolatorio europeo

La direttiva (UE) 2019/2161, c.d. direttiva Omnibus, costituisce probabilmente l'ultimo grande intervento nel quale l'Unione europea ha perseguito l'adeguamento del tradizionale *acquis* consumeristico intervenendo prevalentemente sulle sue strutture consolidate. Essa modifica contestualmente la disciplina delle clausole abusive, dell'indicazione dei prezzi, delle pratiche commerciali sleali e dei diritti dei consumatori, rafforzandone l'enforcement e adattandone alcuni istituti alle trasformazioni del mercato digitale[8].
Ma proprio negli stessi anni emerge un fenomeno differente. Il diritto dell'Unione non si limita più ad aggiornare il diritto dei consumatori per adeguarlo alla dimensione digitale: costruisce una nuova regolazione del mercato digitale all'interno della quale la tutela del consumatore costituisce uno degli interessi protetti.
Il Digital Services Act[9] e il Digital Markets Act[10] sono emblematici di questa trasformazione. Il primo interviene sulla responsabilità e sugli obblighi degli intermediari digitali e delle piattaforme; il secondo introduce una disciplina *ex ante* per i *gatekeepers*.
Ad essi si sono progressivamente affiancati il Data Act (Reg. (UE) 2023/2854) e, soprattutto, l'Artificial Intelligence Act (Reg. (UE) 2024/1689). Si forma così un articolato *digital rulebook* europeo nel quale concorrenza, protezione dei dati, tutela dei consumatori, regolazione delle piattaforme, disciplina dei dati, sicurezza dei prodotti e tutela dei diritti fondamentali tendono sempre più frequentemente a intersecarsi[11].
Non si tratta soltanto di una crescita quantitativa delle regole. Cambia la tecnica regolatoria.
La disciplina consumeristica tradizionale opera prevalentemente attraverso un controllo *ex post* e una valutazione *case-by-case* della condotta del professionista e dei suoi effetti sulla libertà di scelta del consumatore. Una parte significativa della nuova regolazione digitale introduce invece strumenti di carattere preventivo, incidendo sui processi attraverso i quali prodotti e servizi sono progettati e offerti: valutazione dei rischi, obblighi di *due diligence*, audit, valutazioni di conformità, obblighi relativi alla progettazione delle interfacce e dei sistemi.
L'intervento si sposta, in altri termini, dal solo controllo del comportamento alla regolazione dell'architettura entro la quale il comportamento economico si realizza[12].

5. Cfr. L. ROSSI CARLEO, L'Autorità "garante" del consumatore e della concorrenza tra regolazione e decisione, in Conc. merc., 2013, 846 ss.
6. Così G. DE CRISTOFARO, Il «Codice del consumo», in Le nuove leggi civili commentate, 2006, fasc. 5, che dedica specificamente attenzione alle «discipline confluite nel d.lg. 206/2005 e quelle rimaste ad esso estranee» e all'«impostazione sistematica e [alla] struttura del codice del consumo», individuando già ab origine quelli che sono i limiti strutturali del corpus normativo.
7. M. Rabitti, Il consumatore vulnerabile e la fragilità del diritto. Brevi considerazioni, in Dialoghi di Diritto dell'Economia, 2023.
8. Cfr. G. DE CRISTOFARO, *Diritto italiano ed europeo dei consumatori. Cinque anni di evoluzioni normative e giurisprudenziali (2017-2021)*, Milano, 2022, 97 ss., spec. 97-102; ID., *Rimedi privatistici "individuali" dei consumatori e pratiche commerciali scorrette: l'art. 11-bis dir. 2005/29/UE e la perdurante (e aggravata) frammentazione dei diritti nazionali dei Paesi UE*, in *Jus Civile*, 2022, n. 2.
9. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali – Digital Services Act); sul rapporto tra la nuova disciplina delle piattaforme e la tutela dei consumatori, v. G. FINOCCHIARO, Responsabilità delle piattaforme e tutela dei consumatori, in Giorn. dir. amm., 2023, n. 6, 730-736.
10. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Digital Markets Act – DMA). Cfr. M. CAPPAI – G. COLANGELO, Taming Digital Gatekeepers: The "More Regulatory Approach" to Antitrust Law, in Computer Law & Security Review, vol. 41, 2021.
11. Cfr. Commissione europea, Commission Staff Working Document – Fitness Check of EU Consumer Law on Digital Fairness, SWD(2024) 230 final, Bruxelles, 3 ottobre 2024, spec. la parte relativa alla external coherence dell'EU consumer law acquis con il più ampio quadro normativo europeo in materia digitale.
12. M. Brenncke, A Theory of Exploitation for Consumer Law: Online Choice Architectures, Dark Patterns, and Autonomy Violations, in Journal of Consumer Policy, 2024.

È un cambiamento particolarmente evidente nel rapporto tra consumatore e tecnologia. L'obiettivo non è più soltanto assicurare che la decisione commerciale non sia stata determinata da informazioni false o omesse, ma preservare le condizioni nelle quali quella decisione possa essere effettivamente libera quando l'ambiente digitale nel quale viene assunta è progettato e personalizzato dal professionista.
Questa evoluzione assume particolare rilievo con l'intelligenza artificiale. Il consumatore non si confronta più soltanto con un professionista meglio informato, ma con organizzazioni capaci di conoscere, prevedere e, almeno potenzialmente, orientare il suo comportamento attraverso enormi quantità di dati. La tradizionale asimmetria informativa si trasforma progressivamente in una "asimmetria informativa, tecnologica e predittiva".
Ne consegue che anche il paradigma del consumatore medio, normalmente informato e ragionevolmente attento e avveduto, deve essere confrontato con mercati nei quali l'ambiente decisionale può essere individualmente configurato sulla base delle caratteristiche, delle preferenze e delle vulnerabilità del singolo destinatario.
Il nuovo *digital rulebook* non determina tuttavia il superamento del diritto dei consumatori. DSA, DMA, Data Act e AI Act perseguono finalità specifiche, si rivolgono a determinate categorie di operatori, servizi o tecnologie e presentano ambiti applicativi differenti. Non tutte le applicazioni dell'intelligenza artificiale rivolte ai consumatori, ad esempio, rientrano nelle categorie maggiormente regolamentate dall'AI Act; allo stesso modo, le discipline dedicate alle piattaforme non comprendono la totalità delle attività commerciali che si svolgono online.
Proprio per questo il diritto consumeristico orizzontale conserva una funzione essenziale di *baseline di tutela*: una rete di protezione destinata a operare anche negli spazi non coperti specificatamente dalle discipline speciali.
Si determina così un fenomeno apparentemente paradossale. Quanto più il diritto europeo si specializza per governare singole tecnologie, servizi o categorie di operatori, tanto più diventa importante preservare un nucleo orizzontale di principi consumeristici capace di attraversare i diversi mercati e di colmare gli interstizi lasciati dalle discipline speciali.

3. Il consumatore digitale verso il 2030: dalla trasparenza alla fairness

È soprattutto nell'ambiente digitale che questa esigenza emerge con maggiore evidenza.
Il *Fitness Check* della Commissione europea sulla *digital fairness* ha confermato la perdurante rilevanza delle direttive orizzontali in materia di pratiche commerciali scorrette, diritti dei consumatori e clausole abusive, evidenziando tuttavia come esse riescano solo parzialmente ad assicurare un livello elevato di protezione rispetto alle caratteristiche assunte dai mercati digitali[13].
Il quadro normativo esistente continua, dunque, a rappresentare la base della tutela consumeristica, ma incontra crescenti difficoltà rispetto a pratiche e modelli di business che sfruttano le caratteristiche proprie dell'ambiente digitale.
È in questo contesto che si colloca l'iniziativa della Commissione europea per un *Digital Fairness Act*. Essa muove proprio dai risultati del *Fitness Check* e dalla necessità di rafforzare la tutela rispetto a fenomeni quali i *dark patterns*, il design suscettibile di favorire forme di utilizzo compulsivo, determinate pratiche di personalizzazione, l'*influencer marketing* e, più in generale, le tecniche digitali capaci di incidere sulla libertà della decisione economica.
Il percorso verso il *Digital Fairness Act* appare, sotto questo profilo, particolarmente significativo: la questione non è soltanto quella di aggiungere nuovi obblighi al tradizionale acquis consumeristico, ma di verificare se categorie e strumenti elaborati per mercati nei quali la pratica commerciale poteva essere distinta dall'ambiente nel quale la scelta veniva compiuta siano ancora sufficienti quando è la stessa architettura digitale a concorrere alla formazione della decisione.
Il problema non sembra derivare, infatti, soltanto dall'emersione di nuove pratiche commerciali, quanto dalla progressiva trasformazione dell'ambiente nel quale si forma la decisione di consumo. Le tecniche di persuasione proprie dei mercati digitali possono operare non soltanto attraverso il contenuto del messaggio commerciale, ma anche mediante la configurazione dell'interfaccia, l'ordine e la reiterazione delle informazioni, i sistemi di raccomandazione, la personalizzazione delle offerte e, più in generale, l'architettura entro la quale il consumatore è chiamato a scegliere.
Ne deriva una progressiva insufficienza di un modello di tutela prevalentemente imperniato sulla trasparenza e sull'informazione. L'informazione continua naturalmente a rappresentare un presupposto essenziale dell'autodeterminazione del consumatore, ma non è necessariamente in grado di neutralizzare gli effetti di un ambiente decisionale progettato per orientarne il comportamento. Informare il consumatore non equivale, in altri termini, necessariamente a renderlo libero. È in questo passaggio che la *fairness* tende ad assumere un significato più ampio: non riguarda soltanto

13. Cfr. Commissione europea, Commission Staff Working Document – Fitness Check of EU Consumer Law on Digital Fairness, SWD(2024) 230 final, Bruxelles, 3 ottobre 2024, spec. parr. 4-5 e 8, ove, pur confermandosi la persistente rilevanza e necessità della direttiva 2005/29/CE sulle pratiche commerciali sleali, della direttiva 2011/83/UE sui diritti dei consumatori e della direttiva 93/13/CEE sulle clausole abusive, se ne evidenzia una efficacia soltanto limitata rispetto alle specifiche criticità dell'ambiente digitale.

la correttezza delle informazioni fornite, ma investe le condizioni nelle quali la decisione viene concretamente assunta. Questa evoluzione può essere osservata, in particolare, lungo due direttrici tra loro strettamente connesse.

La prima attiene alle tecniche attraverso le quali l'architettura digitale può incidere sulla formazione della volontà del consumatore. *Dark patterns*, *addictive design*, sistemi di raccomandazione, personalizzazione delle offerte e tecniche di *nudging* mostrano come il problema della correttezza della pratica commerciale non possa più essere valutato considerando esclusivamente il contenuto dell'informazione trasmessa o il singolo atto negoziale. Ciò che assume rilievo è anche il modo in cui l'ambiente digitale seleziona, organizza e presenta le alternative, rendendo alcune decisioni più semplici, immediate o attraenti e altre più difficili o onerose.

Sotto il profilo dell'enforcement, i *dark patterns* costituiscono, un caso paradigmatico. La medesima realtà fenomenica è oggi intercettata, secondo presupposti, ambiti applicativi e categorie non sempre coincidenti, dalla disciplina delle pratiche commerciali scorrette e dalle più recenti normative europee relative ai mercati e ai servizi digitali, ai dati e all'intelligenza artificiale[14].

Il *Fitness Check* ha evidenziato proprio come la proliferazione della legislazione digitale abbia accresciuto la complessità regolatoria, determinando aree di sovrapposizione e possibili divergenze interpretative rispetto a pratiche sostanzialmente analoghe[15].

Una seconda direttrice riguarda, invece, il soggetto destinatario della tutela. La capacità degli operatori di personalizzare l'ambiente nel quale si forma la decisione economica impone infatti di interrogarsi sulla perdurante adeguatezza di un modello costruito prevalentemente intorno alla figura astratta del consumatore medio[16].

Se il professionista è in grado di differenziare messaggi, offerte, interfacce e sollecitazioni sulla base delle caratteristiche del singolo destinatario, anche la vulnerabilità – come già osservato in dottrina[17] - assume una dimensione nuova. Essa non costituisce soltanto una condizione stabile, riferibile a categorie predeterminate di soggetti, ma può presentarsi in forma dinamica e situazionale, in relazione all'età, alle competenze, alle condizioni personali e alle concrete caratteristiche dell'ambiente nel quale la scelta viene compiuta.

Il caso dei consumatori più giovani è, da questo punto di vista, particolarmente significativo. I minori operano nei medesimi mercati digitali degli adulti e sono esposti a tecniche commerciali analoghe, ma vi si confrontano in una fase nella quale le capacità decisionali e la stessa *commercial literacy* sono ancora in formazione. Personalizzazione, *influencer marketing*, valute virtuali, sistemi di raccomandazione, tecniche di *AI-enhanced nudging* e meccanismi volti a prolungare il coinvolgimento dell'utente possono pertanto incidere con particolare intensità sulla loro autonomia decisionale[18].

La tutela dei minori consente così di cogliere un ulteriore sviluppo del paradigma consumeristico. La disciplina europea delle pratiche commerciali scorrette già riconosce la necessità di valutare diversamente le pratiche rivolte a gruppi di consumatori particolarmente vulnerabili e vieta, in particolare, le esortazioni dirette ai bambini affinché acquistino prodotti o inducano gli adulti ad acquistarli. Le più recenti iniziative europee sulla protezione dei minori online sembrano tuttavia spingersi oltre tale impostazione, intervenendo non soltanto sulla singola pratica commerciale, ma sulla stessa progettazione e sul funzionamento del servizio.

È particolarmente indicativa, in questa prospettiva, la proposta di *EU KIDS Act*[19]. Il modello delineato dalla proposta muove dalle specifiche vulnerabilità e dalle capacità evolutive dei minori e affianca agli strumenti tradizionali di tutela obblighi di *safety by design*, configurazioni protettive per impostazione predefinita e specifiche garanzie rispetto ai sistemi di raccomandazione, alle transazioni economiche e alle funzionalità suscettibili di determinare forme di utilizzo compulsivo o spese eccessive, impulsive o indesiderate. Particolarmente significativa è, in tale contesto, l'esigenza che la progettazione del servizio non sfrutti la *commercial literacy* ancora in formazione del minore. La responsabilità della tutela tende così a spostarsi, almeno in parte, dalla capacità del consumatore vulnerabile di riconoscere e contrastare il

14. Cfr. ancora Commissione europea, *Commission Staff Working Document – Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final, cit., spec. pp. 70 ss. e 147 ss. Il documento individua proprio nella disciplina dei *dark patterns* uno dei principali problemi di coerenza tra UCPD e diversi strumenti del *digital rulebook*, tra cui DSA, DMA, Data Act e AI Act, rilevando che «the deployment of dark patterns could breach multiple laws at the same time».

15. Sul problema della sovrapposizione tra discipline e competenze nei mercati digitali e sulla possibilità che più autorità intervengano sulla medesima vicenda sulla base di differenti titoli regolatori, v. M. CAPPAI – P. OCCHIUZZI, *Il dovere di leale collaborazione istituzionale nei rapporti tra autorità indipendenti e agenzie: dal coordinamento occasionale alla strutturale interdipendenza*, in F. BASSAN (a cura di), *Piattaforme digitali e consumatori*, Roma, RomaTrE-Press, 2026. I dark patterns ne costituiscono un primo esempio: la medesima tecnica può assumere rilievo alla luce della disciplina delle pratiche commerciali scorrette, del DSA e, a seconda delle caratteristiche della fattispecie, delle ulteriori discipline europee relative ai mercati digitali, ai dati e all'intelligenza artificiale.

16. M. Rabitti - F. Bassan, *Il consumatore e le nuove vulnerabilità*, introduzione al rapporto *Il consumatore vulnerabile tra innovazione e diritti fondamentali – Consumerism 2022*, dicembre 2022, pp. 6 ss.

17. Cfr. M. Rabitti, *Il consumatore vulnerabile e la fragilità del diritto. Brevi considerazioni*, in *Dialoghi di Diritto dell'Economia*, settembre 2023, spec. parr. 2 e 4, la quale, nel ricostruire il progressivo superamento della concezione statica del consumatore vulnerabile, evidenzia come la vulnerabilità debba essere considerata secondo una prospettiva situazionale e funzionale e possa dipendere da una pluralità di fattori, anche transitori e cumulabili.

18. Commissione europea, An EU approach to online child safety, COM(2026) 680 final, 17 settembre 2026.

19. Commissione europea, *Proposal for a Regulation of the European Parliament and of the Council – EU KIDS ACT – "EU Keeping Internet Digital Spaces Accountable and Trustworthy"*, COM(2026) 681 final, 17 settembre 2026, 2026/0286 (COD).

condizionamento alla responsabilità del professionista nella predisposizione dell'ambiente nel quale la decisione viene assunta.
Il dato sistematico appare più importante delle singole soluzioni normative. Se l'architettura digitale è in grado di incidere sull'autonomia del consumatore, la vulnerabilità del destinatario non può essere affrontata soltanto mediante un incremento degli obblighi informativi. Alla tutela successiva rispetto alla pratica si affianca una dimensione preventiva, che tende a incorporare la protezione del consumatore nella stessa progettazione del servizio[20].
Proprio la crescente trasversalità dei fenomeni regolati conferma, peraltro, la persistente centralità del diritto orizzontale dei consumatori. Quanto più l'esperienza economica del consumatore è interessata contemporaneamente da discipline diverse, tanto più emerge l'esigenza di una disciplina capace di assicurare una *baseline* di tutela e di offrire un punto di riferimento comune rispetto a fenomeni che attraversano differenti settori regolatori. La specializzazione delle regole e la trasversalità della tutela non rappresentano, pertanto, tendenze necessariamente contrapposte: è piuttosto dalla loro capacità di integrarsi che dipende la coerenza complessiva del sistema.
In questa prospettiva deve essere letta anche l'iniziativa sul *Digital Fairness Act*. La sua rilevanza non risiede soltanto nell'eventuale introduzione di nuove regole destinate a colmare le lacune emerse nell'ambiente digitale, ma anche nella necessità di chiarire il rapporto tra l'acquis consumeristico e un *digital rulebook* ormai composto da una pluralità di discipline speciali.
La risposta alle nuove criticità non può infatti consistere nella mera stratificazione di ulteriori obblighi: una regolazione efficace deve assicurare un elevato livello di tutela, ma anche rendere prevedibili le regole, chiarirne i rapporti reciproci ed evitare sovrapposizioni che non producano un corrispondente incremento della protezione.
La questione del consumatore 2030 diviene così, anzitutto, una questione di coerenza regolatoria: non soltanto quali regole siano necessarie, ma come discipline elaborate per finalità differenti possano concorrere alla protezione della medesima persona e della medesima decisione economica senza generare lacune, sovrapposizioni o incoerenze.
Accanto alla regolazione e all'*enforcement* rimane, infine, una terza dimensione. Quanto più sofisticate diventano le tecniche di influenza digitale, tanto più la tutela deve comprendere anche l'*empowerment* del consumatore. Alfabetizzazione digitale, capacità di riconoscere le tecniche persuasive e consapevolezza dei propri diritti non possono sostituire la regolazione delle condotte scorrette né trasferire sul consumatore la responsabilità di neutralizzare pratiche o ambienti decisionali suscettibili di comprometterne l'autonomia; ne rappresentano, tuttavia, un necessario complemento.
Anche sotto questo profilo il percorso storico del diritto dei consumatori sembra quindi proseguire: dalla protezione del contraente debole alla promozione di un consumatore attivo e, oggi, alla costruzione delle condizioni - regolatorie, tecnologiche e cognitive - che gli consentano di esercitare effettivamente la propria autodeterminazione in ambienti digitali sempre più complessi.

4. La transizione sostenibile: un secondo banco di prova

La trasformazione digitale non rappresenta l'unica direttrice lungo la quale si sta modificando il diritto dei consumatori. Una dinamica analoga si registra rispetto alla transizione ambientale.
Anche in questo caso, alla tradizionale tutela degli interessi economici del consumatore si affianca progressivamente una diversa dimensione funzionale della disciplina. Le decisioni di consumo sono chiamate a concorrere alla trasformazione dei modelli produttivi e alla transizione verso un'economia più sostenibile e circolare. Il consumatore diviene così, al tempo stesso, destinatario della protezione e attore della transizione[21].
La direttiva (UE) 2024/825 sull'*empowering consumers for the green transition*[22] rappresenta un passaggio particolar-

20. Commissione europea, *Proposal for a Regulation of the European Parliament and of the Council – EU KIDS ACT – "EU Keeping Internet Digital Spaces Accountable and Trustworthy"*, COM(2026) 681 final, 17 settembre 2026, 2026/0286 (COD). La tutela dei minori rappresenta, in questo senso, un laboratorio particolarmente avanzato di una trasformazione che potrebbe assumere rilievo più generale nel diritto dei consumatori: quanto maggiore è la capacità del professionista di conoscere e utilizzare le vulnerabilità del destinatario, tanto meno la protezione può essere affidata esclusivamente alla capacità di quest'ultimo di riconoscere e neutralizzare il condizionamento.

21. Cfr. Commissione europea, *Un nuovo piano d'azione per l'economia circolare. Per un'Europa più pulita e più competitiva*, COM(2020) 98 final, 11 marzo 2020, spec. par. 2.2 e Allegato, ove, nell'ambito del quadro strategico in materia di prodotti sostenibili, si prevede espressamente la responsabilizzazione dei consumatori affinché possano svolgere un ruolo attivo nella transizione ecologica; nonché direttiva (UE) 2024/825 del Parlamento europeo e del Consiglio, del 28 febbraio 2024, che modifica le direttive 2005/29/CE e 2011/83/UE per quanto riguarda la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione, considerando 1, secondo cui, al fine di contribuire al corretto funzionamento del mercato interno, assicurando nel contempo un elevato livello di protezione dei consumatori e dell'ambiente e il progresso della transizione verde, è essenziale consentire ai consumatori di assumere decisioni di acquisto informate e di contribuire, in tal modo, a modelli di consumo più sostenibili. V. altresì Commissione europea, *2030 Consumer Agenda*, 19 novembre 2025, che individua il consumo sostenibile tra le quattro aree prioritarie della politica europea dei consumatori.

22. v. A. Bassi - M. Lamandini - G. Mollo - A. Troisi - F. Vella, Greenwashing e tutela del consumatore per un'economia sostenibile, in Quaderni Giuridici Consob, n. 33, Roma, 2025, spec. p. 30 ss.; M.A. Ciocia, Il Greenwashing: asimmetrie di mercato e interventi normativi nell'Unione Europea, in European Journal of Privacy Law & Technologies, 2025, n. 2.

mente significativo. Il contrasto al *greenwashing*, la disciplina delle asserzioni ambientali generiche, la trasparenza sulla durabilità e sulla riparabilità dei prodotti e la lotta alle pratiche che favoriscono l'obsolescenza anticipata dimostrano ancora una volta come la disciplina delle pratiche commerciali scorrette sia divenuta uno strumento attraverso il quale perseguire obiettivi che trascendono il singolo rapporto di consumo.
La sostenibilità mostra però anche i rischi di un sistema eccessivamente frammentato. Informazione ambientale, progettazione del prodotto, obblighi delle imprese e tutela del consumatore appartengono a corpi normativi diversi, ma incidono sulla medesima scelta economica. Il consumatore è chiamato a orientarsi in una crescente quantità di informazioni, certificazioni, etichette e dichiarazioni ambientali proprio mentre l'esperienza digitale insegna che il semplice incremento dell'informazione non conduce necessariamente a decisioni migliori.
Digitale e sostenibilità pongono quindi, sotto angolazioni diverse, lo stesso problema: come preservare l'autodeterminazione del consumatore in mercati caratterizzati da una crescente complessità tecnica e regolatoria.
Anche in questo campo, pertanto, la prospettiva del 2030 sembra richiedere il passaggio da una tutela costruita esclusivamente intorno all'informazione a una tutela capace di incidere sulla correttezza delle condotte, sull'affidabilità delle dichiarazioni e, più in generale, sull'ambiente nel quale si forma la decisione di consumo.

5. Dalla frammentazione regolatoria alla coerenza del sistema: regole trasversali e coordinamento tra Autorità

Le trasformazioni descritte conducono a una questione più generale. La progressiva specializzazione del consumatore – risparmiatore, assicurato, utente delle comunicazioni, passeggero, utente dell'energia, utilizzatore di una piattaforma digitale – ha storicamente giustificato discipline settoriali e l'attribuzione delle relative competenze a differenti Autorità indipendenti. Tale modello conserva evidenti ragioni di efficienza, legate soprattutto alla specializzazione tecnica dei regolatori.
La trasformazione digitale tende tuttavia a rendere sempre meno netti i confini tra i mercati.
Una piattaforma può essere contemporaneamente intermediaria commerciale, fornitore di servizi digitali, utilizzatore di dati personali, soggetto rilevante ai fini della concorrenza e utilizzatore o fornitore di sistemi di intelligenza artificiale. Una medesima condotta può incidere contemporaneamente sulla protezione dei dati, sulla concorrenza, sulla libertà di scelta del consumatore e sulle regole proprie del mercato interessato. La tutela dei minori nell'ambiente digitale offre, del resto, un esempio particolarmente significativo di tale trasversalità. La protezione del giovane consumatore si colloca infatti all'intersezione tra disciplina delle pratiche commerciali scorrette, Digital Services Act, regolazione dei sistemi di intelligenza artificiale, protezione dei dati personali e disciplina dei servizi audiovisivi. La vulnerabilità del destinatario diviene così il punto di convergenza di discipline diverse, confermando come la crescente specializzazione delle regole richieda, al tempo stesso, strumenti capaci di ricomporne l'unità rispetto alla concreta esperienza del consumatore.
E il problema non riguarda soltanto la sovrapposizione materiale delle norme. Le diverse discipline rispondono a logiche regolatorie e a modelli di *enforcement* non coincidenti[23] (nazionale, europeo o misto).
Il tradizionale diritto europeo dei consumatori affida un ruolo centrale alle autorità e ai giudici nazionali e opera prevalentemente attraverso valutazioni *ex post* della singola fattispecie. DSA e DMA attribuiscono invece alla Commissione europea un ruolo diretto particolarmente significativo nei confronti dei maggiori operatori digitali; altre discipline introducono sistemi di valutazione del rischio, audit, documentazione tecnica, organismi di standardizzazione e forme di coinvolgimento degli stessi soggetti regolati.
Alla pluralità delle norme corrisponde quindi una *pluralità delle architetture di enforcement*.
È questo, forse, uno dei punti sui quali la riflessione sul consumatore 2030 dovrebbe maggiormente concentrarsi.
La frammentazione non deriva necessariamente – e non solo - dall'incoerenza delle singole norme: può manifestarsi anche quando discipline tra loro astrattamente coerenti vengono applicate secondo procedimenti differenti, da autorità diverse e sulla base di categorie interpretative non perfettamente sovrapponibili.
La disciplina dei *dark patterns* ne costituisce ancora una volta un esempio paradigmatico. La stessa configurazione di un'interfaccia può essere scrutinata da differenti autorità sulla base di normative diverse. Se manca un sufficiente coordinamento, il rischio non è soltanto la duplicazione dell'intervento, ma la formazione di interpretazioni divergenti della stessa pratica.

23. Sul possibile concorso tra discipline diverse rispetto alla medesima condotta nei mercati digitali, con particolare riguardo ai rapporti tra protezione dei dati personali e disciplina delle pratiche commerciali scorrette, v. P. OCCHIUZZI, Consumatore attivo, patrimonializzazione dei dati personali ed enforcement tra GDPR e disciplina delle pratiche commerciali scorrette, in Diritto ed economia del consumo, Roma, Roma TrE-Press, 2024, 165 ss.; più recentemente, con riguardo alla più ampia sovrapposizione tra DSA, DMA, AI Act, GDPR e Codice del consumo e ai conseguenti problemi di coordinamento tra autorità, M. CAPPAI – P. OCCHIUZZI, Il dovere di leale collaborazione istituzionale nei rapporti tra autorità indipendenti e agenzie: dal coordinamento occasionale alla strutturale interdipendenza, in F. BASSAN (a cura di), cit.

La questione diviene allora quella della coerenza complessiva del sistema.
Come è stato evidenziato dalla più autorevole dottrina[24] con riferimento alla regolazione delle piattaforme e, più recentemente, alla governance dell'intelligenza artificiale, la risposta a fenomeni strutturalmente trasversali non può essere affidata esclusivamente alla moltiplicazione di discipline verticali e di competenze separate. Diventa necessario sviluppare regole trasversali e forme di *cross-regulation* capaci di conservare la specializzazione senza perdere l'unitarietà del fenomeno regolato.
La prospettiva non dovrebbe pertanto essere quella di sostituire le discipline settoriali con una indistinta regolazione generale. Occorre piuttosto individuare principi e regole trasversali capaci di operare nei diversi mercati, lasciando alle discipline speciali il compito di adattarli alle peculiarità delle singole attività.
Un ragionamento analogo deve essere condotto sul piano istituzionale.
Se la stessa condotta può interessare contemporaneamente differenti interessi pubblici, l'azione delle Autorità competenti non può svilupparsi secondo logiche completamente separate. La specializzazione rimane indispensabile, ma deve essere accompagnata da strumenti capaci di assicurare coerenza nell'interpretazione e nell'applicazione delle norme.
Il rapporto tra tutela dei consumatori e protezione dei dati offre già indicazioni interessanti. Linee guida, pareri e strumenti di consultazione possono contribuire a chiarire l'interazione tra differenti discipline senza richiedere necessariamente un'ulteriore stratificazione normativa. Analogamente, protocolli di cooperazione e meccanismi di consultazione reciproca – quale quello sviluppato nell'ordinamento italiano nei rapporti tra AGCM e Garante per la protezione dei dati personali – rappresentano un primo livello di coordinamento istituzionale.
La complessità del nuovo ecosistema digitale induce tuttavia a interrogarsi sull'opportunità di procedere ulteriormente, individuando sedi stabili di confronto tra le diverse Autorità che esercitano competenze sui mercati digitali, capaci di favorire la convergenza interpretativa e di prevenire sovrapposizioni o contraddizioni nell'enforcement.
La stessa esperienza europea offre alcuni primi modelli, come il *High Level Group* previsto nell'ambito del DMA, nel quale trovano rappresentanza differenti competenze regolatorie. Anche il Digital Fairness Fitness Check individua nella cooperazione più stretta tra differenti autorità europee e nazionali e rispettive reti uno degli strumenti attraverso i quali rafforzare la coerenza del digital rulebook.
La prospettiva non è dunque quella di eliminare la pluralità dei regolatori, che riflette la pluralità degli interessi protetti, quanto piuttosto quella di governarla. La questione centrale diventa come trasformare la pluralità delle competenze da possibile fattore di frammentazione in elemento di specializzazione all'interno di un sistema coordinato.

6. Autorità e consumatori 2030: dalla cross-regulation alla cross-enforcement?

Se la prima sfida del diritto dei consumatori verso il 2030 è quella della coerenza delle regole, la seconda riguarda inevitabilmente la coerenza dell'*enforcement*.
Il problema è già chiaramente percepibile nel sistema vigente ed è stato già chiaramente rilevato dalla dottrina. Il DSA e il diritto europeo dei consumatori dispongono di proprie strutture di *public enforcement*, mentre gli strumenti che disciplinano la cooperazione tra autorità appartenenti ai differenti sistemi rimangono ancora limitati. La possibilità che sulla medesima piattaforma e su un insieme sostanzialmente coincidente di fatti intervengano procedimenti distinti rende concreto il rischio di sovrapposizioni e decisioni divergenti.
Non si tratta di sostenere che una pluralità di interventi sia di per sé patologica. Una stessa condotta può ledere interessi differenti e risultare legittimamente rilevante sotto più discipline. Il problema nasce quando alla pluralità degli interessi protetti non corrispondono strumenti adeguati per assicurare la coerenza delle rispettive valutazioni[25].
La crescente interdipendenza tra diritto dei consumatori, concorrenza, protezione dei dati, regolazione delle piattaforme e intelligenza artificiale rende quindi sempre meno soddisfacente un modello nel quale alla trasversalità sostanziale dei fenomeni corrisponda una rigida separatezza delle rispettive attività di *enforcement*.
Ciò non significa necessariamente concentrare le competenze presso un'unica Autorità. Al contrario.
La questione è piuttosto se sia possibile passare progressivamente da una semplice cooperazione tra Autorità a forme più strutturate di coordinamento dell'*enforcement*.
Una possibile traiettoria può essere immaginata per gradi.
I protocolli bilaterali, la consultazione reciproca e lo scambio di informazioni costituiscono un primo livello. Un

24. v. F. BASSAN, Digital Platforms and Blockchains: The Age of Participated Regulation, in European Business Law Review, 2023; F. BASSAN – M. RABITTI, L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti, in Federalismi.it, 2024, n. 30, 250 ss.; nonché ID., in F. BASSAN – M. RABITTI (a cura di), L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti, Roma, Roma TrE-Press, 2025, 13 ss.
25. v. M. CAPPAI – P. OCCHIUZZI, Il dovere di leale collaborazione istituzionale nei rapporti tra autorità indipendenti e agenzie: dal coordinamento occasionale alla strutturale interdipendenza, in F. BASSAN (a cura di), Piattaforme digitali e consumatori, Roma, Roma TrE-Press, 2026, spec. § 1 e § 3.2

secondo livello può essere rappresentato da sedi permanenti di confronto tra le Autorità interessate alla regolazione dell'ecosistema digitale, finalizzate alla convergenza interpretativa, alla condivisione delle competenze tecniche e all'individuazione precoce delle fattispecie suscettibili di ricadere nell'ambito di più discipline.
Un ulteriore terreno riguarda la condivisione degli strumenti di conoscenza. DSA, DMA e AI Act producono una quantità crescente di informazioni attraverso *risk assessments*, audit, documentazione tecnica e obblighi di trasparenza. La possibilità, nel rispetto delle regole sulla riservatezza e dei limiti propri di ciascuna disciplina, che tali informazioni possano essere utilizzate anche dalle altre Autorità competenti potrebbe ridurre duplicazioni e aumentare la capacità di individuare tempestivamente le condotte dannose per i consumatori[26].
In prospettiva può essere infine posta una questione ulteriore: se, per le fattispecie autenticamente trasversali, sia opportuno immaginare forme di coordinamento anche di alcune fasi dell'attività istruttoria, ferma restando l'autonomia delle decisioni adottate da ciascuna Autorità nell'esercizio delle proprie competenze. Acquisizione e analisi dei dati, strumenti tecnologici di monitoraggio, attività ispettive e, quando consentito dalla disciplina applicabile, condivisione degli elementi acquisiti potrebbero costituire terreni sui quali sperimentare forme più avanzate di cooperazione.
Indicazioni in tale direzione sembrano emergere anche dalla più recente disciplina europea relativa alla protezione dei minori online. La proposta di KIDS Act, pur introducendo specifici obblighi di tutela, tende infatti a innestare la relativa attività di vigilanza sulle strutture di *enforcement* già previste dal DSA e dall'AI Act, dichiaratamente al fine di evitare duplicazioni e assicurare coerenza con i rispettivi sistemi di regolazione. Si tratta di un esempio significativo di come alla trasversalità dei rischi possa progressivamente corrispondere una maggiore integrazione funzionale dei meccanismi di *enforcement*.
La traiettoria potrebbe allora essere descritta come un progressivo passaggio dalla *cross-regulation* alla *cross-enforcement:* non un unico regolatore per mercati sempre più complessi, ma Autorità specializzate capaci di operare all'interno di un sistema nel quale la pluralità delle competenze sia ricondotta a coerenza.
Guardando al 2030, il modello potrebbe dunque poggiare su tre direttrici complementari: regole trasversali capaci di preservare un nucleo comune di tutela nei diversi mercati; un enforcement coordinato, in grado di ricomporre sul piano applicativo la frammentazione delle competenze; l'empowerment del consumatore, necessario affinché la crescente sofisticazione della tutela normativa sia accompagnata dalla capacità concreta delle persone di comprendere e governare le proprie scelte.
Il consumatore 2030 sarà infatti sempre meno definibile attraverso la sola relazione contrattuale con il professionista. Sarà un soggetto immerso in ecosistemi digitali, destinatario di decisioni algoritmiche e di offerte personalizzate, produttore di dati, utilizzatore di sistemi di intelligenza artificiale e, contemporaneamente, attore della transizione ambientale.
La sfida dei prossimi anni non sarà dunque soltanto quella di assicurare più tutela, ma di costruire una tutela più coerente, comprensibile ed effettiva. Se il mercato digitale tende a ricomporre fenomeni che il diritto ha storicamente disciplinato separatamente, anche la regolazione e l'*enforcement* dovranno trovare strumenti capaci di ricomporre quella unità senza rinunciare alla specializzazione.
In fondo, il percorso iniziato con la tutela del contraente debole conduce nuovamente alla persona. Ma vi conduce attraverso un mercato profondamente diverso: non più soltanto luogo dello scambio, bensì ambiente digitale, informativo e sociale nel quale si formano le preferenze e si esercitano diritti fondamentali. È sulla capacità di garantire l'autonomia della persona *nel mercato* – e, quando necessario, *dal mercato* – che dovrà misurarsi l'effettività della tutela del consumatore nel 2030.

26. In ambito europeo, al Digital Markets Act High Level Group, previsto dall'art. 40 del Regolamento (UE) 2022/1925 (DMA), 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 nonché comporta, da un punto di vista squisitamente procedurale, tempi decisionali più lunghi.

IL CONSUMATORE 2030 IN UN *DIGITAL WELFARE* IBRIDO

(di Marco Cappai)

Il contributo esamina le dinamiche evolutive del Digital Welfare State (DWS) nell'era "ibrida", caratterizzata dalla crescente contaminazione reciproca tra pubblico e privato. Prova quindi a trarre delle ricadute applicative, anche in punto di diritto dei consumi, da questo generale mutamento di prospettiva. In particolare, si sostiene che l'Unione sta seguendo un percorso che la porta a occuparsi non più solo di servizi digitali, ma anche di assetti organizzativi degli operatori ITC e, da ultimo, delle infrastrutture tecnologiche abilitanti.

SOMMARIO: 1. Pubblico-Privato, dagli incroci alle rotatorie; 2. Prima rotatoria: digital (fundamental) rights. 3. Seconda rotatoria: technology regulation. 4. Terza rotatoria: Digital (o Technological) Sovereignty. 5. Ricadute per il diritto dei consumi: dai servizi, all'adeguatezza organizzativa, alle infrastrutture

1. Pubblico-Privato, dagli incroci alle rotatorie

Viviamo in un un'"era ibrida"[1] in cui le infrastrutture digitali (piattaforme digitali; *cloud*; IoT; IA; *blockchain*; ecc.) – per lo più, oggi, private – contribuiscono a plasmare (o comunque condizionare) aspetti decisivi della vita pubblica.
La crescente fluidità del sistema induce a raffigurare i rapporti tra pubblico e privato non più come "incroci", bensì come "rotatorie".
Ne risente, anzitutto, il concetto di *welfare* e, con esso, di *Digital Welfare State* (DWS), espressione che – è noto – suole utilizzarsi per descrivere in modo onnicomprensivo quel fascio di diritti di prestazione e livelli di protezione che i cittadini vantano nei confronti dello Stato digitale.
Se, infatti, una porzione non indifferente di *Digital Welfare* è, nella contemporaneità, *non-State*, perché legato in misura consistente a servizi privati erogati in mancanza di un mandato pubblico esplicito, allora sorge l'esigenza di regolare unitariamente gli ambiti, sempre più osmotici, del pubblico e del privato.
Il presente contributo individua tre rotatorie principali: diritti digitali fondamentali[2]; regolazione tecnologica[3]; sovranità digitale (o tecnologica)[4].
L'effetto combinato delle tre – apprezzabile, si dirà, anche in punto di diritto dei consumi – determina un graduale spostamento di prospettiva: dai servizi; all'adeguatezza organizzativa; all'infrastruttura abilitante sottostante[5].

1. Prima rotatoria: Digital (Fundamental) Rights

La dottrina ha definito il "costituzionalismo digitale"[6] come il tentativo, da parte dell'UE, di incanalare il potere digitale privato basandosi sulla dottrina dell'effetto diretto orizzontale dei diritti fondamentali[7].
Una volta che lo *standard* di protezione è fissato a livello costituzionale, esso si applica, in linea di principio, sia ai soggetti digitali privati che a quelli pubblici.
Ad esempio, sulla base degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), nelle cause *Digital Rights Ireland*, seguite da *Tele2* e *La Quadrature du Net*, la Corte di giustizia ha vietato regimi di conservazione indiscriminata di (meta)dati, annullando, per l'effetto, la Direttiva (CE) 2006/24[8]. Ha in quella sede stabilito che le finalità (legittime) di lotta alla criminalità e di salvaguardia della sicurezza pubblica possono essere invocate solo per giustificare misure di conservazione mirate. La direttiva invalidata, al contrario, imponeva un obbligo di conservazione generale e indiscriminata dei (meta)dati incompatibile con i diritti fondamentali digitali dei cittadini. È interessante notare che la stessa logica ispira, sul versante privato, il principio dell'assenza di obblighi di monitoraggio generale o di ricerca attiva di informazioni ("*no general monitoring or active fact-finding obligations*"), sancito dal *Digi-*

1. F. Bassan, L'era ibrida. Sovranità e democrazia tra poteri pubblici e imprese tech, Rubettino, 2026.
2. Infra § 2.
3. Infra § 3.
4. Infra § 4.
5. Infra § 5.
6. G. De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge University Press, Cambridge, 2022.
7. Corte di giustizia, 8 aprile 1976, C-43/75, Gabrielle Defrenne c. Société anonyme belge de navigation aérienne Sabena (Defrenne II).
8. Grande Sezione, 8 aprile 2014, C-293 e 594/12; 21 dicembre 2016, C-203 e 698/15; 8 ottobre 2020, C-511-512 e C-520/18.

tal Services Act (DSA) e che, come noto, che si applica anche alle piattaforme *online* e ai motori di ricerca di dimensioni molto grandi (VLOPs e VLSEs, rispettivamente)[9].

Come chiarito nella "Dichiarazione europea sui diritti digitali", l'articolo 2 del TUE, insieme alla CDFUE e alla Convenzione europea dei diritti dell'uomo (CEDU), in combinato disposto con l'articolo 6, paragrafi 1 e 3 TUE, definisce l'UE come un'"Unione di valori", incentrata sui valori della dignità umana, della libertà, della democrazia, dell'uguaglianza, della solidarietà, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze[10]. Secondo la Dichiarazione, "*il modello dell'UE per la trasformazione digitale delle nostre società e della nostra economia comprende in particolare la sovranità digitale in modo aperto, il rispetto dei diritti fondamentali, lo Stato di diritto e la democrazia, l'inclusione, l'accessibilità, l'uguaglianza, la sostenibilità, la resilienza, la sicurezza, il miglioramento della qualità della vita, la disponibilità di servizi e il rispetto dei diritti e delle aspirazioni di ognuno. Dovrebbe contribuire alla costruzione di un'economia e una società dinamiche, eque ed efficienti in termini di risorse nell'UE*"[11].

È stato osservato che la Dichiarazione apre la strada a una "cittadinanza digitale" dell'UE[12], intesa come "la capacità di partecipare alla società *online*"[13] secondo i valori europei. Questa analogia deriva dal fatto che tale livello di protezione, o *status*, è legato, esattamente come il concetto di cittadinanza dell'UE di Maastricht, al territorio dell'Unione.

A questo proposito, ci si è anche chiesti se debba essere introdotto un nuovo "diritto a non utilizzare Internet", autonomo e complementare al diritto di utilizzarlo, oppure, in alternativa, se alcuni dei diritti esistenti (ad esempio la libertà di espressione, il diritto alla *privacy*, il diritto a un rimedio effettivo) debbano essere interpretati in tal senso[14]. Sebbene si tratti di una questione intrigante, sembra più pragmatico cercare di conciliare il diritto di utilizzare Internet con quello di non utilizzarlo, anziché contrapporli. In particolare, l'accesso *online* e *offline* all'assistenza sociale può essere conciliato progettando infrastrutture dedicate. A questo proposito, l'esperimento svedese dei "centri di servizi sociali" rappresenta una strada promettente. Infatti, la creazione di strutture fisiche che favoriscono l'interazione umana non è vista, in quel contesto, come un'alternativa *offline* all'assistenza digitale[15]. Piuttosto, in quel modello la sede fisica è accessoria rispetto all'erogazione digitalizzata, che rimane l'unico canale a disposizione dei cittadini. Una volta garantita efficacemente l'inclusione, superando il problema della discriminazione posto dal *digital divide*, le nazioni sovrane ben possono promuovere una transizione digitale, assicurando un miglioramento delle prestazioni a costi inferiori.

Per altro profilo, laddove rimanga disponibile un'alternativa *offline* all'assistenza *online*, o laddove la leva digitale sia concepita come complemento all'assistenza *offline* di base, i decisori politici restano liberi di incentivare (*nudging*) soluzioni che privilegino il digitale (*digital-first*).

Ad esempio, questa strategia è particolarmente evidente nei meccanismi di "*opt-out*" previsti dal regolamento sullo Spazio europeo dei dati sanitari (EHDS) per l'"uso primario" e l'"uso secondario" dei dati sanitari[16].

Un approccio similare è poi seguito dal Ministro dell'interno in sede di rilascio della carta di identità elettronica (CIE). La tessera fisica, infatti, incorpora già al suo interno le chiavi crittografiche dell'identità digitale del cittadino, che questi potrà poi decidere se attivare/utilizzare o meno. Si tratta di una opzione di *policy* non scontata, giacché non imposta dal quadro di riferimento eIDAS[17] ed eIDAS 2.0[18], e che infatti si ritrova solo in un limitato numero di Stati membri, tra i quali, per l'appunto, rientra l'Italia[19].

2. Seconda rotatoria: Technology Regulation

La seconda rotatoria si ha lì dove l'Unione avverte l'esigenza di disciplinare, direttamente o indirettamente, la tecnologia (*Technology Regulation*).

Prendendo a riferimento l'architettura tecnologica sottostante, e non i servizi in quanto tali, questa disciplina non può che essere comune, almeno in parte, ai due ambiti del diritto pubblico e del diritto privato.

9. Art. 8 Regolamento (UE) 2022/2065 (e, in precedenza, art. 15, § 1 Direttiva (CE) 2000/31).
10. Dichiarazione congiunta del Parlamento europeo, Consiglio UE e Commissione europea "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" (2023/C 23/01), § 1.
11. Ib., § 6.
12. A. Iliopoulou-Penot, The construction of a European digital citizenship in the case law of the Court of justice of the EU, in CMLR, 59(4)/2022, 969-1006, 974.
13. K. Mossberger - C.J. Tolbert - R.S. McNeal, Digital Citizenship. The Internet, Society and Participation, MIT Press, Cambridge (US), 2007.
14. D. Kloza, The right not to use the internet, in Computer Law & Security Review, 52(2024), 105907, 1-8.
15. A Kaun - A. Liminga, Welfare service centers: Maintenance, repair, and care at the analog interfaces of the digital welfare state, in New Media & Society, n. 27(5)/2025, 3039-3054.
16. Reg. (UE) n. 2025/327, cons. 18 e art. 10; cons. 54 e art. 71, su cui T. Sokol, European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance?, in European Journal of Health Law, n. 31(4)/2024, 365-388.
17. Reg. (UE) 2014/910.
18. Reg. (UE) 2024/1183.
19. https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/48762251/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

Più in dettaglio, è noto che, secondo il principio della "neutralità tecnologica" – comunemente sintetizzato con la formula "stesse attività, stessi rischi, stesse regole" – nella misura in cui i rischi derivanti da un unico tipo di attività siano gli stessi, indipendentemente dalle tecnologie utilizzate per svolgerla, la legislazione non dovrebbe interferire con la progettazione delle diverse tecnologie disponibili sul mercato, né direttamente (imponendo l'uso di una determinata tecnologia), né indirettamente (incoraggiando l'uso di alcune tecnologie piuttosto che di altre). Pertanto, e in questo senso, la legislazione dovrebbe rimanere, in linea di principio, neutrale rispetto alla tecnologia[20].
Tuttavia, ciò non significa che ai legislatori sia precluso qualsiasi intervento normativo in ambito tecnologico.
Ad esempio, gli Stati membri possono incoraggiare l'adozione di una determinata soluzione tecnologica senza violare il diritto dell'Unione, nella misura in cui ciò appaia necessario, subordinatamente a un rigoroso criterio di proporzionalità, per perseguire obiettivi di interesse generale[21].
A livello europeo, diversi atti legislativi disciplinano determinate tecnologie, sia direttamente (ad esempio, AI Act[22]) sia indirettamente (ad esempio, il MiCAR, che disciplina le cripto-attività e, di conseguenza, la *blockchain*; il *Data Act*, che disciplina la circolazione dei dati nell'Internet delle cose – IoT[23]; ecc.). Finora, nell'affrontare aspetti tecnologici complessi, al fine di trovare il giusto equilibrio tra garanzia e innovazione, il legislatore europeo ha privilegiato un approccio in due fasi. In primo luogo, ha fatto ricorso a principi generali per definire i rischi da mitigare/evitare e le relative responsabilità (approccio basato sul rischio). In secondo luogo, ha rimesso agli attori (pubblici o privati) coinvolti la scelta finale sulla misura più idonea per raggiungere gli obiettivi normativi ("*accounting principle*")[24].
Invertendo la prospettiva, si potrebbe sostenere che, quando viene emanata una normativa in materia di tecnologia, una possibile interpretazione del principio di neutralità è che, nella misura in cui le tecnologie alla base dei servizi privati e pubblici sono le stesse, i requisiti tecnici debbano essere, almeno in parte, gli stessi ("stesse tecnologie, stessi rischi, stesse regole").
Questa affermazione non pare contraddetta dal fatto che, talvolta, possano essere imposti requisiti tecnici aggiuntivi esclusivamente per gli enti pubblici[25]. L'aspetto fondamentale da sottolineare in questa sede è che gli elementi centrali della disciplina sono gli stessi nel settore privato e in quello pubblico.
Ad esempio, i requisiti di sicurezza informatica previsti dalla direttiva NIS2 si applicano sia agli attori pubblici che a quelli privati[26].
Allo stesso modo, l'*AI Act* riconosce che i sistemi di IA possono essere impiegati dai governi per fornire servizi pubblici essenziali quali l'assistenza sanitaria e la previdenza sociale, ma qualifica tali applicazioni come "ad alto rischio"[27], a meno che l'IA non svolga un ruolo ausiliario nel contesto del processo decisionale amministrativo[28]. In ogni caso, la pubblica amministrazione deve garantire la supervisione umana[29] e fornire spiegazioni sul ruolo svolto da tali sistemi di IA[30].
Il fatto che questi atti normativi disciplinino determinati aspetti tecnologici anche in relazione al settore pubblico significa che l'UE contribuisce indirettamente alla definizione del DWS. Tuttavia, ciò non si pone in contrasto con il principio di attribuzione. Infatti, concentrarsi sulla tecnologia sottostante, anziché regolamentare la prestazione sociale in quanto tale, consente all'UE di svolgere un ruolo federalizzante senza interferire con l'autonomia degli Stati membri nel campo sociale.
Inoltre, in alcuni contesti l'UE definisce l'architettura delle infrastrutture digitali da mettere a disposizione degli enti pubblici e privati che operano nel territorio europeo. Questa strategia normativa consiste nella combinazione di due elementi: sul versante legislativo, l'armonizzazione normativa; sul versante operativo, la promozione dei partenariati pubblico-privati (PPP) e l'assegnazione di risorse di bilancio dell'UE.
Un esempio di rilievo è rappresentato dagli Spazi europei dei dati (EDS)[31], un modello di *governance* complesso basato sul concetto di "*dataspace*" e costituito dalla combinazione di tre fattori principali: un ampio *pool* di dati; infrastrutture; *governance*. In particolare, gli spazi comuni europei dei dati sono la risposta per garantire fiducia, autonomia, so-

20. Il principio di neutralità tecnologica è di natura intersettoriale. Tuttavia, è stato concepito inizialmente nel settore delle telecomunicazioni. Nel corso del tempo, tale principio generale è stato esteso anche in altri ambiti, come ad esempio il Digital Financial Package: si veda il considerando 9 sia del Regolamento (UE) 2022/858 (DLT Pilot) sia del Regolamento (U)E 2023/1114 (MiCAR).
21. Direttiva 2002/21/CE, cons. 18; Direttiva (UE) 2018/1972, cons. 114.
22. Regolamento (UE) 2024/1689.
23. Regolamento (UE) 2023/2854.
24. Es. art. 5, § 2 Regolamento (UE) 2016/679 (GDPR).
25. Es. Regolamento (UE) 2024/903, Interoperable Europe Act (IEA), il cui campo di applicazione è ristretto ai "servizi digitali pubblici trans-europei" (art. 1, § 1).
26. Direttiva (UE) 2022/2555.
27. Cons. 58, art. 6(2) a All. III.
28. Art. 6, § 3.
29. Art. 14.
30. Art. 86.
31. Comunicazione della Commissione "Verso uno spazio comune europeo dei dati" (COM/2018/232 final).

vranità ed equità, conciliando innovazione e competitività con la tutela dei diritti e dei valori e un'equa distribuzione del valore tra le parti interessate. L'obiettivo principale degli spazi comuni europei dei dati è consentire a ricercatori, amministratori pubblici, aziende e individui di condividere e utilizzare al meglio i dati[32]. In sintesi, la ricetta europea per gli spazi dei dati è "*as open as possible, as closed as necessary*"[33]. Il già citato EHDS rappresenta, allo stato, l'esperimento probabilmente più completo e ambizioso di questo modello.

È importante sottolineare che i diritti (fondamentali)digitali e la regolazione tecnologica, sebbene concettualmente distinti, si intersecano e si sovrappongono in larga misura[34]. Questa caratteristica è particolarmente evidente, ad esempio, nel GDPR e nell'*AI Act*.

Ai fini della presente analisi, i due ambiti possono essere considerati congiuntamente per almeno due ragioni.

In primo luogo, entrambi presentano una competenza federale: la legislazione viene elaborata esclusivamente a livello dell'UE, lasciando agli Stati membri l'attuazione e l'applicazione[35].

In secondo luogo, entrambe hanno portata orizzontale, il che contribuisce a garantire lo Stato di diritto in un contesto di crescente contaminazione tra diritto internazionale (pubblico) e diritto transnazionale (privato), in cui i soggetti privati agiscono, sempre più, come "ordini giuridici privati"[36]. In questo scenario, poiché un numero esiguo di servizi privati può comportare "rischi sistemici", ciò significa anche, ribaltando la prospettiva, che tali servizi possono assumere un'importanza di interesse generale pur essendo prestati – lo si è anticipato – in assenza di un mandato pubblico esplicito. O meglio, si è detto, assumono un interesse se non "sociale", quantomeno "collettivo"[37]. La regolamentazione di tali attività, pertanto, può essere considerata come una necessaria sfaccettatura del DWS.

3. Terza rotatoria: dalla Technology Regulation alla Digital (o Technological) Sovereignty

In tempi più recenti sta maturando la convinzione che porsi come *rule-setter* globali in campo tecnologico (*Brussels effect*) non sia più sufficiente ad assicurare la sopravvivenza del DWS.

La fine del multilateralismo e la ri-regionalizzazione delle catene di approvvigionamento globali, insieme alle difficoltà che sta attraversando l'alleanza NATO, suggeriscono infatti che la continuità, la prosperità e la sicurezza del DWS (e, più in generale, del mercato interno) potrebbero essere compromesse dall'attuale eccessiva dipendenza dell'UE dai fornitori stranieri di servizi informatici.

Secondo la Dichiarazione di Berlino (2025), la sovranità digitale rappresenta la capacità dell'UE e dei suoi Stati membri di agire in modo autonomo e di scegliere liberamente le proprie soluzioni, traendo al contempo vantaggio dalla collaborazione con *partner* globali, ove possibile"[38]. Analogamente, il Parlamento europeo (2026) ha affermato che la sovranità tecnologica è la capacità di progettare, sviluppare e diffondere su larga scala le tecnologie digitali necessarie per la competitività della nostra economia, il benessere dei nostri cittadini e l'autonomia strategica dell'UE in un mondo globalizzato[39]. Per la Commissione europea (2026), la sovranità tecnologica denota la capacità dell'Europa di sviluppare, controllare e scalare le tecnologie, le infrastrutture, i servizi e i dati critici, compresi gli ecosistemi digitali, che sono alla base della sua economia, sicurezza e società, riducendo al contempo i rischi e diversificando le catene di approvvigionamento e l'esposizione tecnologica per ridurre le dipendenze strategiche e resistere alle interferenze straniere[40].

Segnatamente, l'autonomia strategica digitale presenta due dimensioni:

i) reattiva, quando mira a evitare un ulteriore indebolimento della sovranità tecnologica europea (si pensi, ad esempio, e anche al di là del settore tecnologico, allo *screening* degli investimenti diretti esteri[41]; al controllo delle sovvenzioni estere che distorcono il mercato interno[42]; allo strumento anti-coercizione – ACI[43]; ecc.);

32. G. Enes, The Common European Data Space(s). A Governance Model 'the European Way', in G. Enes - I. Neves - T. Morais Rocha (eds.), A Digital Europe for Citizens. Data Governance, Data Markets, Data Services, Springer, Cham, 2026, 54.
33. G. Bruzzone - K. Debackere, As Open as Possible, as Closed as Needed: Challenges of the EU Strategy for Data, in les Nouvelles - Journal of the Licensing Executives Society, n. 56(1)/2021, 44-49.
34. A. Bradford, Digital empires: the global battle to regulate technology, Oxford University Press, Oxford, 2023.
35. V. Papakonstantinou - P. De Hert,The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play, Routledge, 2024, 123 ss.
36. F. Bassan, Digital Platforms and Global Law, Edward Elgar, Northampton, 2021, 118 ss.
37. F. Bassan, L'era ibirida cit., 128.
38. Dichiarazione sulla sovranità digitale europea, 18 novembre 2025, firmata da tutti i 27 Stati membri.
39. Risoluzione del 22 gennaio 2026 "su una sovranità tecnologica e una infrastruttura digitale" (P10_TA(2026)0022), § 2.
40. Comunicazione "sulla sovranità tecnologica europea, accompagnata da una strategia dell'UE per l'open source" (COM(2026) 503 final), 1.
41. Regolamento (UE) 2026/1386, che abroga il Reg. (UE) 2019/452. In argomento, F. Bassan, Il coordinamento europeo delle norme nazionali sugli investimenti esteri e il golden power italiano, in Eurojus, 1/2026,168 ss.
42. Regolamento (UE) 2022/2560.
43. Regolamento (UE) 2023/2675.

ii) assertiva e proattiva, quando l'UE mira a potenziare le proprie capacità tecnologiche, industriali e di ricerca (si pensi, ad esempio, all'istituzione del Centro europeo di competenza per la sicurezza informatica nell'industria, nella tecnologia e nella ricerca e della rete dei centri nazionali di coordinamento; al progetto "AI Gigafactories"[44]; alle iniziative previste per una legge sullo sviluppo del *cloud* e dell'intelligenza artificiale (CADA) e per una strategia sull'*open source*[45]).

L'adozione di una pur sofisticata e avanzata *Technology Regulation*, dunque, non è più sufficiente. Occorre iniziare a *fabbricare* tecnologia o, quantomeno, a contribuire al suo *design*. L'adeguata progettazione della tecnologia diviene, dunque, precondizione della regolazione o, meglio, è essa stessa regolazione.

Si tratta di un salto concettuale non indifferente. Storicamente, invero, l'approccio dell'Unione è stato di accompagnare il mercato con vincoli giuridici esterni, aspettando che si affermasse la soluzione migliore. L'argomento, di crescente attualità, della sovranità digitale ha però spostato l'asse: l'UE vuole avere, sempre più, un ruolo da protagonista sin dallo sviluppo dell'infrastruttura/tecnologia.

E, se vuole raggiungere un risultato non ideologico, ma genuinamente competitivo, l'alleanza con il privato è imprescindibile.

Questo riporta *in auge* il paradigma della "regolazione partecipata", descritta in dottrina come tecnica regolatoria, alternativa alla *co-regulation*, in grado di assicurare una disciplina normativa realmente al passo coi tempi: in questa impostazione, cioè, non sono gli operatori a prendere parte al processo regolatorio, commentando proposte elaborate dalle competenti Autorità; sono queste ultime a partecipare agli esperimenti del mercato e, solo successivamente, ad assumere iniziative regolatorie[46].

Ora, nel momento in cui la *Technology Regulation* assume – per effetto del concorso con la nozione di sovranità digitale (o tecnologica) – colorazioni di politica industriale, la "regolazione partecipata" evolve, divenendo "tecnologia partecipata": gli Stati, opportunamente coordinati a livello UE, stanziano risorse per sviluppare tecnologie/*standard* genuinamente in linea con i valori europei, in una necessaria compartecipazione, operativo-industriale, con il settore privato[47].

4. Ricadute per il diritto dei consumi: dai servizi, all'adeguatezza organizzativa, alle infrastrutture

Le tre "rotatorie" appena descritte ci segnalano una tendenza evolutiva in atto.

Con le prime due, il legislatore si allontana dai "servizi" per concentrarsi, sempre più, sulla disciplina della "tecnologia" che quei servizi abilita. Non intendendo (o non potendo) procedere a una diretta conformazione della stessa, ne disciplina i limiti esterni (i diritti -fondamentali- digitali, che sempre devono essere garantiti). Inoltre, ne disciplina gli aspetti organizzativi, o meglio, potrebbe dirsi, di adeguatezza degli assetti organizzativi (la *Technology Regulation* enuncia quali sono i rischi da sterilizzare/mitigare, lasciando allo sviluppatore/*deployer* la responsabilità delle scelte implementative).

Anche il diritto dei consumi, latamente inteso, segue questa linea evolutiva.

Dopo un cospicuo filone di interventi di *enforcement* che ha interessato i servizi, si assiste infatti a una parziale inversione di rotta.

Si pensi al divieto di *dark patterns* posto dal DSA, che guarda all'architettura e al *design* del servizio[48].

Ai sensi dello stesso Regolamento, le VLOPS e VLSEs sono onerate dell'obbligo di valutare con diligenza i rischi sistemici, individuando specifici profili e aree di rischio[49]. Devono quindi adottare misure di attenuazione ragionevoli, proporzionate ed efficaci per sterilizzare i rischi sistemici mappati[50].

Anche in considerazione della difficoltà di definire compiutamente il concetto di *dark pattern*, nella sua prassi decisionale la Commissione predilige, almeno sin qui, la contestazione (indiretta), nei confronti delle sole VLOPS, dell'inosservanza dell'obbligo di apprestamento di adeguati presidi organizzativi rispetto alla strada, probabilmente più tortuosa, della contestazione (diretta) del divieto di *design* manipolativi[51].

44. Cfr. https://digital-strategy.ec.europa.eu/en/policies/ai-factories.
45. COM(2026) 503 final cit., 4.
46. F. Bassan, Digital Platforms and Blockchains: The Age of Participatory Regulation, in European Business Law Review, n. 34(7)/2023, 1103-1132.
47. Propone una "strategia consortile", ad esempio, F. Bassan, L'era ibrida cit., 63-65.
48. Art. 25, § 1: "I fornitori di piattaforme online non progettano, organizzano o gestiscono le loro interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate".
49. Art. 34.
50. Art. 35.
51. D. Foà, Intervento dal titolo "La collaborazione nell'enforcement del diritto dei mercati digitali" nel corso del Convegno "La vigilanza collaborativa tra procedimento e provvedimento", LUISS, 1° ottobre 2026.

Se si segue ulteriormente il percorso – imboccando, appunto, la terza rotatoria – ci si può (e deve) aspettare una maggiore propensione, del legislatore e degli *enforcer*, a definire in via diretta anche aspetti di architettura. L'interesse verso gli assetti organizzativi dovrebbe cioè estendersi anche agli aspetti infrastrutturali. Proprio questa dovrebbe essere la via per imprimere un reale valore aggiunto alle proposte legislative programmate o in corso, prime fra tutte il *Digital Fairness Act*[52] e il *Kids Act*[53]. A meno di non voler licenziare testi normativi ridondanti rispetto al vigente *acquis* consumeristico.

52. https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act.
53. Proposta di Regolamento del Parlamento europeo e del Consiglio EU Kids Act – L'UE per spazi digitali responsabili e affidabili in internet (2026/0286(COD)).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Priorità e questioni aperte per l'azione delle Autorità indipendenti in un mondo che cambia

(di Aurora Saija)

SOMMARIO: 1. PREMESSA E OBIETTIVO DELL'ANALISI. 2. LE SFIDE PER LA PROTEZIONE DEI DATI DERIVANTI DALLA SITUAZIONE GEOPOLITICA. 3. LE SFIDE PER LA PROTEZIONE DEI DATI DERIVANTI DALL'EVOLUZIONE DELLA TECNOLOGIA. 4. SALVAGUARDARE L'APPROCCIO REGOLATORIO EUROPEO E RAFFORZARE LA COOPERAZIONE.

1. Premessa e obiettivo dell'analisi

Ogni previsione sulle prossime traiettorie della regolazione in materia di protezione dei dati personali e della relativa attività di enforcement, in un orizzonte anche solo di breve periodo, appare oggi estremamente complessa, a causa dell'**incertezza del contesto di riferimento**. Non soltanto la trasformazione digitale e lo sviluppo dell'intelligenza artificiale avanzano a un ritmo non lineare, caratterizzato da accelerazioni e discontinuità, ma avvengono inoltre in uno scenario di **crescenti tensioni e cambiamenti dell'assetto geopolitico**, che investono tanto le relazioni tra i paesi quanto il rapporto e i confini tra potere pubblico e potere privato.

Crisi e conflitti internazionali mettono in luce le differenze tra ordinamenti negli approcci regolatori e rendono **più difficile il percorso verso soluzioni condivise a livello globale** su come assicurare che le istanze della competitività e dell'innovazione vengano conciliate con il rispetto delle libertà e dei diritti fondamentali e con l'attuazione dei valori democratici della società civile. Al contempo si aprono **nuovi fronti di rischio per la sicurezza**, in quanto i dati costituiscono un fattore decisivo per la crescita economica e, quindi, uno strumento di potere e di pressione. Non è un caso che le grandi imprese del settore tecnologico abbiano consolidato posizioni di mercato tali da consentire loro di esercitare un'influenza sempre più marcata sulla politica in materia di dati ed economia digitale. Anche la recente Enciclica papale *Magnifica Humanitas* sottolinea che *"in molti casi nel contesto digitale, il controllo delle piattaforme, delle infrastrutture, dei dati e della capacità di calcolo non è appannaggio degli Stati, ma di grandi attori economici e tecnologici che, di fatto, fissano le condizioni di accesso, le regole della visibilità e le possibilità stesse di partecipazione. Quando un potere di tale portata si concentra in poche mani, tende a farsi opaco e a sfuggire al controllo pubblico, e cresce il rischio di uno sviluppo distorto che genera nuove dipendenze, esclusioni, manipolazioni e disuguaglianze"*[1].

In questo quadro variegato, la **protezione dei dati** assume un ruolo che supera la dimensione della privacy e del controllo consapevole dell'individuo sull'uso delle informazioni che lo riguardano e, da un lato, diventa **fattore decisivo nella realizzazione degli obiettivi di sovranità e resilienza** perseguiti a livello nazionale e sovranazionale, dall'altro, si conferma strumento **indispensabile per affermare la dignità e la centralità della persona**. La questione da affrontare è se il regime giuridico e istituzionale vigente sia adeguato alle sfide emergenti e quali aspetti debbano, eventualmente, essere ripensati e migliorati per garantirne la tenuta a fronte delle evoluzioni in atto.

2. Le sfide per la protezione dei dati derivanti dalla situazione geopolitica

Le trasformazioni geopolitiche degli ultimi anni hanno alterato l'equilibrio nelle relazioni tra i paesi e, per l'effetto, **i temi della sicurezza e della sovranità digitale hanno assunto una rilevanza centrale**. I dati, così come le reti e le infrastrutture che li accolgono e ne consentono la circolazione, sono asset sempre più strategici e, possono costituire bersaglio di attacchi malevoli, eventualmente condotti in parallelo ad azioni militari e tali da mettere in pericolo l'economia reale, la stabilità del sistema finanziario e la democrazia di interi paesi.

Basti pensare alle conseguenze che l'interruzione dei flussi informativi o la distruzione di banche dati può avere rispetto alla prestazione di servizi essenziali, all'operatività dei sistemi di pagamento e all'esercizio dell'attività d'impresa. O, ancora, al fatto che dai dati illecitamente acquisiti possono essere tratte informazioni su caratteristiche della popo-

1. Lettera enciclica Magnifica Humanitas del Santo Padre Leone XIV sulla custodia della persona umana nel tempo dell'intelligenza artificiale, 2026, par. 95.

lazione, utilizzabili a fini di discriminazione e violazione dei diritti umani fondamentali. Comportamenti abusivi in materia di dati possono inoltre essere funzionali a diffondere disinformazione e persino manipolare i processi di voto, compromettendo la partecipazione dei cittadini alla vita politica. Da questo punto di vista, il noto caso *Cambridge Analytica* ha mostrato il ruolo che le piattaforme di social media, mediante algoritmi di profilazione, sono in grado di svolgere nella targetizzazione degli elettori e nella propaganda mirata a orientarne le scelte, anche in linea con gli interessi di regimi terzi rispetto alla collettività specificamente coinvolta.

Come sottolineato dalla Nato, i **metodi di guerra ibridi** – basati sulla combinazione di mezzi militari e non militari – sono stati a lungo utilizzati per confondere i confini tra guerra e pace e seminare dubbi nelle menti delle popolazioni bersaglio, destabilizzando l'avversario; la novità degli attacchi osservati negli ultimi anni risiede nella loro velocità, portata e intensità, facilitate dal rapido progresso tecnologico e dall'interconnessione globale[2].

A prescindere da aggressioni e conflitti veri e propri, le tensioni nei rapporti di natura commerciale tra paesi si intrecciano oggi a **visioni contrapposte sull'accesso ai dati, sull'uso delle tecnologie e sulle corrispondenti garanzie per i diritti individuali**. Accade così che il Governo USA metta in discussione il quadro regolatorio dell'Unione europea in materia digitale (dal GDPR all'AI Act, passando per il Digital Markets Act e il Digital Services Act), in quanto espressione di una tendenza al protezionismo che sfavorisce l'industria digitale statunitense, e adotti provvedimenti che indeboliscono la tenuta degli accordi per il trasferimento di dati personali tra le due sponde dell'Atlantico. A quest'ultimo riguardo, va ricordato il faticoso percorso che, attraverso le sentenze della Corte di giustizia nei casi Schrems I e II, ha portato a un *Data Privacy Framework* contenente l'impegno degli Stati uniti a contenere le possibili ingerenze dei propri servizi di intelligence nella sfera giuridica dei cittadini europei e a rafforzare gli strumenti di tutela giurisdizionale dei diritti nei casi di raccolta o gestione illecita dei dati personali. L'efficacia di questo strumento potrebbe scontrarsi con la decisione, adottata dal Presidente USA nel gennaio 2025 e confermata dalla sentenza della Corte suprema del 29 giugno 2026[3], di rimuovere arbitrariamente (senza "*statutory cause*") uno dei componenti della Federal Trade Commission. L'indipendenza della FTC – che figura tra le autorità designate come competenti a vigilare sul trattamento dei dati personali trasmessi dall'UE verso gli Stati uniti – costituisce, infatti, uno dei presupposti indispensabili affinché l'Unione europea possa riconoscere come equivalente al proprio e, quindi, adeguato il livello di *data protection* offerto dal paese di destinazione dei dati, autorizzando il trasferimento.

Per alcune tipologie di minacce che la situazione geopolitica pone alla protezione dei dati, la risposta dell'Unione europea non può che passare attraverso **l'implementazione di solide misure di sicurezza**, **specialmente sul fronte cyber, e un rigoroso apparato di vigilanza, nonché di intervento rapido in caso di violazioni.** Migliorare la resilienza del sistema implica assicurare che le autorità degli Stati membri siano dotate di poteri e risorse adeguati ai loro compiti e cooperino in modo efficace per prevenire i rischi e minimizzare l'impatto di eventuali incidenti.

Le questioni legate alla diversità degli approcci regolatori al trattamento dei dati e alle conseguenti richieste affinché l'Unione riveda, allentandone le maglie, il proprio quadro normativo, richiedono una riflessione di altro tenore. Si tratta di tornare alle fondamenta del diritto europeo e alle scelte con cui «*l'Europa ha espresso la propria identità politica nel contesto di una competizione mondiale sempre più incentrata sul dominio della tecnica... ha dimostrato di comprendere fino in fondo il valore geopolitico dei dati e ha ridisegnato il proprio ruolo, sullo scacchiere internazionale, promuovendo un governo della tecnica in funzione della democrazia, per renderla "trustworthy"*»[4].

La portata extraterritoriale del GDPR, ripresa dai successivi atti regolamentari in materia digitale, riflette la volontà del legislatore europeo di assicurare una tutela globale dei diritti degli interessati nell'UE e di stabilire, in termini di requisiti sulla protezione dei dati, una parità di condizioni per le imprese attive sui mercati UE, in un contesto caratterizzato da flussi di dati su scala mondiale[5]. Muovendo da questa consapevolezza, e quindi **mantenendo fermo lo standard che ha finora costituito un solido presidio per i diritti e le libertà delle persone e i valori della società e ha alimentato il *Brussels effect***, è possibile valutare se vi siano margini per garantire una maggiore coerenza degli strumenti, alleggerire alcuni vincoli e semplificare la compliance, in un'ottica non già di 'resa' a pressioni esterne, ma di rafforzamento della competitività. Come riconosciuto dalla Commissione europea nella "Strategia europea per i dati", è indispensabile «*un approccio aperto ma assertivo ai flussi di dati internazionali, basato sui valori europei*»[6].

3. Le sfide per la protezione dei dati derivanti dall'evoluzione della tecnologia

2. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats
3. https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf
4. "Fiducia (nel) digitale – Protezione dei dati, IA e democrazia" Discorso del Presidente del Garante per la protezione dei dati personali, Pasquale Stanzione, in occasione della presentazione della Relazione annuale 2025, Roma, 2 luglio 2026.
5. European Data Protection Board, Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3) Versione 2.1, 12 novembre 2019.
6. Comunicazione della Commissione europea, Una strategia europea per i dati, COM (2020) 66 final.

Altrettanto significative sono le sfide poste alla protezione dei dati personali dall'evoluzione della tecnologia, che pure, come già accennato, si intrecciano con quelle connesse alla trasformazione del contesto geopolitico amplificandone i rischi, in quanto la corsa verso la leadership tecnologica è oggi il principale motore della competizione internazionale. Il rapido affermarsi dell'intelligenza artificiale reca **enormi potenzialità** in termini di crescita economica e miglioramento del benessere collettivo, **ma anche criticità connesse tanto allo sviluppo, quanto al successivo impiego pratico delle nuove tecnologie**. L'uso consapevole e responsabile dell'IA richiede un quadro solido di principi che metta al centro la sicurezza, l'autonomia decisionale dell'uomo, il rispetto dei diritti fondamentali. La protezione dei dati personali è una componente essenziale di questo quadro in quanto "*è stata vista da sempre come uno strumento per promuovere uno sviluppo tecnologico responsabile nell'ottica del bene comune*"[7].

Per molti aspetti l'insieme di regole e garanzie consolidato in ambito privacy ha anticipato le istanze di tutela poi rese più evidenti dall'avvento dell'IA e incorporate a livello europeo nell'AI Act (in particolare mediante la lista nera dei sistemi vietati, la previsione di obblighi informativi nei casi di processi decisionali basati su IA e con impatto sulle persone, le prescrizioni sulla trasparenza per determinati sistemi di IA che possono indurre in errore le persone) e a livello nazionale nella legge n. 132/2025. Ne è riprova **l'attenzione che, nel tempo, il Garante per la protezione dei dati personali ha dedicato alle implicazioni e alle ricadute dell'intelligenza artificiale,** analizzando fenomeni quali i deepfake, il ruolo degli assistenti digitali, il social scoring, così come le applicazioni dell'IA in chiave di contrasto all'evasione fiscale, in ambito di polizia predittiva o nel contesto sanitario, e più recentemente sanzionando violazioni del GDPR da parte di imprese che forniscono servizi di IA generativa basati su Large Language Models. Emblematico il caso delle applicazioni di IA generativa che consentono la 'nudificazione': a fine 2025 il Garante si è attivato per bloccare tali applicazioni in ragione della violazione dei principi del GDPR, sottolineando nel provvedimento le gravi ripercussioni sulla dignità e la riservatezza della persona, anche tenuto conto che le immagini artefatte possono riguardare soggetti minori di età; a breve distanza di tempo il legislatore europeo ha integrato l'AI Act con un divieto esplicito che investe l'immissione sul mercato e l'uso di sistemi di IA che generano o manipolano immagini, video e audio intimi non consensuali e contenuti di abuso sessuale su minori.

Lo scenario è però in **continua evoluzione** e ogni conquista della tecnologia mette alla prova l'efficacia del sistema, la sua capacità di intercettare i nuovi rischi e trovare soluzioni a problemi concreti. L'**IA agentica** ad esempio sta facendo emergere problemi inediti, per il fatto che gli agenti, da soli o in combinazione, possono pianificare strategie ed eseguire operazioni per giungere al risultato assegnato al di fuori di istruzioni di programmazione, anche sfruttando vulnerabilità informatiche, violando e scambiando dati riservati, realizzando profilazione invasiva e assumendo decisioni in ultima analisi discriminatorie.

Per quanto riguarda la fase di sviluppo dei modelli e sistemi, **un fronte a cui prestare attenzione è quello delle modalità di reperimento dei dati** e, in stretta connessione, dell'individuazione della corretta base giuridica per potervi procedere. L'IA è notoriamente una tecnologia *data hungry*: la disponibilità di ampi dataset è indispensabile per addestrare modelli e sistemi, ottenere il miglioramento progressivo delle loro prestazioni e affinare l'accuratezza degli output. La possibilità di invocare il legittimo interesse per giustificare il trattamento dei dati personali nel contesto dell'addestramento è un'opzione ragionevole purché siano integrati i presupposti previsti dal GDPR e progressivamente puntualizzati dalla prassi e dalla giurisprudenza.

Il tema assume un rilievo particolare con riferimento all'impiego dei dati ricavati da una fonte praticamente inesauribile e facilmente accessibile, quale il web, che ha svolto e svolge tuttora un ruolo determinante nell'evoluzione della tecnologia, specialmente per i sistemi di IA di tipo generativo. Il ricorso al ***web scraping*** – tramite software che scandagliano continuamente la rete effettuando la raccolta massiva e l'estrazione automatica di dati – **solleva interrogativi delicati sul piano della protezione dei dati personali** che possono essere coinvolti nel 'rastrellamento'. Premessa fondamentale è che la mera circostanza che dei dati personali siano disponibili pubblicamente online non implica un consenso implicito degli interessati alla loro utilizzazione e, quindi, non legittima di per sé la loro acquisizione e il loro impiego da parte di terzi. Chi, ad esempio, condivide post o contenuti sui social media lo fa ragionevolmente per coltivare relazioni, interagire, manifestare opinioni e non per alimentare dataset di addestramento dell'intelligenza artificiale.

Nel parere n. 28/2024 e nelle Linee guida 3/2026 l'EDPB ha utilmente chiarito le condizioni che devono essere soddisfatte per avvalersi del legittimo interesse con riferimento all'IA, alla luce del criterio del bilanciamento sancito dal GDPR e secondo una valutazione in tre passaggi: sussistenza di un interesse lecito, chiaro e preciso, reale, riferibile al titolare del trattamento o ad altri soggetti (quale potrebbe essere ad esempio l'interesse a realizzare un agente conversazionale per l'assistenza agli utenti, a sviluppare un sistema per il riconoscimento di contenuti o comportamenti frau-

7. Privacy 2030: una nuova visione per l'Europa - Il manifesto del pensiero di Giovanni Buttarelli pubblicato dal Garante italiano insieme a IAPP, 2020, pag. 13.

dolenti, a migliorare il rilevamento delle minacce in un sistema informatico); assenza di alternative che permettano di giungere al risultato in modo altrettanto efficace, ma con minore impatto sulle persone, in particolare riducendo la quantità di dati trattati; adozione di opportune misure di attenuazione dei rischi, inclusi filtri di tipo tecnico nell'acquisizione dei dati, a salvaguardia dei diritti fondamentali coinvolti. La preoccupazione è che il *web scraping* possa generare una sensazione di sorveglianza che inciderebbe negativamente sulla libertà di espressione *online* (con una sorta di '*chilling effect*') e sulla fiducia nell'ambiente digitale. Ne consegue, d'altra parte, che tutti i gestori di siti internet e di piattaforme online sono chiamati ad attrezzarsi per prevenire o mitigare la raccolta dei dati personali disponibili online da parte di terzi che intendano addestrare l'IA generativa: sul tema, in funzione di ausilio alla compliance, si segnala la Nota informativa pubblicata dal Garante in materia di *web scraping*, che indica le possibili misure di cautela da implementare (a seconda dei casi di tipo tecnico o legale).

Il tema di come assicurare la qualità dei dati di addestramento dell'IA e la conformità alla normativa in materia di protezione dei dati personali è affrontato nel regolamento europeo sull'intelligenza artificiale (AI Act)[8] con riferimento ai sistemi di IA ad alto rischio. Il legislatore europeo prescrive ai fornitori di tali sistemi l'adozione di misure di governance e gestione dei dati adeguate, che riguardano i processi di raccolta dei dati, le operazioni – quali etichettatura, pulizia, aggiornamento, arricchimento, aggregazione – di preparazione dei dati, la formulazione di ipotesi, la valutazione dell'adeguatezza dei dataset disponibili, l'individuazione di eventuali bias potenzialmente pregiudizievoli nei confronti delle persone e dei modi per attenuarli. Viene specificato che, se sono coinvolti dati personali, deve essere assicurata l'osservanza dei principi di minimizzazione e di *privacy by design* e *by default*, anche con tecniche di anonimizzazione e cifratura o tecnologie che consentano di addestrare i sistemi senza trasmissione tra le parti o copia dei dati grezzi o strutturati. Il regolamento si preoccupa inoltre di stabilire le condizioni alle quali è eccezionalmente ammesso il trattamento dei dati personali che rientrano nelle categorie particolari di cui al GDPR ai fini del rilevamento e della correzione delle distorsioni e indica le garanzie da implementare (misure di sicurezza, controllo degli accessi, preclusione del trasferimento a terzi ecc.). La deroga, inizialmente prevista per i soli fornitori di sistemi di IA ad alto rischio, è stata estesa dal Digital Omnibus anche ai *deployer* di sistemi di IA ad alto rischio, nonché ai fornitori e *deployer* di altri sistemi e modelli di IA. Vi è quindi, da parte del legislatore, il riconoscimento dell'importanza della finalità (evitare i bias) e il tentativo di trovare il giusto equilibrio con la tutela delle persone sempre nel segno della necessità e proporzionalità.

Anche **l'utilizzo dei sistemi di IA** comporta potenziali frizioni con la tutela dei diritti fondamentali e della privacy in particolare. Tra i rischi maggiori vi sono quelli connessi agli **algoritmi di profilazione** e al ruolo che possono avere nell'influenzare valutazioni o decisioni con impatto sulla vita e i diritti fondamentali delle persone, specialmente in ragione della mancanza di accuratezza dei dataset utilizzati nell'addestramento e della **presenza di errori o pregiudizi suscettibili di compromettere l'affidabilità dei risultati e di produrre o perpetuare discriminazioni**. Inoltre, la capacità inferenziale che contraddistingue i sistemi di IA fa sì che, partendo da determinati dati, l'algoritmo possa dedurre informazioni sulla persona e attribuire alla stessa caratteristiche, qualità, interessi o comportamenti legati alla sua sfera più intima e bisognosa di riservatezza.

La cornice normativa in materia di intelligenza artificiale di cui l'Italia si è dotata con la **legge n. 132/2025** è ispirata alla duplice finalità di cogliere le opportunità delle nuove tecnologie e, in via complementare, garantire "la vigilanza sui rischi economici e sociali" e sull'impatto che l'IA produce sui diritti fondamentali. In questa prospettiva, la legge individua i criteri per un adeguato contemperamento tra le istanze in gioco facendo leva sui **principi** di correttezza, attendibilità, sicurezza, qualità, appropriatezza e trasparenza dei dati e dei processi. Inoltre, in linea con le previsioni del GDPR in materia di decisioni automatizzate, la legge prescrive che sistemi e modelli di IA vengano sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza e della spiegabilità, in funzione della **sorveglianza e dell'intervento umano** (*human in the loop*).

La **continuità con il GDPR** trova esplicito fondamento nella previsione per la quale l'utilizzo di sistemi di IA deve garantire la liceità, la correttezza e la trasparenza del trattamento dei dati personali, nonché la compatibilità del trattamento con le finalità per le quali i dati sono stati raccolti, in conformità con il diritto UE in materia di protezione dei dati personali e tutela della riservatezza. In questo contesto, la trasparenza implica che le informazioni e le comunicazioni relative al trattamento dei dati nell'ambito dell'utilizzo di IA debbano essere "rese con linguaggio chiaro e semplice, in modo da garantire all'utente la conoscibilità dei relativi rischi e il diritto di opporsi ai trattamenti autorizzati dei propri dati personali". Viene così rafforzata la tutela dell'individuo che, nell'avvalersi da 'utente' delle tecnologie di IA, deve essere posto in condizione di valutare i potenziali pregiudizi anche per la protezione dei dati e la riservatezza e assumere le conseguenti determinazioni, compresa la scelta di opporsi a un trattamento legittimamente svolto.

8. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2014 che stabilisce regole armonizzate sull'intelligenza artificiale.

Se il quadro di regole appare complessivamente definito (tenendo conto del duplice livello nazionale ed europeo e fatti salvi gli aggiustamenti e le semplificazioni che possono essere valutati sulla base di un'analisi di impatto *ex post*, per aumentare la coerenza ed evitare sovrapposizioni normative), la questione si sposta sul piano dell'applicazione. Si tratta in particolare di **declinare in concreto i principi di trasparenza e spiegabilità**, superando l'opacità tipica della '*black box*' e riequilibrando la situazione di asimmetria informativa in cui versa l'individuo, e di **identificare le modalità per consentire all'interessato l'esercizio dei suoi diritti** (accesso, rettifica, cancellazione) a fronte di sistemi di intelligenza artificiale che si alimentano dei suoi dati personali. Su questi temi, in funzione di ausilio alla compliance, un ruolo chiave possono svolgere gli strumenti di *soft law*, in particolare sotto forma di Linee guida delle Autorità competenti adottate in consultazione con gli stakeholder.

4. Salvaguardare l'approccio regolatorio europeo e rafforzare la cooperazione

Alla luce delle sfide per la protezione dei dati personali legate alla trasformazione del contesto geopolitico e alla rapidità dell'evoluzione tecnologica assume rilievo centrale, come già accennato, la ricerca di un assetto regolatorio che garantisca sicurezza e sovranità digitale, non scoraggi la crescita economica e la competitività, restando al contempo solidamente radicato sui valori europei e sulla tutela dei diritti fondamentali.

La **normativa sulla privacy ha costituito l'architrave** per la successiva elaborazione delle regole europee che insistono sull'ecosistema digitale e sulle nuove tecnologie e un modello di riferimento per altri ordinamenti. La scelta di attribuire centralità alla persona, affermare la necessità della supervisione umana e richiedere una valutazione di impatto come presupposto delle misure di prevenzione dei rischi si ritrova oggi nell'AI Act. È sull'esistenza di regole comuni con queste caratteristiche che l'Unione europea può far leva per contribuire al dialogo necessario a livello internazionale su come "***disarmare l'IA***", secondo la potente espressione utilizzata dal Papa che "*non significa rinunciare alla tecnologia, ma impedirle di dominare l'umano. Significa sottrarla ai monopoli, renderla discutibile, contestabile, e quindi abitabile, restituendola alla pluralità delle culture umane e delle forme di vita*"[9].

L'impegno sembra ben chiaro alla Commissione europea, che ha dichiarato di voler continuare a "*promuovere il proprio approccio basato sui valori in materia di governance digitale e norme digitali al fine di plasmare una trasformazione digitale globale che sia antropocentrica, affidabile e rispetti i diritti umani e le libertà fondamentali. Agendo con decisione, l'UE può costituire una forza motrice di progressi tecnologici guidati in modo responsabile sulla scena mondiale*"[10].

Si tratta quindi di **proseguire con convinzione sulla strada della cooperazione internazionale**, coinvolgendo nelle sedi opportune i diversi attori dell'ecosistema digitale, in quanto solo una prospettiva globale e multistakeholder può consentire di affrontare le questioni complesse che vanno emergendo e i rischi di portata sistemica. Un risultato importante in questa direzione è rappresentato dalla **Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto**, il primo Trattato internazionale giuridicamente vincolante che fissa principi e obblighi generali relativi alle attività lungo l'intero ciclo di vita dei sistemi di IA con lo scopo di preservare efficacemente i valori condivisi dalle parti aderenti e sfruttare i vantaggi derivanti dall'intelligenza artificiale per la promozione di tali valori in modo da favorire un'innovazione responsabile[11]. L'approccio si pone in continuità con quello della Convenzione 108 del 1981 sulla protezione dei dati personali, che ha ricevuto nel tempo l'adesione di vari Paesi extra europei divenendo uno standard globale.

Nell'ambito del dibattito internazionale, un posto centrale occupa il **tema dell'educazione digitale**, come misura volta a consentire alle persone di avvicinarsi alle nuove tecnologie in maniera informata e consapevole, così da preservarne la capacità di autodeterminazione, ad esempio riguardo alla scelta di condivisione di dati personali. L'educazione digitale è essenziale sia per un'effettiva attuazione dei principi di trasparenza e spiegabilità dell'IA, sia per ridurre i divari culturali e cognitivi che possono tradursi in discriminazioni nell'accesso all'IA. In questa prospettiva, è significativo che la Convenzione del Consiglio d'Europa impegni le parti a incoraggiare e promuovere un'alfabetizzazione e delle competenze digitali adeguate per "**tutti i segmenti della popolazione**"[12].

La cooperazione è parola chiave anche riguardo all'attività di enforcement delle regole. Nell'UE, il **coordinamento tra le autorità competenti** all'applicazione del GDPR negli Stati membri appare ben strutturato, anche grazie all'importante **ruolo svolto dall'*European Data Protection Board***. In proposito, merita di essere ricordata l'istituzione di

9. Lettera enciclica Magnifica Humanitas, cit. par. 110.
10. Commissione europea, Una strategia digitale internazionale per l'Unione europea, JOIN(2025) 140 final.
11. Council of Europe Treaty Series (CETS) n. 225. La Convenzione è stata elaborata da un organismo intergovernativo, il Comitato sull'intelligenza artificiale, che ha riunito i 46 Stati membri del Consiglio d'Europa, l'Unione europea e 11 Stati non membri (tra cui Canada, Giappone, Israele e Stati Uniti) e a cui hanno partecipato anche rappresentanti del settore privato, della società civile e del mondo accademico. La Convenzione è stata aperta alla firma il 5 settembre 2024 a Vilnius. L'Unione europea, dopo l'approvazione da parte del Parlamento e del Consiglio, ha depositato la ratifica il 15 maggio 2026.
12. CETS n. 255, art. 20.

una Task Force on Generative AI Enforcement, incaricata di operare quale piattaforma per lo scambio di informazioni sulle indagini relative all'IA generativa allo scopo di rafforzare la cooperazione tra le autorità nazionali e assicurare la compliance con il GDPR. L'interazione e il confronto dovranno auspicabilmente estendersi alle altre autorità a vario titolo chiamate a vigilare sul rispetto della regolazione in materia digitale e di intelligenza artificiale.

Un analogo sforzo è richiesto **sul piano nazionale**. L'AI Act, nel disegnare un sistema di governance a due livelli (all'AI Office nell'ambito della Commissione europea sono riservati compiti di valutazione, monitoraggio e controllo della conformità dei modelli con finalità generali, mentre per il resto la vigilanza sul rispetto di obblighi e requisiti stabiliti dal regolamento è demandata ad autorità designate da ciascuno Stato membro) ha riconosciuto alle autorità garanti per la protezione dei dati personali una competenza specifica per un insieme di sistemi di IA ad alto rischio destinati a interferire con aspetti particolarmente sensibili della vita delle persone, quali i sistemi utilizzati per attività di contrasto dei reati, gestione delle frontiere, amministrazione della giustizia e dei processi democratici e quelli di tipo biometrico utilizzati a tali fini. In Italia la legge n. 132/2025, che ha designato come autorità di riferimento in materia di IA l'AgID (autorità di notifica) e l'ACN (autorità di vigilanza del mercato) e specificato, in conformità al regolamento europeo, la competenza del Garante per la protezione dei dati personali, richiede espressamente di **assicurare il coordinamento e la collaborazione tra le varie autorità designate, le altre pubbliche amministrazioni e le autorità indipendenti**, nonché "ogni opportuno raccordo tra loro per l'esercizio delle funzioni" previste dalla legge. L'esigenza di coordinamento risulta sempre più importante in un **contesto caratterizzato da una complessa stratificazione di norme relative alle tecnologie digitali**, che può pregiudicare la certezza giuridica e tradursi nella duplicazione di interventi da parte dei diversi *enforcers*. Il coordinamento operativo e informativo è inoltre necessario per assicurare **interventi rapidi e minimizzare gli impatti di eventuali violazioni**. La disponibilità al confronto e alla condivisione degli obiettivi sono il presupposto di una cooperazione efficace, che potrà essere disciplinata mediante protocolli di intesa e sviluppata in seno ad appositi comitati.

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

AGCM e tutela del consumatore ibrido

(di Sara Perugini[1])

Nel panorama socio-economico contemporaneo, l'atto del consumo ha smesso di configurarsi come una mera operazione di soddisfacimento di bisogni biologici o materiali e i luoghi fisici del mercato subiscono una riconfigurazione radicale: i punti vendita abbandonano la rigida funzione di spazi transazionali per farsi teatri narrativi ed esperienziali, dove il consumatore non acquista un oggetto, ma interiorizza un racconto e un vissuto emotivo. La transizione verso questa nuova cultura del consumo è accelerata dalla pervasività delle tecnologie digitali, che hanno definitivamente scardinato la tradizionale separazione lineare tra produzione e fruizione. La figura del consumatore passivo, terminale ultimo della catena del valore, cede il passo al prosumer (Toffler, 1980): un soggetto ibrido che si muove fluidamente in un ecosistema multicanale, destabilizzando i confini tra spazio online e offline.
Questa fluidità identitaria e comportamentale pone interrogativi complessi sotto il profilo del diritto. Il legislatore contemporaneo si trova nella condizione di dover tutelare un soggetto che, sebbene mantenga la vulnerabilità tipica della persona fisica di fronte a giganti tecnologici e algoritmi predittivi, esercita al contempo un potere di influenza e produzione mai registrato prima. Una asimmetria informativa e negoziale evoluta che le recenti strategie regolamentari dell'Unione Europea tentano di intercettare. In tale contesto, l'AGCM ricopre un ruolo centrale esercitando la propria azione di enforcement in modo dinamico e proattivo.

SOMMARIO: 1. Premessa – 2. Il quadro normativo di riferimento: cenni – 3. utilizzo delle tecnologie digitali e consapevolezza ambientale: l'azione dell'AGCM a tutela del consumatore ibrido – 4. Considerazioni conclusive

1. Premessa

In un contesto caratterizzato da una nuova cultura del consumo dove i prodotti e le marche non soddisfano più solo bisogni materiali, ma agiscono come veri e propri strumenti di comunicazione e costruzione dell'identità personale[2] e gli spazi di vendita tendono a trasformarsi in ambienti esperienziali e narrativi, il rapporto di consumo tradizionalmente inteso si è evoluto.
A differenza del passato, la persona fisica "*che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta*"[3] si muove fluidamente tra esperienze *online* e *offline* e, talvolta, assume il ruolo di produttore e consumatore insieme, il c.d. *prosumer*[4] partecipando attivamente alla realizzazione di prodotti, servizi e contenuti.
Il pubblico non è più considerato un destinatario passivo, ma un soggetto attivo coinvolto in processi di partecipazione, interazione e co-creazione, dando origine a una nuova figura, il consumatore ibrido che, non a caso, è posto al centro delle recenti strategie giuridiche e regolamentari.
Per rispondere alle vulnerabilità di questa figura ibrida il legislatore europeo ha difatti introdotto e aggiornato diversi testi legislativi che formano una fitta rete di protezione ridisegnando il diritto dei consumi secondo un approccio integrato e aggiornato, che coniuga i principi tradizionali di protezione contrattuale con nuove norme su trasparenza, dati e responsabilità delle piattaforme e rivedendo il modello precedente fondato sulla netta separazione tra settori e canali di vendita.
Un cantiere normativo euro-unitario al quale si accompagna, al contempo, una intensificazione dell'azione dell'Auto-

1. Le opinioni dell'autrice non impegnano l'Istituzione cui appartiene.
2. Come teorizzato dal sociologo Jean Baudrillard e successivamente amplificato dalle dinamiche della post-modernità, i beni e i marchi operano oggi come veri e propri "sistemi di segni". Il prodotto non si esaurisce nel suo valore d'uso, ma si trasforma in un vettore comunicativo attraverso il quale l'individuo proietta, costruisce e negozia la propria identità personale e sociale.
3. Cfr. art. 3, lett. a) del Codice del Consumo.
4. Emblematico in tal senso il caso di chi produce energia con pannelli solari e la immette in rete o di chi più semplicemente, pur non svolgendo una attività professionale, trae un vantaggio economico da uno specifico modello di business come il modello piramidale (Cfr. Corte di Giustizia, sentenza dell'8 giugno 2023, causa C-455/21, Lyoness Europe) o da una singola transazione a patto che non svolga una attività professionale stabile (Cfr. Corte di Giustizia, Sentenza del 24 ottobre 2024, causa C- 347/23 Zabitoń).

rità Garante della Concorrenza e del Mercato che, chiamata ad applicare molte delle novellate disposizioni, interpreta il proprio ruolo in modo propulsivo guardando alle discipline di sua competenza più tradizionali, da specole inedite. In questa sede, si farà pertanto riferimento, distintamente, tanto agli sviluppi legislativi intervenuti più di recente che alla prassi applicativa dell'Autorità per come, in sede di *public enforcement*, è andata consolidandosi.

2. Il quadro normativo di riferimento: cenni

Nell'ambito della transazione digitale ed ecologica la tutela del *consumatore ibrido* passa attraverso una evoluzione del diritto dei consumatori che si concentra, essenzialmente, su tre macro-aree: la tutela del valore economico dei dati personali rilasciati durante i servizi "gratuiti", assicurando che il consenso non sia estorto o manipolato, introdotta dalla Direttiva n. 2019/2161/UE (c.d. *Direttiva Omnibus*)[5] che, nel modernizzare le regole di protezione dei consumatori per adeguarle all'era digitale, ha completato il percorso di ampliamento del raggio di applicazione del diritto dei consumi intrapreso dalla Direttiva 2019/770/UE (c.d. *Digital Content and Services*); il divieto dei *dark patterns*[6] previsto dal *Digital Services Act* (DSA) che regola la responsabilità delle grandi piattaforme[7] e la trasparenza algoritmica intesa come protezione del consumatore da interfacce web ingannevoli progettate per manipolare le scelte d'acquisto mediante l'uso di sistemi di intelligenza artificiale vietate dall'*AI Act*[8]; il contrasto al *greenwashing* e all'obsolescenza programmata dei beni sanciti dalla Direttiva n. 2024/825/UE (c.d. Direttiva *Empowering* o EmpCo)[9] e, sempre in una prospettiva di circolarità dell'economia, la Direttiva 2024/1799/UE che promuove la riparazione dei beni[10].

La Direttiva *Empowering*, in particolare, recepita nell'ordinamento italiano dal Dlgs n. 30 del 20 febbraio 2026, apporta rilevanti integrazioni alle discipline in materia di pratiche commerciali scorrette e *consumer rights* poi confluite nel Codice del Consumo che incidono in maniera diretta sull'ambito di intervento dell'AGCM competente in materia.

La novella, in particolare, delinea con maggiore precisione l'oggetto delle comunicazioni ambientali, dei marchi di sostenibilità e delle caratteristiche ecologiche dei beni e introduce diverse modifiche di tipo sostanziale accomunate dall'obiettivo del legislatore di compiere progressi nella transizione verde e contribuire a modelli di consumo più sostenibili, rafforzando il livello di protezione dei consumatori e dell'ambiente[11].

Il cantiere normativo rimane, tuttavia, aperto. Il quadro descritto è infatti destinato ad essere integrato dal *Digital Fairness Act* (DFA) una imminente riforma prospettata dall'Europa per eliminare o quantomeno attenuare le nuove forme di danno che il digitale – in continuo mutamento – può portare ai consumatori. Il progetto legislativo, non ancora pubblico[12], rappresenta il punto di approdo di un "*fitness check*" delle principali direttive europee a tutela dei consumatori, avviato dalla Commissione europea nel 2022 che dovrebbe avere ad oggetto cinque principali aree grigie: i) l'estensione del divieto dei *dark pattern* previsto *Digital Services Act* per le grandi piattaforme a tutti gli operatori digitali B2C; ii) il *design* creato per creare dipendenza (il c.d. *design addictive*) nel quale rientrano lo *scroll* infinito, le notifiche *push* ottimizzate per massimizzare i ritorni, i sistemi di ricompensa mutuati dalla psicologia del gioco d'azzardo: tutte pratiche che portano i consumatori, in particolare i minori, a trascorrere più tempo e denaro *online* di quanto intendessero; iii) la profilazione e la pubblicità personalizzata e, in particolare, l'uso dei dati per sfruttare vulnerabilità individuali a fini commerciali (come i c.d. *prezzi dinamici* che cambiano in base al profilo dell'utente e alle

5. La Direttiva Omnibus ha stabilito espressamente il principio, già affermatosi in via di prassi sul piano nazionale, 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.

6. Il *Digital Services Act* definisce i *dark patterns* come interfacce che "deformano o alterano in modo consistente" la capacità dell'utente di prendere decisioni libere e informate, vietando alle piattaforme di progettare o organizzare le interfacce in modo da ingannare o manipolare l'utente o alterarne significativamente il comportamento di scelta. Cfr. inoltre OCSE, *Dark Commercial Patterns*, OECD Digital Economy Papers, October 2022 No. 336, p.8, che propone una definizione di *dark pattern* quali pratiche commerciali che utilizzano elementi di architettura delle scelte digitali, in particolare nelle interfacce utente online, che minano o compromettono l'autonomia, il processo decisionale o la libertà di scelta dei consumatori. I *dark pattern* spesso ingannano, costringono o manipolano i consumatori e sono suscettibili di causare loro un danno diretto o indiretto in vari modi, sebbene in molti casi possa risultare difficile o impossibile quantificare tale danno.

7. Cfr. Piattaforme digitali e consumatori il ruolo delle Autorità indipendenti, (a cura di) F. Bassan, Roma Tre Press, 2026.

8. Cfr. Reg. UE 2024/1689 del 13 giugno 2024 entrato in vigore il 1° agosto 2024 (AI Act). Per un'analisi Cfr. S. Perugini, Antitrust e tutela dei consumatori alla prova dell'AI, in Concorrenza tutela dei consumatori e AI, (a cura di) Carlo Edoardo Cazzato e Francesco di Giorgi, Giuffrè, 2026.

9. L'intervento euro-unitario dà seguito al Green Deal europeo e rientra tra le iniziative previste dall'Agenda dei consumatori 2020. La Direttiva avrebbe dovuto essere integrato dalla proposta di Direttiva 2023/0085, (c.d. "Green Claims Directive"), sull'attestazione e la comunicazione delle asserzioni ambientali esplicite intrapresa per definire gli elementi minimi richiesti alle imprese, assicurare attendibilità, trasparenza e comparabilità alle proprie asserzioni ambientali. Dopo due anni di iter legislativo e intensi negoziati, tuttavia, il 20 giugno 2025 la Commissione Europea ha comunicato l'intenzione di ritirare il provvedimento mentre il 23 giugno 2025 il Consiglio UE ha bloccato l'ultima fase del "trilogo", lasciando quindi incerti i prossimi passi.

10. La Direttiva è stata recentemente attuata nell'ordinamento italiano dal D.lgs. 25 settembre 2026, n. 176.

11. In estrema sintesi dallo scorso 27 settembre, è espressamente vietato utilizzare sulle confezioni o nelle pubblicità termini vaghi come "green", "eco-friendly", "sostenibile", "biodegradabile" o "amico dell'ambiente" se l'azienda non è in grado di dimostrare un'eccellenza riconosciuta nelle prestazioni ambientali; non è più consentito esibire marchi o bollini di sostenibilità autocertificati o creati dai reparti marketing aziendali in quanto sono ammessi solo marchi basati su sistemi di certificazione ufficiali o istituiti da autorità pubbliche; le aziende non possono più fare promesse future vaghe (es. "Saremo a impatto zero entro il 2030"). Tali dichiarazioni sono lecite solo se accompagnate da un piano di attuazione dettagliato, pubblico, con scadenze precise, obiettivi misurabili e periodicamente verificati da un terzo indipendente. Per una analisi cfr. S. Perugini, La Disciplina del Greenwashing: profili introduttivi, in Contratti dei consumatori, a cura di E. Cazzato, corso di pubblicazione.

12. La proposta formale dovrebbe arrivare tra ottobre e dicembre 2026 con l'adozione definitiva attesa entro la fine del prossimo anno.

offerte calibrate su momenti di fragilità emotiva); iv) l'armonizzazione delle regole che governano il *marketing degli influencer*, e sulle relative collaborazioni commerciali, oggi gestite in modo disomogeneo tra i ventisette Stati membri; v) le *trappole sugli abbonamenti* ossia i flussi di cancellazione intenzionalmente labirintici, i rinnovi automatici poco trasparenti, i prezzi che cambiano dopo il periodo promozionale senza notifica adeguata.

3. Utilizzo delle tecnologie digitali e consapevolezza ambientale: l'azione dell'AGCM a tutela del consumatore ibrido

Gli interventi normativi accennati muovono da una comune matrice: la scelta commerciale del consumatore *ibrido* non si fonda più solo sul binomio prezzo-qualità, ma sulla combinazione tra consapevolezza ambientale e utilizzo avanzato delle tecnologie digitali[13], due versanti sui quali, non a caso, si concentra parte dell'attività di *enforcement* dell'AGCM in ambito consumeristico.

Invero, nel più ampio quadro dell'attenzione verso i *mercati digitali*, negli ultimi mesi l'Autorità ha indirizzato la propria azione sui servizi di intelligenza artificiale generativa[14], entrati nell'uso quotidiano di milioni di utenti e sulle modalità con cui le interfacce digitali e le tecniche di comunicazione *online* possono orientare le scelte del consumatore.

Come noto, la personalizzazione eccessiva delle interfacce e l'uso di strategie persuasive basate su profilazioni comportamentali possono compromettere la libertà negoziale del consumatore e, più in generale, il corretto funzionamento del mercato.

Emblematico, in tal senso, è il ricorso a tecniche di *neuromarketing* algoritmico, una delle espressioni più avanzate dell'evoluzione dell'AI applicata al mercato. Tali tecniche, che si fondano sull'analisi delle risposte neurofisiologiche dei consumatori, permettono di modulare i contenuti e le offerte in base agli stimoli cerebrali, orientando le decisioni di consumo con livelli di efficacia persuasiva senza precedenti.

L'attenzione degli interpreti si è andata, quindi, concentrando intorno alla necessità di garantire anche un adeguato livello di consapevolezza per gli utenti circa la fallibilità dei risultati offerti dalle elaborazioni creative generate tramite l'AI, con un richiamo insistito alla verifica delle fonti (i c.d. *data set*) utilizzati per "addestrare" le piattaforme.

In questa prospettiva va letta l'azione condotta dall'Autorità per contrastare il fenomeno delle *allucinazioni* che possono essere generate nei processi di intelligenza artificiale, situazioni cioè in cui, a fronte di un dato *input*, vengono generati *outputs* contenenti informazioni inesatte, fuorvianti o inventate.

Sono stati in particolare chiusi tre procedimenti nei confronti di fornitori di sistemi di intelligenza artificiale - le società che sviluppano e gestiscono il sistema di IA denominato DeepSeek[15] e le *start up* Mistral[16] e Nova[17] - che, a differenza di quanto viene tipicamente fatto da altre piattaforme, omettevano di informare gli utenti di questo rischio.

Le istruttorie, concluse mediante impegni di natura *strutturale*, restituiscono l'immagine di modelli generativi che incorporano un rischio intrinseco di produzione di risultati inaccurati o addirittura inesistenti o inventati: se l'utente medio tende infatti a percepire i contenuti generati come corrispondenti alla realtà o comunque corretti, l'asimmetria conoscitiva relativa ai limiti tecnici del modello può tradursi in una pratica ingannevole quando le informazioni sulle allucinazioni risultino assenti, generiche o comunque inadeguate.

Gli impegni accolti nei procedimenti delineano, sul piano della *compliance*, un nucleo minimo di obblighi organizzativi e informativi per i servizi di AI finalizzato a rafforzare la trasparenza informativa sul rischio di "allucinazioni" dei sistemi offerti, intervenendo sui canali di fruizione dei servizi (siti internet e app) e nelle varie fasi del processo decisionale che precede l'acquisto o la registrazione mediante: l'introduzione di *disclaimer* ***permanenti nelle interfacce di utilizzo sotto le*** *chat* ***che avvertono, in lingua italiana, della presenza delle allucinazioni, anche con*** *hyperlink* ***dedicati; l'integrazione dell'informativa precontrattuale con esplicite avvertenze sui limiti di affidabilità dei contenuti generati e sulla necessità di verificarli***[18].

L'assunto che se ne può trarre è quello secondo cui nel caso di un servizio di IA generativa, l'utente-consumatore deve essere posto nelle condizioni di comprendere le caratteristiche essenziali del servizio, incluse le sue limitazioni, quando

13. Lo stretto legame che corre tra tecnologia e protezione dell'ambiente viene evidenziato nelle pagine di F. Bassan, L'era ibrida, sovranità e democrazia tra poteri pubblici e imprese tech, Catanzaro, 2026.
14. I sistemi di intelligenza artificiale generativa sono ormai entrati nell'uso quotidiano di milioni di utenti. Strumenti come *ChatGPT*, *Claude* o *Copilot* vengono utilizzati per redigere testi, cercare informazioni, ottenere suggerimenti, pianificare attività o ricevere indicazioni su questioni anche delicate. La loro forza sta nella capacità di produrre risposte articolate, fluide e spesso apparentemente autorevoli. Proprio questa caratteristica, tuttavia, rende particolarmente insidioso uno dei loro limiti più noti: la possibilità di generare contenuti inesatti, fuorvianti o inventati.
15. Cfr. provv. n. 31784, del 16 dicembre 2025, PS12942, in Boll. 1/2026.
16. Cfr. provv. n. 31864, del 17 febbraio 2026, PS12968, in Boll. 10/2026.
17. Cfr. provv. n. 31935, del 21 aprile 2026, PS12973, in Boll. 18/2026.
18. Nel procedimento chiuso nei confronti di DeepSeek, la società ha anche previsto un investimento tecnologico per mitigare il fenomeno delle "allucinazioni" e, negli impegni relativi a NOVA AI, è stato anche chiarito al consumatore che si tratta di un servizio che offre solo accesso, mediante un'unica interfaccia, ad alcune chatbot (delle quali sono stati dati maggiori dettagli), senza fornire un servizio di aggregazione e di elaborazione delle risposte.

queste possono incidere sulla scelta di utilizzarlo, registrarsi, acquistare funzionalità ulteriori o fare affidamento sulle risposte ricevute.
Invero, la crescente attenzione dell'Autorità verso le modalità con cui le interfacce digitali e le tecniche di comunicazione *online* possono orientare le scelte del consumatore si coglie anche da altri due interventi concernenti due tecniche, apparentemente differenti, i *countdown* promozionali[19] e il *clickbaiting*[20], accomunate dalla capacità di orientare il comportamento del consumatore attraverso il *design* dell'interfaccia e le modalità di fruizione dei contenuti.
Nell'ambito del primo procedimento concluso nei confronti di una società operante nel settore dell'*e-commerce*, l'Autorità ha esaminato l'utilizzo di *countdown* promozionali che, pur presentati come limitati nel tempo, venivano sistematicamente reiterati alle medesime condizioni economiche. Il meccanismo è stato sanzionato in violazione dell'art. 23, co. 1 lett. g) Cod. Cons.[21] in quanto integrante uno strumento che, facendo leva su meccanismi cognitivi, induceva l'utente a ritenere l'offerta prossima alla scadenza, orientandone così la scelta: un *dark pattern* idoneo a creare un artificiale senso di urgenza, inducendo il consumatore ad assumere una decisione commerciale più rapidamente di quanto avrebbe fatto in assenza di tale pressione.
Diverso, ma per certi aspetti complementare, è il secondo provvedimento, riguardante il ricorso da parte di una testata giornalistica *online* a tecniche di *clickbaiting*, una strategia di comunicazione digitale adottata da *news outlets* (testate giornalistiche, blog, canali di informazione etc.) caratterizzata essenzialmente dall'utilizzo di titoli sensazionalistici e accattivanti, volti a catturare l'attenzione del lettore mediante formule enfatiche e sensazionalistiche, per indurlo a cliccare sul relativo articolo, il quale si rivela poi, a seguito di lettura, non conforme al titolo, o addirittura privo di un reale contenuto informativo.
La condotta è stata assimilata a un *dark pattern*: come in essi, le architetture della scelta adottate dai professionisti al fine di amplificare il numero delle visualizzazioni e aumentare, di conseguenza, il valore dello spazio pubblicitario offerto agli inserzionisti, comportano un pregiudizio per i consumatori soprattutto in termini di riservatezza dei dati e scelta relativa al tempo da dedicare alla fruizione di un determinato servizio.
La pratica è stata qualificata sia come ingannevole, per la falsa aspettativa generata dal titolo, sia come aggressiva, in quanto la progettazione della pagina induceva l'utente a permanere sul sito più a lungo di quanto avrebbe liberamente scelto.
Sul secondo versante, quello della consapevolezza ambientale, l'esperienza applicativa dell'AGCM, antecedente alla riforma introdotta dal D.lgs. 30/2026, appare particolarmente emblematica del contributo fornito dal *public enforcement* al processo di transizione verso un'economia maggiormente sostenibile.
In numerose occasioni, l'Autorità ha sanzionato l'utilizzo scorretto di *green claims* nei diversi settori del mercato, contestando l'ingannevolezza dei vanti ambientali sfruttati dalle imprese laddove non supportati da studi o evidenze reali ed oggettive.
Risale al 2009, uno dei primi interventi adottato nel settore delle acque minerali, concernente *green claims* ingannevoli relativi alla quantità di plastica utilizzata come "eco-friendly" o "Impatto Zero" in quanto prive di evidenze documentali o fattuali[22].
Nel 2016, l'Autorità ha sanzionato la casa automobilistica Volkswagen per aver commercializzato in Italia autoveicoli e veicoli commerciali con emissioni inquinanti non conformi a quanto dichiarato in sede di omologazione e per aver diffuso successivamente messaggi pubblicitari "*in relazione ai vanti ecologici e alle indicazioni circa la conformità degli stessi ai parametri concernenti le emissioni inquinanti e ambientali*"[23].
Più di recente, nel 2024, l'Autorità ha condotto numerose istruttorie in materia e intrapreso iniziative di *moral suasion* al fine di contrastare l'uso scorretto delle dichiarazioni ambientali invitando alcune imprese operanti nel settore dell'energia elettrica e nel settore automobilistico a eliminare asserzioni ambientali non chiare o formulate in termini del tutto assoluti e generici.
Nel febbraio 2025 nel settore delle spedizioni, l'Autorità ha sanzionato diverse società, facenti capo al gruppo Gls, per aver sviluppato un programma di sostenibilità ambientale servendosi, sul sito web di riferimento, di asserzioni ambientali ambigue e non verificabili e per aver obbligato i clienti abbonati a aderire al suddetto programma corrispondendo un importo, a prescindere dalla verifica dei costi, al fine di ottenere un certificato non richiesto relativo all'avvenuta

---

19. Cfr. provv. n. 31999, del 23 giugno 2026, PS13027, in *Boll.* 26/2026.
20. Cfr. provv. n. 31995, del 9 giugno 2026, PS13016, in Boll. 26/2026.
21. Si considera pratica commerciale in ogni caso ingannevole ai sensi dell'art. 23, co. 1 lett. g) Cod. Cons. «dichiarare, contrariamente al vero, che il prodotto sarà disponibile solo per un periodo molto limitato o che sarà disponibile solo a condizioni particolari per un periodo di tempo molto limitato, in modo da ottenere una decisione immediata e privare i consumatori della possibilità o del tempo sufficiente per prendere una decisione consapevole».
22. Cfr. provv. n. 20559, del 10 dicembre 2009, PS4026, in Boll. n. 52/2009; provv. n. 23278, dell'8 febbraio 2012, PS7235, in Boll. n. 6/2012; provv. del 14 novembre 2012, n. 24046, PS6302, in Boll. n. 46/2012.
23. Cfr. provv. n. 26137, del 4 agosto 2016, PS10211, in Boll. n. 28/2016.

compensazione delle emissioni di CO2 connesse alle spedizioni.
Si pensi ancora al procedimento concluso nel settore dell'abbigliamento con riferimento al modello del *fast* e *superfast fashion* utilizzato da un noto sito di compravendita *online*, dove l'intervento dell'Autorità è risultato utile a contrastare l'utilizzo di dichiarazioni ambientali ambigue o presentate in modo non chiaro, con diretto pregiudizio dei consumatori[24].
Una prassi che ha il merito di aver in gran parte anticipato il contenuto della riforma cui si accennava.

4. Considerazioni conclusive

Le conclusioni che possono trarsi dalla breve analisi che precede sono essenzialmente due. In primo luogo, il complesso *framework* normativo che emerge in queste pagine testimonia la sussistenza di una convergenza degli interventi normativi verso una sempre maggiore valorizzazione del ruolo centrale degli operatori economici per il corretto andamento del mercato. Si pensi, da un lato, sul versante della consapevolezza ambientale, alla normativa diretta a contrastare il *greenwashing* e l'obsolescenza programmata dei beni, mediante una responsabilizzazione degli operatori economici in relazione a tutte le fasi del rapporto di consumo e lungo tutta la catena di distribuzione; dall'altro, in ambito digitale, alla responsabilità delle grandi piattaforme introdotta dal *Digital Service Act* e alla previsione di una sua prossima estensione soggettiva contenuta nel *Digital Fairness Act*.
In secondo luogo, in sede di *enforcement*, la lettura congiunta degli ultimi provvedimenti adottati in ambito digitale, mostra come l'AGCM guardi sempre di più non soltanto al contenuto del messaggio commerciale, ma anche al modo in cui esso viene costruito e presentato. I *dark pattners*, i c*ountdown* promozionali e *clickbaiting* rappresentano tecniche differenti, ma accomunate dalla capacità di orientare il comportamento del consumatore attraverso il *design* dell'interfaccia e le modalità di fruizione dei contenuti.
Una prassi che conferma la valorizzazione da parte dell'Autorità di una lettura evolutiva delle tradizionali disposizioni del Codice e al tempo stesso la capacità di saper cogliere una delle principali sfide poste dalle nuove modalità di interazione tra professionisti e consumatori: saper fluttuare insieme al consumatore, garantendo spazi di libertà, espressione e co-creazione senza che questi si traducano in nuove forme di sfruttamento digitale o in vuoti di tutela giuridica.

24. Cfr. provv. n. 31639, del 29 luglio 2025, PS12709, in Boll. n. 30/2025.

COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA

LA TUTELA DELL'INVESTITORE RETAIL VERSO IL 2030: DIGITALIZZAZIONE DEI MERCATI, METAMORFOSI DELLE INFRASTRUTTURE E NUOVE SFIDE PER LA VIGILANZA

(di Matteo Ghezzi)

SOMMARIO: 1. Premessa. – 2. Dall'intermediazione finanziaria tradizionale alle piattaforme di trading: nuove modalità di accesso al mercato dell'investitore retail – 3. La metamorfosi delle infrastrutture: blockchain e cryptoassets. – 4. I fattori di rischio connessi alla digitalizzazione delle infrastrutture e nuove forme di tutela. – 5. Verso un'agenda CONSOB 2030: consolidamento di una vigilanza data-driven e multilivello.

1. Premessa

Il mercato finanziario nel quale è destinato a operare il risparmiatore-investitore *retail* 2030 sarà contrassegnato da metamorfosi già oggi in atto[1], destinate nei prossimi anni a consolidarsi e a incidere in misura crescente sulla posizione dell'investitore al dettaglio.

Cruciale fattore di trasformazione è costituito dall'innovazione tecnologica, il cui impatto si riverbera su una pluralità di livelli nel settore finanziario[2]; in primo luogo, sui prodotti e sui servizi disponibili, poi sulle modalità di accesso al mercato dell'investitore *retail* e sulle infrastrutture destinate ad ospitare gli scambi, nonché, infine, sulla stessa architettura dell'ecosistema digitale nel quale viene assunta la decisione di investimento.

La diffusione delle piattaforme di *trading*, come si vedrà nel prosieguo, favorisce una partecipazione più diretta dell'investitore *retail* ai mercati e lo sviluppo di forme di investimento sempre più "in prima persona". Ne deriva una parziale attenuazione della tradizionale relazione con l'intermediario, accompagnata dalla riduzione dei relativi costi di accesso e dalla crescente centralità dell'interazione dell'investitore con la piattaforma e la relativa interfaccia digitale[3].

A ciò si aggiungono metamorfosi ancora più profonde, inerenti le stesse infrastrutture sulle quali gli scambi finanziari possono svolgersi. In tale prospettiva, si colloca lo sviluppo della *blockchain*, le cui evoluzioni saranno discusse nel prosieguo.

Tuttavia, l'innovazione infrastrutturale costituisce soltanto una manifestazione della trasformazione di cui trattasi. La maggiore facilità di accesso ai mercati espone infatti l'investitore a rischi connaturati alla stessa progettazione dell'ambiente digitale: *dark patterns*, *gamification* e forme di personalizzazione manipolativa possono sfruttare le vulnerabilità cognitive e comportamentali dell'utente e incidere sulla concreta formazione delle decisioni di investimento[4].

---

1. Per una ricognizione delle metamorfosi del mercato finanziario, si v. i contributi contenuti in A. Sacco Ginevri, (a cura di), Princìpi di riforma del Testo unico della finanza, Giuffrè, Milano, 2026.

2. Già F. Annunziata, Retail Investment Strategy. How to Boost Retail Investors' Participation in Financial Markets, Policy Department for Economic, Scientific and Quality of Life Policies, Commissione ECON, Parlamento Europeo, Lussemburgo, 2023, 22 evidenziava quanto segue: "Digitalisation of financial markets has been steadily increasing over the past years, including in the area of investment services. According to the Report, for instance: "Some 14% of respondents stated that they had received digital advice. When asked about the more granular sources of advice, we see that 12% say they received advice or guidance through a robo-advisor, web-comparator or equivalent. In other words, while digital advice (or digital means to search and select products) still concerns a minority, it is not negligible, as today more than 1 in 10 investors/aspiring investors use it. The share of consumers using digital sources to select products is particularly high in Poland (22%) and Romania (19%), while it is low in Italy (7%)". Anche F. Annunziata, Fintech: tra infrastrutture tecnologiche e intelligenza artificiale, in Quaderni di Ricerca Giuridica, Banca d'Italia, 2024, p. 265 ss.

3. N. Ciocca, Alcune riflessioni su intermediari finanziari ed evoluzione tecnologica, in A. Sacco Ginevri (a cura di), Princìpi di riforma del Testo unico della finanza, Milano, 2026, pp. 180-181, secondo cui, "L'evoluzione tecnologica ha acceso un attivismo di investimento in prima persona (...) Sussistono però indicatori di una permanente partecipazione ai mercati dei capitali che poggia saldamente su intermediari autorizzati: l'architettura del Micar, impostata come disciplina di prestatori di servizi, conferma il ricorso agli intermediari, autorizzati e sottoposti a vigilanza"; C. Brescia Morra, D. Colonnello, M. Gargantini, G. Sandrelli, G. Trovatore, La gamification degli investimenti finanziari, in Quaderni Giuridici CONSOB, n. 32, 2025, p. 8 ss.; A. Guaccero, Tra democrazia e populismo nel mercato finanziario: lezioni dal caso Gamestop, in Riv. Soc., 2023, 240 ss.

4. M.B. Armiento, Dark pattern e tutela degli investitori: prospettive di regolazione, in Banca Impresa Società, n. 3/2024, pp. 499-501, il quale evidenzia: "la digitalizzazi-

In tale contesto, il baricentro della tutela, tradizionalmente ispirato al rispetto dei princìpi di trasparenza e alla necessità di ridurre asimmetrie informative nel rapporto intermediario-investitore, deve (e dovrà) spostarsi verso la costruzione di architetture digitali capaci di consentire all'investitore *retail* l'adozione di decisioni finanziarie libere e consapevoli, scevre da influenze derivanti dall'adozione di tecniche manipolative.
In questa prospettiva, si accennerà alla nozione di *choice architecture*[5] e, più in generale, alla crescente attenzione alla *digital fairness*, cui si ricollega anche la prospettata adozione del *Digital Fairness Act* europeo[6].
Tali fenomeni acquistano particolare rilievo alla luce delle politiche europee già in atto; si fa riferimento alla *Retail Investment Strategy* (*RIS*) e alla *Savings and Investments Union* (*SIU*) che muovono nella direzione di una maggiore mobilitazione del risparmio verso i mercati dei capitali; l'ampliamento dei potenziali partecipanti al mercato rende ancor più stringente l'esigenza di adeguare gli attuali presìdi di tutela ai rischi connessi alla digitalizzazione e alle nuove forme di investimento[7].
Il suddetto scenario non è privo di conseguenze sulle attività delle autorità di vigilanza. Da un lato, la CONSOB è già orientata verso una supervisione sempre più *data-driven*, fondata anche su applicazioni di intelligenza artificiale e strumenti di *early warning*[8]; dall'altro lato, la crescente dimensione europea e centralizzazione della vigilanza rafforza l'esigenza di coordinamento, convergenza degli approcci e condivisione delle informazioni fra CONSOB, ESMA e le altre autorità nazionali, ridefinendo il ruolo dell'autorità[9].
In questo quadro di progressiva europeizzazione, occorre valutare se e in quale misura la capacità della CONSOB di governare i mercati finanziari del 2030 possa dipendere dalla qualità degli strumenti tecnologici di vigilanza e dalla possibilità di impiegare le evidenze emerse nel mercato finanziario nazionale per contribuire all'evoluzione della regolazione e delle prassi di supervisione europei, in linea con un approccio *bottom-up*.

2. Dall'intermediazione finanziaria tradizionale alle piattaforme di *trading*: nuove modalità di accesso al mercato dell'investitore *retail*

Nel settore finanziario, la figura del consumatore presenta già una prima dimensione di "ibridità": l'investitore al dettaglio è, sotto il profilo della tutela, un consumatore, ma al contempo un soggetto chiamato a operare all'interno di un mercato caratterizzato da peculiari asimmetrie informative, elevata complessità tecnica e specifici rischi decisionali[10].
Il funzionamento tradizionale dei mercati finanziari si fonda su un sistema di relazioni fra investitori *retail* e intermediari, attraverso cui gli investitori danno seguito a decisioni di investimento in un contesto improntato al rispetto dei principi di correttezza e trasparenza[11].
La disciplina dei flussi informativi, come stabilito dalla MIFID II, opera secondo una logica bidirezionale che si traduce, in primo luogo, nel dovere dell'intermediario di fornire all'investitore le informazioni necessarie a consentirgli decisioni di investimento informate e consapevoli e, in secondo luogo, nel dovere di acquisire dal cliente le informazioni funzionali e propedeutiche alla corretta prestazione del servizio[12]. La *ratio* di tale meccanismo risiede nell'esigenza di

---

one contribuisce a rendere più vulnerabili gli investitori al dettaglio: i dark pattern possono indurre questi ultimi ad adottare scelte di consumo non in linea con il proprio interesse (e ad acquistare, ad esempio, prodotti finanziari che non sono affatto vantaggiosi o che, come emergerà, presentano costi nascosti che gli investitori non avevano considerato nell'acquisto)".

5. C. Busch-A. Fletcher, Harmful online choice architecture, CERRE Report, 2024, 5; N. Helberger - M. Sax - J. Strycharz - H.W. Micklitz, Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in Journal of Consumer Policy, 45, 2021, p. 175 ss.

6. Commissione Europea, 2030 Consumer Agenda and action plan for consumers in the single market, COM(2025) 848 final, p. 7, ove si statuisce che "(...) the digital fairness fitness check of EU consumer law identified shortcomings and problematic practices in the digital environment that require action at EU level to fill gaps in consumer protection, reduce legal uncertainty for businesses, prevent regulatory fragmentation and facilitate enforcement (...) the Commission will also propose a Digital Fairness Act to further strengthen the protection of consumers online against practices such as: dark patterns that can unfairly influence consumer decisions; addictive design features; problematic practices by influencers; unfair personalisation that takes advantage of consumers' vulnerabilities and problematic features in digital products such as social media, video games and e-commerce. The Digital Fairness Act will also aim at simplifying rules for businesses, in particular by looking at consumer information requirements in specific types of contracts and in repetitive transactions with the same traders".

7. Commissione europea, *Savings and Investments Union. A Strategy to Foster Citizens' Wealth and Economic Competitiveness in the EU*, COM(2025) 124 final, p. 5 ss.; a livello nazionale, si pone nella stessa direzione anche la CONSOB nel suo Piano Strategico 2025-2027.

8. Consob, Piano strategico 2025-2027, p. 26.

9. Consob, *Piano strategico 2025-2027*, p. 26; Esma, *Union Strategic Supervisory Priorities*, 2026, pp. 1-3.

10. Invero, l'investitore retail, come osservato, non è altro che un consumatore ritenuto particolarmente vulnerabile alla luce del peculiare contesto in cui opera; così; tale circostanza giustifica la rigidità delle regole di condotta imposte agli intermediari. In dottrina, si v. L. Rossi Carleo, Consumatore, consumatore medio, investitore e cliente: frazionamento e sintesi nella disciplina delle pratiche commerciali scorrette, in «Europa e diritto privato», 3, 2010, pp. 687-688: "L'innegabile frantumazione di una figura, peraltro solo in apparenza puntualmente definita, da una parte vede il «consumatore», o meglio, la sua nozione, specificarsi e, contemporaneamente, dilatarsi, nella figura (...) ora del cliente, ora dell'investitore, e così via"; anche M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 501. Similmente a quanto fatto nella Direttiva MIFID II (Direttiva 2014/65/UE, modificata dalla Direttiva (UE) 2024/790 del 28 febbraio 2024), nel Testo Unico della Finanza (d.lgs. 24 febbraio 1998, n. 58), l'investitore retail è definito per sottrazione rispetto a quello "professionale" (i.e., "i clienti o gli investitori che non sono clienti professionali o investitori professionali", come stabilito dall'art. 1, comma 1, lett. m-duodecies).

11. Sul ruolo della trasparenza e dell'informazione nel funzionamento del mercato finanziario e nell'assunzione di scelte di investimento, si v. R. Lener-P. Lucantoni, Il mercato finanziario, Torino, 2024; p. 19 e ss.; N. Moloney, How to protect investors. Lessons from EC and UK, Cambridge, 2010, 288 ss.; D.C. Langevoort, The SEC as a Lawmaker: Choices about Investor Protection in the Face of Uncertainty, in 84 Wash. U. L. Rev., 2006, 1951 ss.

12. La disciplina è contenuta, come noto, nel pacchetto MIFID II (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) e nella MIFIR. G. Liace, L'investitore tra deficit informativi e bias comporta-

attenuare le asimmetrie informative e gli squilibri contrattuali propri del mercato finanziario[13], assicurando, al contempo, un'adeguata tutela dell'investitore *retail*, che, per sua natura, è più vulnerabile[14].
L'evoluzione tecnologica tende a modificare le tradizionali modalità di accesso al mercato[15], incidendo anche sulla tradizionale relazione intercorrente tra intermediario e cliente.
In tale direzione muove la progressiva diffusione delle piattaforme di *trading* (i c.d. *neobrokers*[16]), che favoriscono crescenti forme di attivismo diretto dell'investitore al dettaglio al mercato, riducendo costi, *fees* e tempi di accesso e semplificando le modalità operative di invio degli ordini di investimento[17]. In determinati casi, le commissioni dei *neobrokers* sono state del tutto azzerate con sistemi di remunerazione basati sui c.d. benefici *payment for order flow*[18].
Siamo, pertanto, dinnanzi a "nuove generazioni"[19] di investitori al dettaglio, che operano quotidianamente scelte di investimento tramite i propri dispostivi, esponendosi a nuovi fattori di rischio[20] e rendendo necessario adeguare, ripensare e potenziare le tradizionali forme di tutela, anche alla luce della giovane età, minor esperienza e maggiore propensione al rischio dei soggetti operanti nel contesto di queste piattaforme [21].
Quale corollario di quanto precede, per un verso, l'utilizzo di piattaforme di *trading* si muove in un'ottica di progressiva democratizzazione dell'investimento e di riduzione delle barriere economiche, come dimostrato dalla possibilità di effettuare investimenti di piccolo taglio, ad esempio, in portafogli automatizzati[22]; per altro verso, l'investitore *retail* tende in misura crescente a emanciparsi dal tradizionale modello basato sul rapporto personale tra investitore e intermediario, assumendo sempre più decisioni di investimento autonome, con un'interazione prevalente con l'interfaccia della piattaforma e con le sollecitazioni, anche manipolative, che la stessa porta con sé [23].
È evidente, tuttavia, che il rapporto tra investitore *retail* e intermediario non è destinato, di qui al 2030, a venir meno, quanto piuttosto a trasformarsi. L'intermediario sarà chiamato ad assumere un ruolo diverso, nell'ambito di una strategia di tutela integrata che tenga conto delle peculiarità dell'ambiente digitale. Come autorevolmente osservato, non appare infatti realistico né ipotizzare un'assistenza quotidiana dell'intermediario nelle scelte di investimento digitali, né immaginare piattaforme prive degli stimoli, anche grafici e comportamentali, che ne caratterizzano fisiologicamente l'operatività[24].
Ciò premesso, come si vedrà nel prosieguo, la tutela dell'investitore non potrà più essere affidata soltanto alla predisposizione di adeguati *package* informativi, ma dovrà misurarsi sempre più con la configurazione della *choice architecture*, ossia con la progettazione di piattaforme di *trading* capaci di preservare, per quanto possibile, la libertà e l'autonomia della scelta di investimento.
L'evoluzione tecnologica, pertanto, tende ad accentuare il carattere già "ibrido" dell'investitore *retail*, il quale è sempre più inserito in un ecosistema nel quale piattaforma, infrastruttura tecnologica e processo decisionale tendono a sovrapporsi.
Questa trasformazione si colloca, peraltro, come anticipato, in un contesto europeo nel quale l'ampliamento della partecipazione degli investitori *retail* ai mercati dei capitali rappresenta esso stesso un obiettivo di politica economica.

---

mentali, in Banca Impresa Società, n. 3/2018, p. 445 ss., spec. p. 445-448; C. Cioffi, L'informazione la trasparenza e la causa dei contratti derivati, Napoli, 2018; A. Cilento, I doveri di informazione del consulente finanziario tra regole di validità e regole di responsabilità, Napoli, 2017; A. Dell'Atti - S. Sylos Labini, La trasparenza informativa, Milano, 2014.

13. Per un'analisi sulle asimmetrie informative nel mercato finanziario e sui correttivi introdotti dalla disciplina MIFID, si v. F. Capriglione, *Intermediari finanziari, investitori, mercati. Il recepimento della Mifid. Profili sistematici*, Padova, 2008, p. 151 ss. Assolvimento ad obblighi informativi e di trasparenza che non sono sempre fattori idonei a contrastare le asimmetrie informative del mercato (cfr. F. Vella, *La finanza è bella: regole per viverla meglio*, in «AGE», 1, 2012, pp. 217-218). M.B. Armiento, *Dark pattern e tutela degli investitori*, *cit.*, p. 500; G. Liace, *L'investitore tra deficit informativi e bias comportamentali*, *cit.*, p. 445 ss.; U. Minneci, *Servizi di investimento e gradazione dei clienti*, Milano, 2013; V. Piccinini, *I rapporti tra banca e cliente. Asimmetrie e condotte abusive*, Padova, 2008.
14. M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 500.
15. F. Annunziata, Retail Investment Strategy., cit., p. 22, ove si evidenzia che: "Digitalisation can impact retail investors in different ways, from the simple automatisation of transactions through online platforms (...)".
16. Tra i principali esempi vengono annoverati da E. Franza, I nuovi intermediari: "i Neobroker", in dirittobancario.it, 19 novembre 2025, a livello globale, Robinhood (USA) ed eToro (social trading); in Europa, Trade Republic e Scalable Capital (Germania), Degiro (Paesi Bassi) e Revolut; in Italia, Directa Sim, Fineco Bank, Young Platform e Moneyfarm.
17. C. Brescia Morra, D. Colonnello, M. Gargantini, G. Sandrelli, G. Trovatore, La gamification degli investimenti finanziari, cit., p. 18 ss.; A. Guaccero, Tra democrazia e populismo nel mercato finanziario, cit., 240; Teleborsa, Neobroker alla conquista dell'Italia: i piani delle app da zero commissioni, La Stampa, 24 giugno 2022, disponibile su https://finanza.lastampa.it/
18. Sotto questo profilo, dal 30 giugno 2026 tale pratica è vietata in tutti i paesi dell'Unione Europea nell'ambito della revisione normativa del pacchetto MIFID II/MIFIR.
19. N. Ciocca, Alcune riflessioni su intermediari finanziari ed evoluzione tecnologica, cit., pp. 180-181.
20. F. Annunziata, Retail Investment Strategy., cit., p. 22; J.A. Barefoot, Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech, Harvard Kennedy School M-RCBG Associate Working Paper Series No. 151, 2020 disponibile su: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf.
21. Gli utenti dei neobroker risultano mediamente più giovani, meno esperti e più propensi al rischio, con operatività più frequente. Una survey tedesca ha osservato le criticità connesse alla scarsa alfabetizzazione finanziaria degli utenti e alla scarsa comprensione dei meccanismi di guadagno della piattaforma tra gli utenti.
22. E. Franza, I nuovi intermediari: "i Neobroker", in dirittobancario.it, 19 novembre 2025.
23. N. Ciocca, Alcune riflessioni su intermediari finanziari ed evoluzione tecnologica, cit., p. 177 ss. che evidenzia: "Possibili indicatori di accesso più diretto degli investitori ai mercati vengono invece dalle piattaforme di trading, che veicolano investimenti effettuati con modalità operative più autonome da parte di investitori al dettaglio. (...)"; Anche E. Franza, I nuovi intermediari, cit.
24. N. Ciocca, Alcune riflessioni su intermediari finanziari ed evoluzione tecnologica, cit., p. 182.

Si fa riferimento alle già menzionate *Retail Investment Strategy*[25] e *Savings and Investments Union*[26], le quali mirano, tra l'altro, a favorire una più ampia partecipazione dei risparmiatori ai mercati finanziari, senza che ciò, naturalmente, determini pregiudizi in termini di tutela in capo a quest'ultimi[27].
In tale quadro, la Commissione europea ha presentato il "*Market Integration and Supervision Package*" e la *Consumer Agenda* 2030, entrambi volti a facilitare l'accesso degli investitori a più ampie opportunità di investimento e a garantire ai cittadini dell'Unione un accesso sicuro ai mercati, anche nell'era dei servizi digitalizzati; nella stessa direzione si muove, sul piano della vigilanza, la nuova *Union Strategic Supervisory Priority* ("USSP"), operativa dal 2027, che coniuga la promozione dell'innovazione digitale con un adeguato livello di tutela degli investitori. La medesima tensione tra ampliamento della partecipazione e rafforzamento della tutela emerge, sul piano nazionale, nel Piano strategico CONSOB 2025-2027, che all'obiettivo di favorire una maggiore presenza degli investitori *retail* sul mercato mobiliare, affianca l'esigenza di potenziare i presìdi di protezione rispetto ai rischi connessi all'ecosistema digitale.

3. La metamorfosi delle infrastrutture: *blockchain* e *cryptoassets*

Come anticipato nelle premesse del presente contributo, la metamorfosi dei mercati finanziari estende il suo raggio di operatività anche alle infrastrutture sulle quali gli scambi finanziari possono svolgersi. In tale prospettiva, si colloca la tecnologia *blockchain*, che sta contribuendo notevolmente a fenomeni di ibridazione tra "norme, ordinamenti, imprese, individui", mutando le modalità con cui l'individuo si atteggia negli acquisti di prodotti e servizi[28].
In particolare, come noto, la *blockchain* costituisce un registro informativo, aperto e distribuito, che consente lo scambio anonimo di nuove categorie di servizi e prodotti, e, più in generale, di valore[29], ivi incluse le cripto-attività, memorizzando le informazioni e transazioni eseguite su detta infrastruttura[30]. La tecnologia *blockchain* si pone a fondamento del Web 3.0, che è connotato dalla decentralizzazione dei processi e dall'operatività di *smart contracts* con automatizzazione delle transazioni[31].
Se da un lato tale *tecnologia* consente di dar luogo a transazioni finanziarie immediate su cripto-attività, contribuendo, così, a una progressiva democratizzazione dei mercati[32], dall'altro lato, *blockchain* e cripto-attività hanno posto evidenti esigenze di regolazione[33], a tutela dei rischi connessi alla stabilità dei mercati, alla sicurezza – anche informatica – delle infrastrutture e alla tutela degli investitori[34].
Nell'Unione europea, quanto sopra ha condotto all'adozione del Regolamento MiCA ("Markets in Crypto-Assets Regulation")[35], cui si collegano la proposta di *Pilot-Regime for DLT-based Market Infrastructures* e il *Digital Operatio-*

25. Commissione europea, Strategia per gli investimenti al dettaglio - Proposta di direttiva del Parlamento europeo e del Consiglio che modifica le direttive 2009/65/CE, 2011/61/UE, 2013/36/UE e 2014/65/UE per quanto riguarda il rafforzamento della tutela degli investitori al dettaglio e la promozione degli investimenti al dettaglio, COM(2023) 279 final, 24 maggio 2023.
26. Cfr. Commissione europea, Comunicazione sulla strategia per l'Unione del risparmio e degli investimenti: una strategia per promuovere la ricchezza dei cittadini e la competitività economica dell'UE, COM(2025) 124 final, 19 marzo 2025.
27. Commissione europea, Savings and investments union strategy to enhance financial opportunities for EU citizens and business, 19 marzo 2025. In dottrina, sul tema, si v., tra l'altro, M. Rabitti, Gli intermediari finanziari nel contesto attuale dei mercati finanziari: considerazioni minime introduttive, in A. Sacco Ginevri (a cura di), Princìpi di riforma del Testo unico della finanza, Milano, 2026, 155 ss.; P. Lucantoni, Dalla Capital Market Union alla Savings and Investment Union: Tutela degli investitori e (assenza di) rimedi nella prospettiva euronitaria, in A. Sacco Ginevri (a cura di), Princìpi di riforma del Testo unico della finanza, Milano, 2026, 187 ss., ove si osserva che "*è nella Relazione Letta (...) che si propone una trasformazione della CMU nella odierna Savings and Investments Union (SIU) (...) funzionale alla realizzazione degli obiettivi di equità, transizione ecologica e digitale alla base della costruzione del "new Single market*".
28. F. Bassan, L'era ibrida. Sovranità e democrazia tra poteri pubblici e imprese tech, Catanzaro, 2026, pp. 41. Le criptoattività si moltiplicano in misura progressivamente crescente; già al 2019, con numeri oggi ancora maggiori, un rapporto ESMA ne individuava oltre 2050, con capitalizzazione di oltre 110 miliardi (Esma, Advice on Initial Coin Offering, ESMA 50-57-1391, 9 gennaio 2019, p. 8). Sul punto, si v. F. Annunziata. La disciplina del mercato dei capitali, Torino, 2026, p. 488.
29. 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 distribuito 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 delle quali, si rinvia al predetto documento.
30. Per una ricostruzione dei connotati della blockchain, si v. F. Annunziata. La disciplina del mercato dei capitali, cit., p. 487 ss., che specifica: "I partecipanti sono definiti "nodi" e sono connessi tra loro; i dati, contenuti in "blocchi", sono immutabili: non possono essere retroattivamente alterati senza modificare tutti i blocchi successivi, operazione che richiederebbe il consenso della maggioranza della rete. Ogni blocco è identificato da un codice, contiene le informazioni di una serie di transazioni e detiene il codice del blocco precedente, così da ripercorrere la catena fino al blocco originale. Tutti i nodi memorizzano l'intera blockchain"; anche F. Bassan, Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain', in Rivista di Diritto Bancario, 2023, p. 561 ss.
31. Sulla Web 3.0, F. Bassan, Web 3 in Transition and participatory regulation, in CPI-Tech Cronicle, 2023.
32. F. Bassan, L'era ibrida. cit., p. 24, ove si evidenzia che: "Gli sviluppi della blockchain nei sistemi finanziari, mediante la contestualità ("atomica") degli scambi tra prestazione e controprestazione garantita dalla tecnologia blockchain, consentono da un lato di rendere più democratici i processi, dall'altro sia di disintermediare gli intermediari che non creano valore, sia di permettere a quelli che restano di superare l'esigenza del rapporto fiduciario, oggi garantita da una terza parte centrale".
33. Come osservato, infatti, da F. Annunziata, La disciplina del mercato dei capitali, cit., 488: "la mancanza di un quadro regolamentare specifico e l'incertezza sull'applicabilità delle discipline esistenti (...) hanno favorito una proliferazione massiccia delle ICOs [Initial Coin Offerings] a livello mondiale, con l'affermarsi di grandi piattaforme di scambio dei token e di un vasto mercato secondario, per lo più non regolamentato e opaco".
34. Come già osservato da F. Annunziata, Fintech, cit., 267, "sono emersi rischi e problemi nient'affatto lontani da quelli che connotano la più tradizionale industria e regolazione finanziaria: tutela delle controparti più deboli; asimmetrie informative; inefficienza dei mercati e rischi di manipolazione; rischi di stabilità finanziaria, finanche a livello sistemico; frodi e, come noto, elevati rischi di antiriciclaggio. I clamorosi default che hanno interessato, soprattutto negli Stati Uniti, taluni grandissimi operatori del settore a cavallo tra il 2022 e il 2023 (il c.d. "crypto winter"3) e culminati nel fallimento dell'exchange "FTX"4, sono stati soltanto i casi più evidenti di una lunga serie di fenomeni patologici che, da subito, avrebbero dovuto sollecitare una risposta regolatoria sia in Europa, sia altrove.".
35. Nel contesto nazionale, con il D.lgs. n. 129/2024 – attuativo del Regolamento MiCA, che, come noto, delinea una disciplina inerente al mercato e non alle criptoattività

nal Resilience Act; per altro verso, negli Stati Uniti, è stato avviato un processo normativo in materia di cripto-attività e *stablecoin*, che si affianca all'autoregolamentazione dell'autorità di vigilanza tipica dei sistemi di *common law*[36].

Ciò premesso, occorre rilevare come anche nell'ecosistema della *blockchain* emergano sistemi ibridi. Tale profilo deve essere esaminato alla luce della natura multiforme di tale tecnologia, che sfrutta sia modelli *public* sia *private*, il cui distinguo si effettua sulla base del livello di accesso, di controllo e di decentralizzazione degli stessi; in estrema sintesi, i modelli *public* concretizzano i prìncipi dell'accesso libero e della decentralizzazione, mentre i modelli *private* sottostanno a un'autorità centrale che vigila sull'accesso all'entrata e sui trasferimenti di valore[37].

Sotto questo profilo, sono stati effettuati due ordini di osservazioni in dottrina[38].

In primo luogo, l'originaria predilezione dei legislatori e regolatori verso le *blockchain private* si sta orientando sempre più verso modelli *public*; in particolare, di maggior utilizzo sono sistemi di *blockchain* nei quali la decentralizzazione dell'infrastruttura sottostante convive con forme di controllo sull'accesso e sulle attività svolte, anche nell'ottica di ridurre le difficoltà legate all'attribuzione di responsabilità nel contesto delle transazioni su cripto-attività in modelli totalmente *public*. Si nota, dunque, che tali "piattaforme logiche ad accesso controllato"[39] non riproducono nella loro integralità la logica della *blockchain public*, ma si appropriano di elementi tipici dei sistemi *private*, dando luogo a un evidente fenomeno di ibridazione tra *blockchain*.

A ciò si aggiunga che la capacità della *blockchain* di sviluppare nuove attività e strumenti di pagamento influirebbe altresì sul rapporto tra poteri pubblici e privati; governare l'infrastruttura diventerebbe, in tal senso, una lotta alla sovranità. Il controllo dell'infrastruttura *blockchain* e dei mezzi di pagamento che su essa operano può tradursi nel controllo dell'intero ecosistema della tokenizzazione, incidendo su ambiti tradizionalmente riconducibili alla sovranità statale. In questo quadro, le piattaforme e gli operatori del Web 3.0 tendono ad assumere un ruolo potenzialmente concorrente ai poteri pubblici nel governo delle infrastrutture di scambio[40].

4. I fattori di rischio connessi alla digitalizzazione delle infrastrutture e nuove forme di tutela

L'ascesa di nuove infrastrutture tecnologiche costituisce soltanto una delle manifestazioni della più ampia trasformazione digitale dei mercati finanziari.

La crescente facilità di accesso dell'investitore *retail* al mercato tramite piattaforme di *trading* e di scambio di cripto-attività, si accompagna infatti all'emersione di nuovi fattori di rischio, connessi non soltanto ai prodotti offerti, ma anche alle modalità di interazione con la piattaforma nella quale il soggetto opera. Quest'ultima può incidere concretamente sul processo decisionale dell'investitore, facendo leva sulle sue vulnerabilità cognitive e comportamentali e conducendolo all'adozione di scelte di investimento in prodotti finanziari potenzialmente contrarie ai propri interessi e vantaggiose per le piattaforme.

Costituiscono esempi di tali pratiche i *dark patterns*[41], definiti anche "modelli di progettazione ingannevole"[42], e la *gamification*, intesa come l'utilizzo di meccanismi propri del gioco in ambiti estranei al contesto ludico[43].

Con particolare riferimento ai *dark patterns*, queste costituiscono pratiche che interessano il consumatore nella sua interezza ma che assumono particolari connotazioni con riferimento al settore finanziario. Si pensi alle tecniche di *nudging* sfruttate dagli intermediari per indurre l'investitore al dettaglio ad acquistare strumenti finanziari "personaliz-

– si attribuiscono già oggi poteri di indagine e vigilanza alla Consob in materia di criptoattività; talvolta in via esclusiva, talvolta condivisi con la Banca d'Italia. In particolare, ai sensi del predetto decreto legislativo, in merito ai prestatori di servizi, la Banca d'Italia vigila sul contenimento del rischio, sulla stabilità patrimoniale e sulla sana e prudente gestione; la CONSOB sulla trasparenza, correttezza delle condotte di mercato e sull'articolarsi delle negoziazioni; inoltre, la CONSOB è, ad esempio, competente in via esclusiva per la prevenzione e la vigilanza sugli abusi di mercato. Si prevedono inoltre meccanismi di cooperazione reciprocamente tra le autorità nazionali e tra quest'ultime e quelle europee, che risultano disciplinate da apposito Protocollo ai sensi dell'art. 7 del Regolamento MiCA.

36. Si fa riferimento al Genius Act, avente ad oggetto le stablecoin e alla proposta legislativa del c.d. Clarity Act, che si occuperebbe sia di stablecoin sia di altri assets, attualmente colpita da uno stallo in Senato).

37. Sui modelli di blockchain, si v. F. Bassan, Recenti evoluzioni dei contratti sulla blockchain., cit., passim.

38. In tal senso si pongono le riflessioni di F. Bassan, L'era ibrida. cit. p. 41.

39. F. Bassan, Recenti evoluzioni dei contratti sulla blockchain. cit., p. 601, il quale ritiene che "le piattaforme logiche ad accesso controllato che operano sulle blockchain pubbliche sembrano essere una soluzione idonea sia per l'attuale fase di transizione dal Web2 al Web3".

40. F. Bassan, L'era ibrida. cit. p. 67.

41. La locuzione dark pattern è rinvenibile in H. Brignull, Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff, 8 luglio 2010, reperibile al seguente link: https://90percentofeverything.com/2010/07/08/dark-patternsdirty-tricks-designers-use-to-make-people-do-stuff/: si v. anche F. Di Porto - A. Egberts, The Collective Welfare Dimension of Dark Patterns Regulation, in European Law Journal, 29, 2023, p. 115, nota 7 e I. Graef, The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?, Discussion Paper TILEC, aprile 2023, p. 2, nota 2. V. anche J. Liguri - L. Strahilevitz, Shining a Light on Dark Patterns, in Journal of Legal Analysis, 13, 1, 2021, p. 43 ss.

42. Si tratta della definizione offerta dal Garante per la protezione dei dati personali nel contesto delle Linee Guida n. 3/2022 intitolate «Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them» del Comitato europeo per la protezione dati (EDPB), adottate il 24 febbraio 2023.

43. C. Brescia Morra, D. Colonnello, M. Gargantini, G. Sandrelli, G. Trovatore, La gamification degli investimenti finanziari, cit., passim; M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 500; 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, p. 9 ss.

zati"[44]; da un'indagine extra-europea[45], emergono, poi, i c.d. *hidden costs*, ossia costi reali scoperti dall'investitore solo a posteriori e il meccanismo degli *alert* che, segnalando la disponibilità limitata nel tempo di un prodotto finanziario scontato, fa leva sulla *loss aversion* dell'investitore e lo induce a effettuare l'acquisto.
Si tratta di fenomeni che si collegano anche al mutamento delle infrastrutture, trovando terreno fertile di sviluppo, oltre che nelle piattaforme di *trading*, anche nella peculiare operatività del mercato delle cripto-attività[46].
In tal senso, un esempio è costituito dai conti dedicati alle cripto-attività, i quali sono integrati nella medesima applicazione utilizzata per il *trading* tradizionale, catturando così l'attenzione dell'utente e inducendolo a investire in cripto-attività[47]; come nel caso dei pulsanti "scopri le cripto", presentati come opzione predefinita attraverso il posizionamento e l'uso dei colori dopo che l'utente ha effettuato un versamento sul proprio conto.
Ancora, i c.d. *recurring investments*, ossia strumenti attraverso i quali le piattaforme si avvalgono di manipolazioni sensoriali per promuovere investimenti ricorrenti, nei quali l'utente acconsente ad acquistare periodicamente, *inter alia*, cripto-attività; la rappresentazione visiva di un'opzione ricorrente può ridurre la diversificazione e aumentare i costi effettuando più transazioni di quante altrimenti avrebbe scelto.
Da ultimo, anche l'interfaccia principale delle piattaforme di *trading* può orientare malevolmente l'utente verso azioni correlate alle cripto-attività, con pubblicità aventi funzionalità di *staking*; tale funzionalità consente all'utente di vincolare le proprie cripto-attività per ottenere ricompense, a fronte dell'applicazione, da parte della piattaforma, di corpose commissioni. Si tratta di funzionalità che orientano l'investitore all'assunzione di rischi più elevati ancor prima della sua registrazione a un conto cripto.
In un mercato connotato da alta rischiosità, come quello delle criptoattività, la diffusione di *dark patterns* (e *gamification*), che potrebbe condurre a fenomeni di speculazioni inconsapevoli sui mercati da parte degli utenti, solleva ancor di più interrogativi in termini di tutela dell'utente[48]. Sul punto, la dottrina[49] si è di recente occupata di valutare l'attualità e adeguatezza della disciplina delle pratiche commerciali scorrette, cui il Regolamento MiCA rinvia, a far fronte a detti fenomeni digitali emergenti e in rapido sviluppo.
In sostanza, nel settore degli investimenti *retail*, come anche nel mercato delle cripto-attività, i *dark patterns* possono incidere in modo pregnante sull'autonomia decisionale dell'investitore-utente[50]. La piattaforma, servendosi dei *bias* cognitivi di quest'ultimo (i.e., *inter alia*, lo *status quo bias*, l'avversione alla perdita, la scarsità o gli effetti di *framing*), ne orienta le scelte in modo non necessariamente coerente con il suo interesse e con una corretta percezione del rischio[51].
Il fenomeno si innesta sulla fragilità del paradigma informativo già da tempo evidenziata dalla dottrina. La disponibilità di informazioni corrette e complete non elimina infatti i limiti cognitivi del destinatario, né assicura che questi sia in grado di elaborarle correttamente. È stato già evidenziato, sotto questo profilo, come le modalità di presentazione dell'informazione, il contesto e il tempo disponibile per processare le informazioni assumano rilievo ai fini della qualità della decisione[52].
In un mercato sempre più digitalizzato il livello di tutela accordato all'investitore *retail*, tradizionalmente ispirato al rispetto dei princìpi di trasparenza e alla necessità di ridurre asimmetrie informative nel rapporto intermediario-investitore, dipenderà, in misura crescente, dalle modalità di progettazione del mercato digitale e, quindi, dalla c.d. *choice architecture*.
Ogni interfaccia nella quale sono offerte alternative incorpora necessariamente una determinata modalità di presentazione delle scelte: l'ordine delle opzioni, le impostazioni predefinite, il grado di visibilità di un'alternativa e la rappre-

44. ESMA, Makes Recommendations to Improve Investor Protection, 29 aprile 2022, con allegato il report Technical Advice on Retail Investor Protection. In dottrina, M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 508.
45. Si fa riferimento allo studio dell'Ontario Securities Commission, Digital Engagement Practices: Dark Patterns in Retail Investing, del 21 febbraio 2024.
46. C. Failla, Gamification, dark patterns e cripto-attività. Prospettive di adattabilità della disciplina delle pratiche commerciali scorrette, in Osservatorio del diritto civile e commerciale, n. 1/2024, pp. 113 ss., spec. pp. 118-119 che osserva come: "il mercato delle cripto-attività nasce e si sviluppa insieme a tale progresso tecnologico, costituendone una componente rilevante dell'ultimo decennio, con la conseguenza che l'ingresso in tale ecosistema della gamification e dei dark patterns è stato non soltanto quasi immediato, ma ne ha trovato un terreno fertile per il loro sviluppo".
47. Ontario Securities Commission, Digital Engagement Practices, cit., 17.
48. C. Failla, Gamification, dark patterns e cripto-attività, cit., p. 133.
49. C. Failla, Gamification, dark patterns e cripto-attività, cit., p. 133 ss.
50. M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 511; sul tema, anche M. Brenncke, Regulating Dark Patterns, in Notre Dame Journal of International & Comparative Law, 14, 1, 2024, p. 39 ss., il quale individua molteplici manifestazioni della "compressione" dell'autonomia del consumatore; sempre sul tema, si v. F. Ferretti, L'Open Finance. Quali prospettive regolatorie per una strategia UE in materia di protezione dei consumatori nella finanza digitale?, in Banca Impresa Società, 2, 2023, 277 ss.
51. Si v. Ontario Securities Commission, Digital Engagement Practices, cit., 17; M.B. Armiento, Dark pattern e tutela degli investitori, cit., p. 511 ss.; Già G. Liace, L'investitore tra deficit informativi e bias comportamentali, cit., p. 454, evidenziava che l'avversione alle perdite esprime la tendenza dell'individuo ad attribuire un peso maggiore alle variazioni negative rispetto a quelle positive di analoga entità. La valutazione, inoltre, non avviene in termini assoluti, ma rispetto a un punto di riferimento iniziale, rispetto al quale perdite e guadagni vengono percepiti; D. Kahneman - J.L. Knetsch - R.H. Thaler, Anomalies: The Endowment Effect, Loss Aversion, and Status quo Bias, in The Journal of Economic Perspectives, 5, 1, 1991, p. 193 ss.
52. G. Liace, L'investitore tra deficit informativi e bias comportamentali, cit. p. 454; S. Iyengar - E. Kamenica, Choice Overload and Simplicity Seeking, University of Chicago, Graduate School of Business, 2007.

sentazione grafica contribuiscono a strutturare il contesto decisionale[53]. L'architettura della scelta è dunque un concetto in sé neutro, ma può essere utilizzata per rendere la decisione più agevole oppure per orientarla in una direzione non corrispondente alle preferenze dell'utente[54].
Ne deriva che, nel mercato finanziario digitalizzato, il tradizionale obiettivo di ridurre l'asimmetria informativa diviene insufficiente se non accompagnato dalla progettazione di infrastrutture digitali capaci di consentire scelte frutto di una libera autodeterminazione dell'investitore.
La questione travalica, pertanto, i confini della sola disciplina finanziaria e si inserisce nel più ampio dibattito europeo sulla *digital fairness*. Il quadro normativo UE contiene già una pluralità di disposizioni potenzialmente rilevanti rispetto ai *dark patterns*, distribuite, tra la disciplina delle pratiche commerciali scorrette, il *Digital Services Act*, la normativa sulla protezione dei dati e la disciplina dei contratti finanziari a distanza. Trattasi di una frammentazione che è stata indicata come una possibile fonte di incertezza e disomogeneità nell'applicazione[55].
La *Consumer Agenda 2030* colloca in questo contesto il *Digital Fairness Act*, la cui proposta legislativa è programmata per il quarto trimestre del 2026 e che dovrebbe intervenire su *dark patterns*, *addictive design* e forme di personalizzazione capaci di sfruttare le vulnerabilità dei consumatori[56].
Si registrano orientamenti divergenti in ordine alle soluzioni più idonee a contrastare tali fenomeni. Per un verso, vi è chi ritiene necessario rafforzare la regolazione europea per colmare le lacune di tutela rispetto alle tecniche manipolative e al *design* capace di compromettere l'autonomia decisionale dell'utente, auspicando l'adozione del *Digital Fairness Act*; per altro verso, l'industria digitale sostiene che il problema principale risieda nell'applicazione disomogenea delle normative vigenti a livello di *enforcement*, dovendosi irrobustire il coordinamento tra autorità e l'uso di strumenti tecnologici nella vigilanza[57].
Questa contrapposizione anticipa un'ulteriore questione di particolare rilevanza: una regolamentazione più sofisticata nella vigilanza di fenomeni digitali dovrà essere accompagnata dall'utilizzo di uno strumentario tecnologico sofisticato.

5. Verso un'agenda CONSOB 2030: consolidamento di una vigilanza *data-driven* e multilivello

La rivoluzione digitale del mercato finanziario si riflette anche in mutamenti di rilievo sotto al profilo della vigilanza domestica e sovranazionale.
Un primo riflesso di tale trasformazione concerne gli strumenti di cui la stessa Autorità intende dotarsi per svolgere la propria funzione di vigilanza. È attualmente in via di sviluppo il percorso di progressiva digitalizzazione della CONSOB, in esecuzione del Piano Strategico dell'Autorità per gli anni 2025-2027, orientato verso una vigilanza sempre più *data-driven*, basata sull'utilizzo di applicazioni integrate dall'intelligenza artificiale, sistemi di *early warning* e, più in generale, strumenti di analisi innovativi capaci di intercettare tempestivamente anomalie e fenomeni emergenti nel mercato[58].
La tecnologia diviene, in altri termini, parte integrante dello strumentario della vigilanza, consentendo di intercettare vulnerabilità e asimmetrie dell'investitore *retail* che non sono più soltanto informative, ma assumono una crescente dimensione "digitale" [59].
L'intuizione non è del tutto nuova. Già in dottrina è stato osservato come i *big data* potessero essere integrati nelle attività del regolatore affievolendo le asimmetrie informative e tracciando con maggior precisione eventuali errori

53. L'incertezza sulla possibilità di una "genuina" autodeterminazione dell'investitore operante nel mercato digitale è rappresentata anche da N. Ciocca, Alcune riflessioni su intermediari finanziari ed evoluzione tecnologica, cit., p. 185, che individua le seguenti ragioni a sostegno di ciò: "Innanzitutto, l'informazione è spesso veicolata con modalità programmate per influenzare il fruitore, con la finalità di indurlo a essere più attivo sul mercato. In secondo luogo, la "filtratura" delle informazioni si realizza con meccanismi tecnologici, che permettono di selezionare potenziali investitori a livelli sempre più specifici". Sulla choice architecture, si v. C. Busch - A. Fletcher, Harmful Online Choice Architecture, cit., p. 7 ss.
54. Sulla choice architecture, C. Busch - A. Fletcher, Harmful Online Choice Architecture, cit., 7; N. Helberger, M. Sax, J. Strycharz, H. W. Micklitz, Choice Architectures in the Digital Economy: cit., p. 186; R. H. Thaler- C. R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness, in Yale University Press, 2008.
55. P. Car - F. Cassetti, Regulating dark patterns in the EU: Towards digital fairness, 2025 p. 1-2.
56. Commissione Europea, 2030 Consumer Agenda and action plan for consumers in the single market, p. 4. The European Consumer Organization, Joint call for an ambitious Digital Fairness Act to better protect people online, 13 marzo 2026; Digital Europe, Digital fairness: enforcement, not a new Law, 2026; P. Car-F. Cassetti, Regulating dark patterns, cit., p. 1.
57. Per la prima posizione, J. Albert - M. Sax - N. Helberger, Digital Fairness Act: Why we need an ambitious DFA to protect digital consumers from manipulative and addictive design practices, 2026. In senso critico rispetto alla necessità di una nuova disciplina, che comporterebbe duplicazioni di regolazioni, si v. Digital Europe, Digital fairness: enforcement, not a new law, 2026, pp. 1 e 3, ove si precisa che: "There is no absence of rules: the problem lies in uneven enforcement. Rather than producing duplicative requirements that only burden compliant businesses, the EU should focus on strengthening enforcement of existing laws".
58. Consob, Piano strategico 2025-2027, passim.
59. J. Albert - M. Sax - N. Helberger, Digital Fairness Act, cit., 2.

cognitivi[60]. Il passaggio dalle potenzialità dei *big data* a quelle connesse all'utilizzo dei più evoluti strumenti di intelligenza artificiale rende oggi quella prospettiva assai più concreta nonché sempre più in ascesa.

I *dark patterns* e le tecniche di *gamification*, tanto per i loro riflessi attuali, quanto per quelli futuri, necessitano di strumenti di vigilanza sempre più innovativi; ciò anche tenendo conto che la CONSOB, nell'esercizio della sua funzione di vigilanza, si prefigge già nel proprio Piano Strategico 2025-2027 di prestare particolare attenzione ai profili applicativi e all'osservanza della disciplina MiCAR in materia di cripto[61], che, come anticipato, costituirà terreno fertile per l'emersione di pratiche manipolative dei partecipanti al sistema.

Sotto altro profilo, si assiste poi a una progressiva europeizzazione e centralizzazione della vigilanza nel settore finanziario. La Commissione Europea nel dicembre 2025[62] ha proposto un ampliamento dei poteri dell'ESMA sui mercati finanziari e delle criptoattività; si tratta di una proposta, ancora in fase di negoziazione tra il Parlamento Europeo e il Consiglio, che attribuirebbe ad ESMA le "competenze di vigilanza diretta", per quanto di interesse in questa sede, sui *crypto-asset service providers* (CASPs) e sulle piattaforme di *trading*.

Di recente, proprio l'ESMA, per un verso, ha risposto alla consultazione pubblica della Commissione europea sulla revisione del MiCAR[63], promuovendo norme più stringenti che regolino lo scambio di *crypto-assets*, maggiore tutela per gli investitori, nonché un irrobustimento dei propri poteri di vigilanza per contrastarne rischi e abusi (quali, ad esempio frodi *online*); per altro verso, ha definito nuove *Union Strategic Supervisory Priorities* a partire dal 2027, che includono attività di vigilanza sull'innovazione digitale e IA nel mercato finanziario, in collaborazione con le autorità nazionali, tra cui, naturalmente, la CONSOB[64].

La prospettiva di una crescente estensione delle forme di supervisione esercitate direttamente a livello Unionale determina un sistema multilivello in cui autorità nazionale ed europea coesistono e cooperano.

In tale contesto, il ruolo della CONSOB nei mercati finanziari tende a ridefinirsi. La dimensione europea della vigilanza rende ancor più essenziale la coerenza degli approcci adottati, la continuità dei flussi informativi e la condivisione delle evidenze tra CONSOB, ESMA e le altre autorità nazionali, così da assicurare un'applicazione uniforme ed efficace della disciplina[65].

Ciò premesso, la capacità della CONSOB di conservare un ruolo centrale nel governo delle trasformazioni in atto, senza ridursi a mero esecutore degli indirizzi definiti a livello europeo, potrebbe dipendere proprio dalla qualità e dall'efficacia degli strumenti digitali di vigilanza di cui saprà dotarsi.

Una vigilanza tecnologicamente avanzata consentirebbe infatti di intercettare tempestivamente sia ipotesi di mancata osservanza della disciplina, sia prassi di mercato e condotte virtuose degli investitori che, difficilmente, potrebbero essere colti con la medesima granularità a livello sovranazionale; si alimenterebbe così il processo di c.d. *bottom-up*[66], attraverso il quale l'esperienza applicativa può contribuire all'evoluzione della regolazione e degli stessi approcci di supervisione.

60. A. Dell'Atti, Asimmetria informativa nel mercato dell'intermediazione mobiliare e big data: quale contributo per la nudge regulation, in Rivista Trimestrale di Diritto dell'Economia, n. 4, supplemento al n. 1, 2016, p. 71 ss., spec. p. 74.

61. Consob, Piano Strategico 2025-2027, p. 2.

62. Si fa riferimento alla proposta di Regolamento del Parlamento Europeo e del Consiglio per quanto riguarda l'ulteriore sviluppo dell'integrazione dei mercati dei capitali e della vigilanza nell'Unione, COM(2025) 943 final, 10, ove si legge: "All'ESMA sarebbero trasferiti anche poteri di vigilanza per le infrastrutture di mercato transfrontaliere più significative (controparti centrali, CSD e sedi di negoziazione) e per tutti i prestatori di servizi per le cripto-attività (crypto-asset service providers, CASP)".

63. Esma, Response to the EC Consultation on the review of Regulation (EU) 2023/1114 (MiCA), 30 settembre 2026, ove evidenzia: "ESMA's experience to date suggests that MiCA provided a solid framework for investor protection through its conduct, governance and disclosure requirements applicable to CASPs. However, the level of investor protection under MiCA remains less comprehensive and distinct from the regulatory framework applicable to traditional financial instruments. This distinction and the co-existence in the crypto space of traditional financial services providers and entities specialised in services in crypto-assets create the risk of duplicative requirements and legal uncertainty, thereby increasing the burden on firms and reducing investor protection in crypto assets. ESMA invites the Commission to consider these regulatory frictions when assessing the effectiveness of the EU rulebook in its MiCA review".

64. Esma, Union Strategic Supervisory Priorities, 2026.

65. Consob, Piano strategico 2025-2027, p. 2.

66. F. Bassan, L'era ibrida. cit. p. 87. di avviare il processo bottom-up del circolo regolatorio, in base al quale la disciplina applicativa e poi quella normativa vengono formulate a partire dalle prassi dei mercati.

BANCA D'ITALIA

DAL CONSUMATORE DIGITALE AL CONSUMATORE AGENTICO: INFRASTRUTTURE E REGOLE DEI SERVIZI DI PAGAMENTO EUROPEI VERSO IL 2030.

(di Armando Di Cello)

Il contributo esamina l'evoluzione del mercato europeo dei pagamenti nella prospettiva del 2030, muovendo dalla progressiva formazione di un'infrastruttura ibrida, nella quale moneta pubblica e privata, sistemi tradizionali e tecnologie basate sulla tokenizzazione saranno destinati a coesistere. Su questa infrastruttura è destinato a innestarsi il commercio agentico, nel quale sistemi di intelligenza artificiale potranno ricercare beni e servizi, confrontare le offerte e avviare pagamenti sulla base di istruzioni e limiti definiti dall'utente. Il contributo analizza le conseguenze di questa trasformazione sulla posizione del consumatore, soffermandosi brevemente sull'adeguatezza delle categorie giuridiche proprie della disciplina tradizionale dei servizi di pagamento e sull'effettività delle tutele riconosciute agli utenti.

SOMMARIO: 1. Premessa. Dal consumatore digitale al consumatore agentico – 2. L'architettura europea dei pagamenti verso il 2030 – 3. I pagamenti agentici: nuovo paradigma, stesse regole? – 4. Conclusioni. Le priorità per la tutela dell'utente di servizi di pagamento nel 2030

1. Premessa. Dal consumatore digitale al consumatore agentico

Durante il primo quarto di secolo, l'avvento dell'economia digitale e del commercio elettronico ha portato con sé lo sviluppo di servizi e strumenti in grado di consentire a chiunque di pagare in maniera sicura e affidabile nel nuovo spazio digitale. La progressiva digitalizzazione dei servizi di pagamento ha infatti man mano modificato le modalità attraverso le quali il consumatore acquista beni o servizi, senza tuttavia alterare un elemento fondamentale del processo: la centralità dell'azione umana nel momento dell'inizializzazione del pagamento. Il paradigma dominante è rimasto quello del consumatore che seleziona il bene, sceglie uno strumento di pagamento e compie un atto riconoscibile attraverso il quale manifesta il proprio consenso a pagare. La tecnologia ha progressivamente ridotto i passaggi necessari e gran parte delle frizioni tra il bisogno e la sua soddisfazione, ma non ha eliminato la condotta attiva dell'utente nel momento autorizzatorio. In questo scenario, gli interventi legislativi UE di matrice consumeristica si sono focalizzati principalmente sul ribilanciamento delle asimmetrie informative tra consumatore e professionista e sulla regolazione dei servizi digitali, presupponendo un utente mediamente avveduto che esprimeva il proprio consenso negoziale attraverso l'interazione manuale e consapevole con interfacce web o applicative.

Oggi, il mercato dei servizi di pagamento si trova dinanzi a una nuova transizione epocale, in grado di ridisegnare non soltanto il modo in cui il valore viene trasferito, ma gli stessi binari tecnologici su cui viaggia il denaro. Sotto questo profilo, l'emersione dell'AI agentica[1] rappresenta un'innovazione dirompente per il commercio elettronico. Gli agenti di nuova generazione non si limitano a produrre informazioni o raccomandazioni, ma sono progettati per interpretare un obiettivo, scomporlo in una sequenza di attività, utilizzare strumenti e servizi esterni e, entro limiti prestabiliti, compiere autonomamente le azioni necessarie alla sua realizzazione. Nell'*e-commerce* ciò significa che ricerca del prodotto, comparazione delle offerte, selezione del venditore, negoziazione delle condizioni e completamento dell'acquisto possono progressivamente essere riuniti in un unico processo delegato.

1. Con *"agentic AI"* si fa riferimento all'evoluzione degli *agents AI* tradizionali (es. *bot* e/o *chatbot*) verso sistemi che agiscono e prendono autonomamente decisioni per conto dell'utente. Per alcune definizioni di "*agentic AI*", si veda: D. BIRCH, D. GAMBLE, *Agentic commerce and payments: Exploring the implications of robots paying robots,* in *Journal of Payments Strategy & Systems,* vol. 19, n. 1*, 2025*; R. SAPKOTA, K. I. ROUMELIOTIS, and M. KARKEE, *AI Agents vs. Agentic AI: A Conceptual Taxonomy, Applications and Challenges, in Information Fusion,* vol. 126, 2026; o, ancora, R. YINWANG *et al.* in, *AI Agents and Agentic AI-Navigating a Plethora of Concepts for Future Manufacturing,* in *Journal of Manufacturing Systems,* vol. 83, 2025, secondo cui l'*agentic AI* è un paradigma emergente nell'intelligenza artificiale che denota sistemi autonomi in grado di perseguire in modo indipendente obiettivi complessi con una supervisione umana minima in ambienti dinamici e incerti. Viene espressamente introdotto il concetto di *"agenticness"* (agenticità), definito come il grado in cui un sistema può raggiungere in modo adattivo obiettivi complessi in ambienti dinamici con una supervisione diretta limitata. Secondo gli autori, l'agenticità non è una classificazione binaria ("agentico" vs "non-agentico"), ma uno spettro graduale. Un sistema AI transita naturalmente verso un sistema di *agentic AI* man mano che le sue capacità aumentano. Nello stesso senso, si veda anche: D. B. ACHARYA, K. KUPPAN, B. DIVYA, *Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey*, in *IEEE Access*, vol. 13, 2025.

Nell'ambito dei servizi di pagamento, il precipitato più evidente di questa trasformazione è rappresentato dal venir meno della necessità che l'utente impartisca un ordine puntuale in corrispondenza di ogni singolo passaggio dell'operazione. L'avvio della singola transazione diviene il risultato di un processo decisionale mediato dalla macchina, svolto nell'ambito di un'autorità precedentemente delegata[2].

Sebbene l'adozione di questi strumenti sia ancora in fase di sperimentazione, le dimensioni prospettiche del fenomeno sono tutt'altro che irrilevanti[3]; esse descrivono un ordine di grandezza sufficiente a mostrare perché le principali piattaforme tecnologiche stiano già investendo nello sviluppo di protocolli destinati a consentire all'AI agentica di interoperare con i principali sistemi di pagamento[4].

In brevissimo tempo, alla figura del consumatore digitale, che conserva un ruolo diretto e riconoscibile nella disposizione dell'operazione di pagamento, potrebbe affiancarsi quella delegata e adattiva del consumatore agentico. Questi cambiamenti impongono una riflessione urgente sull'adeguatezza delle categorie giuridiche e sull'effettività delle tutele proprie della disciplina tradizionale del diritto dei consumatori e, più nello specifico, di quella dei servizi di pagamento.

2. L'architettura europea dei pagamenti verso il 2030

L'affermazione del commercio agentico si innesta nel più ampio processo di ridefinizione dell'architettura europea dei pagamenti, la cui portata si coglie appieno assumendo la centralità della dimensione infrastrutturale quale presidio dell'autonomia strategica e della sovranità monetaria dell'UE. In questa prospettiva, la traiettoria dell'Eurosistema verso il 2030 è caratterizzata dalla complessa transizione verso il paradigma del Web3 *(DLT e blockchain),* la cui affermazione ridisegna la configurazione stessa delle infrastrutture di pagamento attraverso l'introduzione della programmabilità e l'integrazione contestuale di processi storicamente disaggregati, quali la messaggistica, la riconciliazione e il regolamento definitivo.

La strategia tracciata dall'Eurosistema[5] ricava da questo mutamento una tassonomia dei nuovi *asset* digitali nettamente ripartita tra dimensione pubblica e privata, ponendosi a salvaguardia del *two-tier monetary system* e preservando la funzione di ancoraggio della moneta di banca centrale. La componente pubblica si articola lungo due direttrici distinte: sul versante *retail*, nel progetto dell'Euro digitale[6]; sul versante *wholesale*, nelle iniziative *Pontes* e *Appia*[7], volte ad assicurare il regolamento in moneta di banca centrale delle transazioni basate su DLT. La componente privata si compone, invece, dei depositi tokenizzati delle banche commerciali e delle *stablecoin* euro-denominate conformi alla disciplina MiCAR[8].

Queste iniziative, siano esse di matrice pubblica o privata, non devono essere intese quali soluzioni disorganiche, bensì come componenti complementari della medesima architettura monetaria digitale a due livelli. L'innovazione nell'ambito della moneta privata non recide infatti il vincolo funzionale con la moneta di banca centrale, che rimane presidio ineludibile della convertibilità alla pari e dell'unicità della moneta. L'obiettivo finale – che va oltre il tentativo di affrancarsi dai circuiti di carte e dai *digital wallet* gestiti da operatori extra-UE[9] – è quello di dotare l'Europa di una gamba monetaria per la gestione delle operazioni nei mercati del Web3, scongiurando il rischio che *stablecoin*

---

2. S. DAVIDOVIC, H. TOURPE, *How Agentic AI Will Reshape Payments*, International Monetary Fund, Washington D.C., Note n. 2026/004, aprile 2026, p. 5, secondo cui: *«[T]his evolution can be characterized as a shift from explicitly human-initiated transactions ("click-to-pay") toward agent-mediated decision processes ("decide-to-pay"), in which execution increasingly occurs at machine speed and across multiple layers of the payment value chain, subject to predefined objectives, constraints, and governance arrangements»*.

3. Secondo alcune stime, il valore globale delle transazioni riconducibili al commercio agentico potrebbe raggiungere 1,5 trilioni di dollari entro il 2030, rispetto agli 8 miliardi stimati per il 2026. Stime più ampie, che considerano il valore complessivo del commercio abilitato dall'AI agentica, prospettano invece fino a 17,5 trilioni di dollari entro il 2030, con circa il 30% del valore delle transazioni del commercio digitale potenzialmente influenzato da sistemi agentici. Cfr. JUNIPER RESEARCH, *Agentic Commerce Market: 2026-2031*, disponibile in: <https://www.juniperresearch.com/research/fintech-payments/ecommerce/agentic-commerce-research-report/>; DELOITTE, *The Future of Commerce in an Agentic World: How Agentic AI Will Reshape Commerce and What Payment Networks Must Do Next*, agosto 2025, , disponibile in: <https://www.deloitte.com/us/en/Industries/financial-services/articles/how-agentic-ai-is-transforming-e-commerce-and-commerce-payments.html>.

4. Tra le principali iniziative di mercato si segnalano: *Agentic Commerce Protocol* (ACP) di OpenAI e Stripe, *Rufus e Buy for Me* di Amazon, *Universal Commerce Protocol* (UCP) di Google, *Visa Intelligent Commerce* e *Mastercard Agent Pay*. Per una sintesi delle caratteristiche tecniche dei protocolli citati, v. S. DAVIDOVIC, H. TOURPE, *How Agentic AI Will Reshape Payments*, cit., p. 13. Queste soluzioni costituiscono, allo stato, standard tecnici e sperimentazioni di mercato.

5. BANCA CENTRALE EUROPEA, *The Eurosystem's Comprehensive Payments Strategy*, marzo 2026, disponibile in: <https://www.ecb.europa.eu/press/pubbydate/2026/html/ecb.eurosystemcomprehensivepaymentsstrategy202603.en.html>.

6. L'Euro digitale è una passività della Banca Centrale Europea concepita per preservare, anche nell'economia digitale, l'accesso diretto dei cittadini alla moneta pubblica di banca centrale, quale complemento digitale del contante. Nell'ottobre 2025 il Consiglio direttivo della BCE ha deciso di proseguire il progetto con l'obiettivo di essere pronto a una possibile emissione nel 2029, subordinatamente all'adozione del relativo quadro legislativo; una fase pilota, con le prime transazioni, potrebbe iniziare già dalla metà del 2027.

7. Sulle iniziative *Pontes* e *Appia*, attraverso cui l'Eurosistema persegue una strategia a doppio binario per l'integrazione della DLT nei pagamenti *wholesale*, v. BANCA CENTRALE EUROPEA, *Tokenisation and DLT*, disponibile in: <https://www.ecb.europa.eu/paym/dlt/html/index.en.html>.

8. Tra le principali iniziative europee si segnalano *Qivalis*, progetto consortile paneuropeo partecipato da 37 istituzioni finanziarie e volto all'emissione di una stablecoin euro-denominata, ed *EUR-BANK*, progetto di Bancomat S.p.A. dedicato principalmente all'ecosistema italiano dei pagamenti.

9. Il tema della dipendenza da operatori e infrastrutture extra-UE conserva una posizione centrale nella ridefinizione del sistema europeo dei pagamenti. Secondo la BCE, oltre due terzi delle transazioni con carta nell'area dell'euro sono elaborate sulla base di regole commerciali definite da società non europee e 13 Paesi dell'area dell'euro dipendono da circuiti internazionali di carte o da soluzioni *wallet-based* per i pagamenti effettuati presso i punti vendita.

globali sostituiscano il regolamento finale in moneta di banca centrale. La vera sfida, pertanto, non si giocherà nella contrapposizione tra moneta pubblica e moneta privata, quanto nella capacità di prevenire la frammentazione del mercato interno e di mantenere il controllo sui binari tecnologici attraverso cui circola il valore. Nel prossimo futuro, si delineerà così un ecosistema finanziario strutturalmente ibrido, nel quale la persistenza e la modernizzazione delle infrastrutture tradizionali convergeranno verso le nuove forme di trasferimento del valore basate sulla tokenizzazione e sui registri distribuiti (DLT).

A fronte della riconosciuta centralità del controllo infrastrutturale, è necessario poi comprendere come questa complessa architettura possa interfacciarsi in sicurezza con sistemi agentici di intelligenza artificiale[10]. È in questo punto di intersezione che si producono conseguenze profonde sulla posizione del consumatore finale e che si rende indispensabile strutturare adeguati presidi per fronteggiare i nuovi rischi emergenti.

3. I pagamenti agentici: nuovo paradigma, stesse regole?

Delegare l'avvio e la gestione di operazioni di pagamento a sistemi algoritmici autonomi solleva interrogativi cruciali circa la tenuta dell'attuale impianto normativo in materia.

La questione assume, in primo luogo, particolare rilievo nella prospettiva del diritto dei consumi. La tutela del consumatore digitale si è tradizionalmente fondata su un paradigma informativo, in base al quale l'autonomia decisionale dell'utente presuppone la disponibilità di informazioni non equivoche, complete e trasparenti. Nei mercati digitali questo paradigma è tuttavia da tempo sottoposto a tensione: piattaforme e sistemi di personalizzazione algoritmica non si limitano a informare il consumatore, ma contribuiscono a orientarne le scelte, facendo leva anche su condizioni di particolare suscettibilità. La stessa *Consumer Agenda 2030*[11], pur senza abbandonare il paradigma informativo, ne evidenzia i limiti di fronte a processi di profilazione, personalizzazione e influenza comportamentale[12]. La questione diviene allora distinguere la personalizzazione funzionale alle preferenze dell'utente da quella che utilizza inferenze sulla sua particolare suscettibilità per orientarne la decisione.

Con il commercio agentico si compie un passaggio ulteriore: la tecnologia non si limita più a orientare il contesto nel quale il consumatore decide, ma può intervenire direttamente nel processo decisionale, potendo assumere ed eseguire decisioni entro i limiti fissati dall'utente. La progressiva riduzione delle frizioni nell'atto del pagamento è stata finora considerata soprattutto in termini di efficienza; tuttavia, una frizione minima svolge anche una funzione cognitiva, rendendo percepibile il momento nel quale la decisione economica si traduce nei fatti in trasferimento di valore. Nel pagamento agentico questo momento può divenire pressoché invisibile, poiché decisione e inizializzazione dell'operazione si svolgono di fatto dietro le quinte. In aggiunta, la riduzione della consapevolezza immediata della spesa può accrescere il rischio di comportamenti finanziariamente insostenibili, specie se l'agente opera mediante strumenti di credito[13].

Il quadro normativo vigente non appare propriamente calibrato sulle specificità del commercio agentico, mancano regole espressamente volte a disciplinare l'ampiezza del mandato conferito all'agente (*e.g.* limiti dell'autonomia di spesa), la tracciabilità delle decisioni assunte dal sistema e le conseguenze derivanti da un eventuale scostamento rispetto agli interessi o alla situazione finanziaria dell'utente. Il problema non è quindi soltanto quello di provare ad applicare categorie esistenti a un nuovo strumento tecnologico, ma di verificare se queste categorie siano sufficienti a governare una delega di spesa esercitata autonomamente da un sistema algoritmico.

In secondo luogo, la questione assume ulteriore rilevanza sotto il più specifico profilo della disciplina dei servizi di pagamento. Un primo nodo riguarda la formazione del consenso e l'inquadramento del soggetto che mette a disposizione il servizio di pagamento agentico. La PSD2 stabilisce che, in mancanza del consenso del pagatore, l'operazione

10. La programmabilità e la rapidità di regolamento proprie delle infrastrutture DLT possono favorire l'integrazione con protocolli agentici, prospettando sistemi finanziari nativamente digitali in grado di automatizzare i flussi di pagamento e ridurre gli attriti delle infrastrutture tradizionali. In questa direzione si collocano, tra l'altro, meccanismi di attestazione sicura *off-chain*, come ERC-1812, utilizzabili da *smart contracts* per verificare identità, attributi e vincoli prima dell'autorizzazione, nonché standard quali ERC-6900, per l'applicazione di limiti di spesa e altri controlli sui portafogli programmabili, ed ERC-8004, volto a introdurre registri *on-chain* per l'identità, la validazione e la reputazione degli agenti. V. S. DAVIDOVIC, H. TOURPE, *How Agentic AI Will Reshape Payments*, cit., p. pp. 9 e 14.

11. Adottata dalla Commissione europea il 19 novembre 2025 quale nuovo quadro strategico della politica europea dei consumatori per il quinquennio successivo, v. COMMISSIONE EUROPEA, 2030 Consumer Agenda, 19 novembre 2025, disponibile in: <https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/2030-consumer-agenda_en>.

12. V. L. ZOBOLI, *Vulnerabilità dinamica nei mercati digitali. Riflessioni a partire dalla Consumer Agenda 2030*, in Dialoghi di Diritto dell'Economia, fasc. 2/2026, agosto 2026, sul concetto di *"architettura della scelta"*, inteso quale ambiente decisionale costruito e personalizzato dalle piattaforme digitali attraverso sistemi di raccomandazione, *ranking* e altre tecniche di personalizzazione, idoneo a incidere sulle condizioni entro cui le preferenze del consumatore vengono formate ed espresse.

13. In tal senso, M.C. Paglietti osserva come la vulnerabilità del consumatore nei pagamenti digitali sia legata anche alla progressiva "invisibilità" dell'atto di pagamento, divenuto dematerializzato e quasi impercettibile. Ne consegue una riduzione del c.d. *"pain of paying"*, ossia delle emozioni negative associate alla spesa, avvertite più intensamente nel pagamento in contanti e progressivamente meno con carte e dispositivi digitali; la minore percezione del pagamento può così accrescere l'esposizione del consumatore al rischio di sovraindebitamento. V. M.C. PAGLIETTI, *The Vulnerable Digital Payment Systems Consumer. A New Normative Standard?*, in V. PROFETA (a cura di), *Competition and Payment Services. Conference Papers,* Banca d'Italia, Rome, 16-17 June 2022, Quaderni di Ricerca Giuridica della Consulenza Legale, n. 93, Banca d'Italia, dicembre 2022, pp. 34-35.

è considerata non autorizzata, ma ammette al contempo che lo stesso possa essere prestato prima o, se concordato con il PSP, anche dopo l'esecuzione dell'operazione, nonché per il tramite del beneficiario[14] o di un prestatore di servizi di disposizione di ordine di pagamento[15]. La disciplina vigente conosce, dunque, forme di autorizzazione non contestuale e ipotesi nelle quali il consenso è prestato per il tramite di soggetti diversi dal pagatore. Questi soggetti sono, tuttavia, specificamente individuati all'interno della PSD2. L'intervento di un agente AI nell'iniziazione del pagamento pone quindi un problema preliminare di qualificazione soggettiva del *provider* che offre il servizio all'utente, potenzialmente estraneo alle categorie contemplate dalla disciplina vigente. Il servizio di pagamento agentico non costituisce, infatti, una fattispecie autonomamente tipizzata tra i servizi di pagamento elencati nell'allegato I alla PSD2, né trova una disciplina specifica nel testo di compromesso del pacchetto PSD3/PSR, tuttora in corso di adozione. A seconda delle funzioni concretamente svolte dall'agente, occorre pertanto stabilire se l'attività del *provider* possa essere ricondotta a uno dei servizi di pagamento già disciplinati, con conseguente assoggettamento al relativo regime autorizzativo, oppure se possa essere prestata attraverso forme di collaborazione con un PSP già autorizzato.

Ulteriore profilo problematico attiene alla *Strong Customer Authentication* (SCA). Ai sensi dell'art. 97 della PSD2, salve le ipotesi di esenzione, il PSP deve applicare l'autenticazione forte quando il pagatore dispone un'operazione di pagamento elettronico[16]; per le operazioni a distanza, inoltre, l'autenticazione deve essere dinamicamente collegata a uno specifico importo e a uno specifico beneficiario (c.d. *dynamic linking*)[17]. La disciplina presuppone, quindi, una stretta relazione tra autenticazione dell'utente e operazione successivamente eseguita. Nel pagamento agentico questa relazione tende invece a spezzarsi. L'utente può autenticarsi nel momento in cui conferisce all'agente un mandato definito soltanto sulla base di parametri generali – una soglia di spesa, una categoria di beni o una determinata finalità – mentre importo effettivo, beneficiario e momento dell'operazione vengono individuati successivamente dall'agente. Una SCA effettuata al momento del conferimento del mandato potrebbe pertanto non soddisfare il requisito del *dynamic linking* rispetto alla singola operazione; al contrario, richiedere una nuova autenticazione dell'utente nel momento in cui l'agente paga finirebbe per ridurre significativamente l'autonomia che caratterizza il modello.

A ciò si aggiunga, inoltre, che l'autenticazione del pagatore non presuppone, di per sé, anche la verifica contestuale dell'identità dell'agente cui il mandato è stato conferito, né che la singola operazione sia stata effettivamente disposta entro i limiti del mandato stesso. Il pagamento agentico impone quindi di tenere distinti il momento dell'autenticazione dell'utente, quello dell'identificazione dell'agente e quello della verifica della conformità dell'operazione ai limiti della delega. Si tratta di esigenze che l'attuale disciplina della SCA, costruita attorno al rapporto tra pagatore, PSP e singola operazione, non contempla espressamente.

In conclusione, residua il tema dell'allocazione della responsabilità in caso di operazioni di pagamento non autorizzate. La PSD2 costruisce il relativo regime secondo un criterio di responsabilità oggettiva del PSP del pagatore, allocando il rischio dell'operazione non autorizzata sul soggetto ritenuto maggiormente in grado di prevenirlo e sopportarne le conseguenze, salvo che la perdita sia riconducibile alla frode dell'utente o alla violazione, con dolo o colpa grave, degli obblighi posti a suo carico.

L'interposizione di un agente AI rende tuttavia meno immediata l'applicazione di questo schema, perché introduce un ulteriore livello tra la volontà del pagatore e l'esecuzione dell'operazione. La prima difficoltà consiste nello stabilire quando un pagamento disposto dall'agente possa considerarsi effettivamente non autorizzato. L'operazione potrebbe eccedere i limiti del mandato, derivare da un'erronea interpretazione delle istruzioni, da *hallucination*, da una *prompt injection* o da altre forme di compromissione del sistema[18]. In queste ipotesi non è sempre agevole distinguere tra operazione priva del consenso del pagatore, inesatta esecuzione del mandato conferito all'agente e malfunzionamento del servizio tecnologico. La qualificazione della fattispecie non è priva di conseguenze, poiché da essa dipende il criterio di imputazione della perdita tra i diversi soggetti coinvolti e, di riflesso, la disciplina applicabile ai rapporti che intercorrono tra essi.

Il provider dell'agente potrebbe essere distinto dal PSP e non rientrare direttamente nel perimetro soggettivo della

14. L'esempio tipico di operazione nella quale il consenso del pagatore è prestato per il tramite del beneficiario è l'addebito diretto *(SEPA Direct Debit – SDD)*. Ai sensi dell'art. 4, punto 23, della Direttiva (UE) 2015/2366, per «addebito diretto» si intende «*un servizio di pagamento per l'addebito di un conto di pagamento del pagatore in cui un'operazione di pagamento è disposta dal beneficiario in base al consenso dato dal pagatore al beneficiario, al prestatore di servizi di pagamento del beneficiario o al prestatore di servizi di pagamento del pagatore stesso*».

15. V. art. 64 della Direttiva (UE) 2015/2366 (PSD2).

16. Per autenticazione forte del cliente si intende un'autenticazione basata sull'uso di almeno due elementi, tra loro indipendenti, appartenenti alle categorie della conoscenza, del possesso e dell'inerenza. V. art. 4, punto 30, della Direttiva (UE) 2015/2366 (PSD2).

17. V. art. 97, par. 2, della Direttiva (UE) 2015/2366 (PSD2).

18. Sui rischi derivanti dalle *hallucinations*, v. I. ALDASORO, L. GAMBACORTA, A. KORINEK, V. SHREETI, M. STEIN, *Intelligent Financial System: How AI Is Transforming Finance*, BIS Working Papers, n. 1194, Bank for International Settlements, giugno 2024; sul rischio di manipolazione degli agenti attraverso attacchi di *prompt injection*, v. J. SALMON, J. BLACK, L. CRAWFORD, D. LEE, F. SCRIVENS, *Agentic AI in Financial Services: Regulatory and Legal Considerations*, Hogan Lovells, 5 dicembre 2025, ove si evidenzia come l'accesso degli agenti AI a sistemi e reti interne possa accrescere i rischi di *cybersecurity*, consentendo a soggetti malevoli di influenzarne o controllarne il comportamento anche attraverso attacchi di *prompt injection*.

PSD2. Occorre allora stabilire se e in quale misura la responsabilità debba continuare a gravare sul PSP nei confronti dell'utente e come debbano essere regolati gli eventuali rapporti di regresso verso il fornitore del servizio agentico[19]. Analogamente, è necessario chiarire quando la configurazione o l'utilizzo dell'agente da parte del pagatore possa incidere sulla valutazione della colpa grave dell'utente che, nel sistema attuale, incide sull'allocazione della perdita[20]. Resta da verificare se, e in quale misura, la condotta dell'utente debba conservare il medesimo rilievo quando una parte del processo decisionale e operativo è affidata a un agente autonomo. La valutazione della colpa grave non può infatti prescindere dalle condizioni concrete nelle quali l'utente opera e dal suo grado di vulnerabilità. Se le categorie tradizionali fanno riferimento soprattutto a condizioni relativamente stabili o riconoscibili, quali l'età o il livello di alfabetizzazione digitale, gli ambienti digitali possono generare forme di vulnerabilità dinamica e contestuale, legate alla profilazione e a particolari condizioni di suscettibilità del singolo utente. Anche sotto questo profilo, il commercio agentico impone quindi di interrogarsi sulla tenuta del tradizionale equilibrio tra consumatore medio e consumatore vulnerabile[21].

L'interposizione dell'agente complica anche la ricostruzione probatoria dell'operazione. Diventa infatti necessario accertare l'esistenza e l'ampiezza del mandato conferito dall'utente, ricostruire l'operazione concretamente disposta e verificare se essa rientrasse nei limiti dell'autorità attribuita, nonché individuare i mezzi di prova idonei a documentare le suddette circostanze.

In definitiva, appare evidente come la disciplina vigente, costruita essenzialmente sul rapporto tra pagatore e PSP, non offra ancora criteri specifici per governare questa ulteriore articolazione della catena decisionale e per ripartire il rischio tra utente, PSP ed eventuale *provider* dell'agente.

4. Conclusioni. Le priorità per la tutela dell'utente di servizi di pagamento nel 2030

L'integrazione dei modelli di AI agentica all'interno delle piattaforme di pagamento rappresenta un'evoluzione dal potenziale dirompente. Tuttavia, il principale elemento di tensione deriva dall'incontro di due logiche di funzionamento architetturale profondamente diverse.

Da un lato, gli agenti AI operano attraverso processi probabilistici, caratterizzati da un certo margine di imprevedibilità in grado di produrre risultati diversi pur partendo da condizioni simili; dall'altro, i sistemi di pagamento si fondano su regole certe e predeterminate secondo una logica tipicamente deterministica. La principale sfida consiste quindi nel consentire all'agente di esercitare autonomia nella fase decisionale senza trasferire l'incertezza propria del modello algoritmico alla fase di esecuzione del pagamento. In questa prospettiva, la separazione netta tra una componente agentica deputata all'interpretazione dell'intento dell'utente e una componente incaricata di verificare con estrema certezza le condizioni dell'operazione e darvi esecuzione appare un presupposto essenziale per preservare la fiducia nell'infrastruttura dei pagamenti[22]. A questa incompatibilità architetturale si accompagnano poi specifici rischi per la tutela del consumatore. L'opacità dei processi decisionali, combinata con la possibilità di attribuire all'agente accessi continuativi a strumenti e conti di pagamento e ampi margini di autonomia, può rendere meno trasparente la formazione della scelta e favorire condotte non necessariamente coerenti con l'interesse dell'utente nel lungo periodo.

La tutela dell'utente di servizi di pagamento dovrà anzitutto misurarsi con la necessità di delimitare in modo effettivo l'autonomia attribuita all'agente. Il mandato dovrebbe essere circoscritto a parametri verificabili relativi, quantomeno, alla durata della delega, ai limiti di spesa, alle tipologie di operazioni consentite e alle eventuali controparti, preservando la possibilità per l'utente di modificarlo o revocarlo in qualsiasi momento[23]. La delimitazione dell'autorità conferita non esaurisce, tuttavia, il problema. Occorre anche poter identificare con certezza l'agente e verificare che sia effettiva-

19. Quale possibile criterio per la regolazione dei rapporti interni tra i diversi soggetti coinvolti può richiamarsi l'art. 92 della Direttiva (UE) 2015/2366 (PSD2), relativo al diritto di regresso tra prestatori di servizi di pagamento e altri intermediari.

20. Sul punto, v. I. ALDASORO, L. GAMBACORTA, A. KORINEK, V. SHREETI, M. STEIN, *Intelligent Financial System: How AI Is Transforming Finance,* cit., i quali, nel rilevare i rischi derivanti dall'impiego di sistemi di IA generativa e agenti autonomi nel settore finanziario, evidenziano altresì l'esigenza di assicurare maggiore chiarezza nell'allocazione delle relative responsabilità.

21. Si veda, in proposito, BEUC, *EU Consumer Protection 2.0. Structural Asymmetries in Digital Consumer Markets*, Bruxelles, 2021.

22. In questa prospettiva, il Fondo Monetario Internazionale propone un modello a tre livelli. Il primo (*intent and orchestration layer*) è affidato ai sistemi agentici e concentra la componente probabilistica, deputata a interpretare gli obiettivi dell'utente e a formulare l'azione da intraprendere. Il secondo (*control and authorization layer*) opera invece come filtro deterministico: verifica che l'azione proposta rispetti mandato, limiti, condizioni e controlli applicabili e la trasforma, solo in caso positivo, in un'istruzione di pagamento autorizzata. Il terzo livello (*settlement layer*) esegue infine l'operazione secondo logiche deterministiche, senza reinterpretare né modificare la decisione a monte. La separazione tra questi livelli mira così a impedire che l'incertezza propria del ragionamento agentico si propaghi alle fasi di autorizzazione, esecuzione e regolamento. V. S. DAVIDOVIC, H. TOURPE, *How Agentic AI Will Reshape Payments*, cit., pp. 8-10.

23. Una possibile risposta tecnica è offerta dall'*Agent Payments Protocol* (AP2) che associa le azioni dell'agente a mandati crittograficamente verificabili, nei quali possono essere predeterminati l'identità del soggetto, l'ambito e i limiti della delega, nonché le condizioni alle quali l'operazione può essere autorizzata. La verifica crittografica consente tuttavia di accertare soltanto che l'agente abbia agito entro i limiti formalmente codificati, non necessariamente che il risultato perseguito corrisponda alla volontà sostanziale dell'utente. Resta quindi da stabilire, ad esempio, se l'acquisto di un prodotto diverso da quello effettivamente inteso dall'utente, ma conforme ai parametri formalmente impartiti all'agente, integri un'operazione "non autorizzata" ai sensi della PSD2. È in questa zona intermedia che le categorie tradizionali mostrano le maggiori tensioni.

mente legittimato ad agire per conto dell'utente. In questa prospettiva, forme di *Know Your Agent* (KYA) potrebbero affiancarsi alla *Strong Customer Authentication* (SCA) e agli ordinari presidi di identificazione della clientela, introducendo un livello di verifica specificamente riferito al soggetto tecnologico che interviene nell'operazione[24]. Mandato e identificazione devono poi potersi tradurre in processi verificabili anche in caso di contestazione. Diventa quindi essenziale assicurare la tracciabilità dell'attività dell'agente e individuare mezzi di prova idonei a ricostruire quale sistema abbia operato, sulla base di quale delega, entro quali limiti e a seguito di quale evento, assicurando la disponibilità di elementi verificabili e di *audit trail* sufficienti a collegare *ex post* la volontà dell'utente all'ordine di pagamento[25]. Da questa ricostruzione dipende anche la possibilità di distinguere tra operazione non autorizzata, inesatta esecuzione del mandato e malfunzionamento del servizio, nonché di definire con maggiore certezza il riparto delle responsabilità tra utente, PSP e *provider* dell'agente.

La tutela dovrà inoltre considerare che l'automazione può incidere sul grado di esposizione del consumatore a nuove condizioni di vulnerabilità. Un agente dotato di accesso continuativo agli strumenti di pagamento e capace di operare sulla base di dati personali e comportamentali può interagire con forme di vulnerabilità dinamica dell'utente. La valutazione della sua condotta, in particolare ai fini della colpa grave, dovrà quindi essere calibrata sulle concrete condizioni nelle quali l'interazione con il sistema agentico si è svolta.

Infine, il rafforzamento della tutela richiede necessariamente un corrispondente adeguamento degli strumenti di vigilanza e di *enforcement*. La vulnerabilità dinamica presenta infatti un tratto che la rende difficilmente riconducibile alle logiche tradizionali dell'illecito consumeristico, ossia la sua tendenza a rimanere incorporata nei processi algoritmici che governano profilazione e personalizzazione. L'oggetto stesso della vigilanza tende così a spostarsi dai risultati visibili ai processi che li hanno generati, imponendo l'accesso a informazioni e logiche decisionali spesso nella disponibilità esclusiva degli operatori[26]. Questa smaterializzazione dell'oggetto dell'attività di vigilanza — che sposta l'indagine dai risultati osservabili ai processi latenti che li hanno generati — paralizza infatti sia gli strumenti di tutela a disposizione del consumatore che quelli a disposizione dell'*enforcement* pubblico. Sul piano della vigilanza, infatti, la marcata personalizzazione dell'esperienza digitale determina una ancora più marcata asimmetria informativa tra autorità e soggetti vigilati. Gli operatori dispongono di una conoscenza diretta dei criteri di profilazione e personalizzazione incorporati nei propri sistemi, mentre le autorità sono chiamate a ricostruirne il funzionamento sulla base di informazioni tecniche spesso difficilmente accessibili. Non è quindi sufficiente predisporre regole sostanziali adeguate a tutela del consumatore, ma occorre anche dotare le autorità di strumenti e poteri idonei a comprendere il funzionamento dei processi algoritmici e valutarne concretamente gli effetti sull'interazione con l'utente. Le autorità di settore saranno chiamate a dotarsi di nuovi strumenti di *audit* algoritmico, atti a verificare le logiche decisionali, le soglie di rischio e i modelli comportamentali che agiscono negli ecosistemi. Ne discende la necessità di integrare i sistemi agentici negli *stress test* e nelle analisi di scenario, aggiornando se necessario le linee guida di supervisione e potenziando tanto le capacità computazionali a disposizione dei controlli quanto il coordinamento tra singole autorità[27].

24. In questa direzione si collocano *Visa Intelligent Commerce* e *Mastercard Agent Pay*, iniziative concentrate su modelli di *Know Your Agent* (KYA) e volte a fornire meccanismi di registrazione idonei a distinguere gli agenti legittimi da *bot* malevoli. A ciò si affiancano meccanismi di autorizzazione tokenizzata, che consentono agli agenti di operare mediante strumenti di pagamento previamente approvati dall'utente senza accedere direttamente alle relative credenziali, riducendo così l'esposizione dei dati sensibili e rafforzando i presidi di sicurezza dell'operazione.

25. Sul piano della *governance*, l'AI Act prevede già, per i sistemi classificati ad alto rischio – tra i quali rientrano, ad esempio, quelli destinati alla valutazione del merito creditizio delle persone fisiche – specifici presidi di tracciabilità e controllo, tra cui la registrazione automatica degli eventi (logging), la documentazione del funzionamento del sistema e meccanismi di supervisione umana idonei a consentire il monitoraggio, l'intervento e, ove necessario, l'interruzione dell'operatività del sistema. V. artt. 12-14 del Regolamento (UE) 2024/1689 (AI Act). Tali obblighi non si estendono, tuttavia, automaticamente a un sistema agentico per il solo fatto di essere impiegato nell'inizializzazione o nell'esecuzione di pagamenti, attività che non è autonomamente qualificata come ad alto rischio dall'Allegato III. Sul punto, con specifico riferimento all'impiego dell'IA agentica nei servizi finanziari e alla necessità di assicurare *audit trail*, documentazione della logica decisionale e forme effettive di *human oversight*, v. P. ATHANASSIOU, S. CZÁK-LUDWIG, N. DI GABRIELE, *Neo-conglomerates and EU Regulatory Perimeter Challenges – State of Play and Evaluation of Policy Options*, ECB Occasional Paper Series, n. 394, 2026, p. 17.

26. Sulla difficoltà di accertamento dell'illecito algoritmico, dovuta all'opacità dei sistemi di profilazione e targeting e alla conseguente asimmetria conoscitiva tra operatori e autorità di vigilanza, v. L. ZOBOLI, *Vulnerabilità dinamica nei mercati digitali. Riflessioni a partire dalla Consumer Agenda 2030*, cit., pp. 312-313; F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge (MA), 2015.

27. In questa direzione, v. P. ATHANASSIOU, S. CZÁK-LUDWIG, N. DI GABRIELE, *Neo-conglomerates and EU Regulatory Perimeter Challenges*, cit., p. 17.

ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI (IVASS)

ASSICURARE L'IMPIEGO NON PROFESSIONALE DI AGENTI IA

(di Vincenzo Orsini)

La diffusione nel largo consumo di agenti di intelligenza artificiale, capaci di compiere operazioni per conto dell'utente, pone il problema dei danni che tali sistemi possono arrecare a terzi. Il contributo si interroga sulla possibilità, per il consumatore che se ne avvale, di assicurare la propria responsabilità. Dopo aver rilevato che l'AI Act non impone alcun obbligo a chi impiega sistemi di IA per scopi personali non professionali, e che le proposte di assicurazione obbligatoria presuppongono un'imputazione certa della responsabilità, l'indagine muove dalla nozione di interesse di cui all'art. 1904 c.c., mostrando che l'assicurabilità del rischio dipende dal criterio di imputazione applicabile. Vengono quindi vagliate le opzioni interpretative possibili, cioè la colpa, che circoscrive la responsabilità del consumatore alle istruzioni imprudenti, e la responsabilità da cosa in custodia, che gli imputa le conseguenze del funzionamento dell'agente, salvo il regresso verso il produttore per i danni derivanti da malfunzionamento. Quest'ultima appare la soluzione più convincente. L'esame del d.lgs. n. 160/2026 mostra infine che gli strumenti processuali da esso introdotti, e in particolare l'azione diretta nei confronti dell'assicuratore, presuppongono un criterio di imputazione che il legislatore non ha fissato, e suggerisce l'introduzione di una regola modellata sull'art. 2054 c.c.

SOMMARIO: 1. L'Agentic AI. 2. Il dato positivo. 3. La proposta di un'assicurazione obbligatoria. 4. Il problema dell'interesse all'assicurazione. 5. I criteri di imputazione della responsabilità. 6. Considerazioni conclusive.

1. L'AGENTIC AI

In una riflessione sulle prospettive future del diritto delle assicurazioni non può mancare il riferimento, ormai quasi rituale, ai sistemi di intelligenza artificiale (IA). Il tema, tuttavia, si arricchisce oggi di una declinazione nuova. La diffusione nel largo consumo di sistemi di IA agentica, in grado di compiere scelte e concludere operazioni per conto dell'utente, solleva interrogativi inediti sulla tutela del consumatore. La dottrina si è finora soffermata soprattutto sulle ricadute che l'impiego di tali sistemi da parte delle imprese di assicurazione può produrre sul mercato e sui rischi che ne derivano per gli assicurandi[1]. Qui si intende invece ribaltare la prospettiva, interrogandosi sulle conseguenze del ricorso all'IA da parte dei consumatori stessi.

I sistemi di IA generativa ai quali siamo ormai abituati sono essenzialmente conversazionali: interrogati dall'utente, producono un testo, un'immagine, un video o un documento, lasciando a chi li ha interpellati ogni decisione sul da farsi e ogni iniziativa conseguente. Il sistema agentico, invece, non si arresta alla produzione di un contenuto. Lo inserisce in una sequenza di azioni orientate a un risultato operativo, sceglie gli strumenti per conseguirlo e corregge il proprio percorso in funzione degli esiti intermedi. Muta, di conseguenza, la natura stessa del rischio[2]. Nel primo caso il problema giuridico si concentra sull'attendibilità degli *output*, esposti al rischio di allucinazioni, e sulle conseguenze dell'affidamento che l'utente vi ripone. Nel secondo, il rischio non attiene più soltanto all'esattezza di ciò che il sistema dice, ma investe la sua capacità di incidere direttamente sulla realtà.

Non si tratta di uno scenario futuribile. Gli assistenti di uso comune, come Claude[3], integrano ormai funzioni che consentono di navigare il *web*, compilare moduli, gestire la posta elettronica e completare acquisti per conto dell'utente, mentre i circuiti di pagamento hanno predisposto infrastrutture destinate ad autenticare l'agente e a registrare l'autorizzazione del consumatore[4]. L'impiego dell'agente fuoriesce così dal contesto imprenditoriale, per entrare nella vita quotidiana di chi agisce per scopi estranei alla propria attività professionale.

1. Per tutti, si v. M. Rabitti, Gli agenti di intelligenza artificiale nei servizi assicurativi, in corso di pubblicazione.
2. Cfr. A. Del Ninno, Impiegare gli agenti di intelligenza artificiale nell'attività di impresa, maggio 2026, disponibile su dirittobancario.it.
3. Maggiori informazioni sono reperibili su claude.com/it/product/cowork.
4. Il riferimento è alle soluzioni VISA Intelligent Commerce (visa.com/en-us/solutions/intelligent-commerce) e Mastercard Agent Pay (mastercard.com/it/it/business/intelligenza-artificiale/mastercard-agent-pay.html).

La dottrina ha colto in questo passaggio soprattutto un'opportunità[5]. Si è osservato che l'IA agentica, abbattendo i costi di ricerca e di elaborazione delle informazioni, potrebbe restituire al consumatore un'autentica autonomia decisionale e trasformarlo in un operatore avveduto, capace di esaminare e mettere a confronto ciò che il mercato gli offre. La medaglia ha però il suo rovescio. All'acquisto di autonomia corrisponde l'assunzione di un rischio, perché il sistema che agisce per conto del consumatore può arrecare danni anche a terzi. Occorre allora chiedersi chi sia chiamato a risponderne e se, e in quale misura, tale rischio possa trovare copertura sul mercato assicurativo. È da questi interrogativi che muove il presente contributo.

2. IL DATO POSITIVO

Sul piano del diritto positivo, l'*AI Act*[6] non offre una definizione di intelligenza artificiale agentica. L'agente IA rientra comunque nella nozione di «sistema di IA» di cui all'art. 3, punto 1, che si riferisce a sistemi «progettati per funzionare con livelli di autonomia variabili» i cui *output* «possono influenzare ambienti fisici o virtuali». Quando è basato su un modello di IA per finalità generali e può perseguire varie finalità, l'agente IA si qualifica inoltre come «sistema di IA per finalità generali» ai sensi dell'art. 3, punto 66. Ne consegue che la sua disciplina non è unitaria, ma dipende dalla finalità per la quale l'agente IA è impiegato e dal livello di rischio che ne deriva, secondo le disposizioni generali del regolamento.

Poiché il medesimo modello può essere integrato tanto in un sistema conversazionale quanto in un sistema agentico, ciò che caratterizza l'agente va ricercato nel funzionamento del sistema. Ai fini del presente lavoro si può allora intendere per agente IA un sistema che, ricevuto un obiettivo da chi lo utilizza, ne individua autonomamente le fasi e le esegue, servendosi di strumenti, applicazioni e risorse digitali, senza che ciascun passaggio debba essere necessariamente approvato da una persona.

La polivalenza dei sistemi agentici fa sì che la loro qualificazione dipenda dalla finalità cui sono concretamente destinati. L'agente IA costituisce un sistema ad alto rischio soltanto quando è impiegato in uno degli ambiti elencati nell'allegato III (modificabile dalla Commissione) o come componente di sicurezza di un prodotto soggetto alla normativa richiamata nell'allegato I. In tal caso il regolamento impone al fornitore, ossia chi sviluppa sistemi di IA, un articolato insieme di requisiti di progettazione e controllo, tra cui l'adozione di un sistema di gestione dei rischi e *standard* di qualità dei dati; e al *deployer*, cioè a chi utilizza il sistema sotto la propria autorità, di impiegarlo conformemente alle istruzioni, di affidarne la sorveglianza a persone competenti, di monitorarne il funzionamento e di conservarne i registri[7]. Quando invece l'agente non è un sistema ad alto rischio, il regolamento si limita a richiedere che le persone siano informate di interagire con un sistema di IA e che fornitori e *deployer* sostengano l'alfabetizzazione in materia di IA del proprio personale. Restano fermi, in ogni caso, gli obblighi che gravano a monte sui fornitori dei modelli per finalità generali sui quali l'agente è sviluppato.

Il consumatore, tuttavia, non è destinatario di alcuno di questi obblighi. Che non possa qualificarsi come fornitore è evidente; meno scontato, ma altrettanto chiaro nel testo, è che non sia neppure un *deployer*. L'art. 3, punto 4, esclude infatti da tale nozione chi utilizza il sistema nel corso di un'attività personale non professionale, e l'art. 2, par. 10, ribadisce che il regolamento non si applica agli obblighi dei *deployer* che siano persone fisiche e si avvalgano di sistemi di IA per scopi puramente personali. Il consumatore compare dunque nel regolamento soltanto come destinatario di tutele, mai come soggetto gravato da obblighi.

La scelta ha ragioni comprensibili. Gravare il privato di oneri pensati per l'organizzazione dell'impresa sarebbe stato sproporzionato, e il regolamento concentra coerentemente i presidi a monte, sui fornitori di sistemi e di modelli. Questa impostazione è convincente finché i sistemi a disposizione del consumatore restano strumenti di consultazione, i cui effetti si esauriscono nella sfera di chi li interroga, ma lo è meno quando il sistema agisce verso terzi, come accade in caso di impiego di sistemi agentici. In tal caso, infatti, i presidi *ex ante* gravano su chi progetta il sistema, che tuttavia non può prevedere gli obiettivi che ciascun utente gli assegnerà né le circostanze in cui si troverà a operare; l'utente, che quegli obiettivi definisce, non è tenuto ad alcuna cautela specifica e difficilmente disporrebbe, del resto, delle competenze necessarie per adottarla. Le conseguenze dell'azione dell'agente nei confronti dei terzi finiscono allora per essere affidate in larga misura ai rimedi *ex post*, e dunque alle categorie generali del diritto dei contratti e della responsabilità civile, chiamate a misurarsi con un'attività che non è più riconducibile per intero né alla volontà dell'utente né al progetto del fornitore.

5. Si v. A. Davola, R. Pardolesi, Il riscatto del consumatore. Ovvero: del valore competitivo dell'Agentic-AI nei fenomeni di consumo, in Danno resp., 3/2026, p. 277 ss.
6. Reg. 13 giugno 2024, n. 1689.
7. Occorre sottolineare che, quando un sistema per finalità generali è destinato a una finalità ad alto rischio, chi ne modifica in tal senso la destinazione risponde degli obblighi gravanti sui fornitori ai sensi dell'art. 25, par. 1, lett. c).

3. LA PROPOSTA DI UN'ASSICURAZIONE OBBLIGATORIA

Il rischio che l'impiego di agenti IA da parte dei consumatori proietta sui terzi è tutt'altro che trascurabile. Conviene precisare che il presente lavoro si occupa soltanto dei pregiudizi arrecati a terzi, lasciando da parte quelli che il consumatore subisce in proprio, come l'acquisto indesiderato o il contratto concluso oltre le sue intenzioni, che attengono ai rapporti con il fornitore del sistema e con le controparti e pongono problemi in larga parte diversi. La casistica, invero, è ampia[8]: l'agente IA, ad esempio, può ledere la reputazione altrui comunicando in nome dell'utente; può diffondere accidentalmente dati personali di terzi[9]; può danneggiare o compromettere il funzionamento di sistemi e servizi in rete; e può persino cagionare, attraverso dispositivi domestici connessi, danni fisici a persone.

Di fronte a rischi di questo tipo, e all'incertezza su chi debba sopportarne le conseguenze, si è guardato all'assicurazione come a uno strumento capace di garantire comunque il ristoro dei danneggiati[10].

L'idea si è affacciata presto nel dibattito europeo. Già la risoluzione del Parlamento europeo del 16 febbraio 2017 sulla robotica indicava nell'assicurazione obbligatoria una possibile soluzione alla complessità dell'attribuzione della responsabilità per i danni cagionati da robot sempre più autonomi, invitando la Commissione a valutare un regime che imponesse ai produttori e ai proprietari di specifiche categorie di robot di coprire i danni potenzialmente cagionati, affiancato da un fondo di garanzia per i casi di mancata copertura[11]. Il gruppo di esperti incaricato dalla Commissione di esaminare la responsabilità per le nuove tecnologie ha poi ritenuto che un'assicurazione obbligatoria della responsabilità possa essere tanto più opportuna quanto più il danno potenziale è frequente o grave e quanto meno è probabile che l'operatore sia in grado di risarcire individualmente le vittime[12], e la risoluzione del Parlamento europeo del 20 ottobre 2020 ha proposto di imporre agli operatori di sistemi ad alto rischio, soggetti a una responsabilità oggettiva, la stipula di un'assicurazione della responsabilità civile[13]. La proposta di direttiva sulla responsabilità da IA del 2022, infine, si limitava a rinviare a una successiva valutazione l'opportunità di introdurre regole di responsabilità oggettiva, eventualmente accompagnate da un obbligo assicurativo[14].

L'idea non è estranea al nostro ordinamento, che conosce da tempo forme di assicurazione obbligatoria e ne ha di recente introdotte di nuove. Tra le più note figurano, accanto alla RC auto, l'obbligo, posto a carico delle imprese, di assicurarsi contro i danni da eventi catastrofali e, da ultimo, quello di assicurare la responsabilità civile per la circolazione dei monopattini elettrici. Si tratta, tuttavia, di modelli eterogenei. L'assicurazione contro gli eventi catastrofali copre i danni subiti dallo stesso assicurato, al fine di mutualizzare un rischio che sfugge a ogni imputazione, e prescinde perciò da qualsiasi questione di responsabilità. La RC auto, e con essa l'obbligo esteso ai monopattini, è invece un'assicurazione della responsabilità civile, volta a contrastare il rischio di insolvenza del responsabile. Proprio per questo presuppone che sia già chiaro chi debba rispondere del danno. Il criterio di imputazione è fissato dall'art. 2054 c.c., e l'assicurazione si innesta su una responsabilità che la legge ha già allocato. Non a caso, la risoluzione del 2020 collocava l'obbligo assicurativo all'interno di un regime di responsabilità oggettiva dell'operatore.

L'assicurazione della responsabilità, in altri termini, segue la responsabilità e non può sostituirsi alla sua individuazione. Né l'obbligo potrebbe di per sé sciogliere il nodo dell'imputazione, perché l'assicuratore è tenuto a tenere indenne l'assicurato soltanto di quanto questi debba a un terzo in conseguenza di un fatto di cui sia responsabile. Per il consumatore che si avvale di agenti IA, quel nodo è ancora tutto da sciogliere. Le proposte europee, riferendosi al proprietario o all'operatore, non escludevano le persone fisiche che agiscono a titolo privato, ma riguardavano robot di specifiche categorie o sistemi ad alto rischio, assai lontani dagli agenti IA di uso quotidiano, e nella versione più compiuta accompagnavano l'obbligo a un regime di responsabilità già definito.

4. IL PROBLEMA DELL'INTERESSE ALL'ASSICURAZIONE

8. Sul punto si v. Center for Security and Emerging Technology, Adding Structure to AI Harm. An Introduction to CSET's AI Harm Framework, luglio 2023, disponibile su cset.georgetown.edu. Si v. inoltre OECD, Stocktaking for the development of an AI incident definition, in OECD Artificial Intelligence Papers, ottobre 2023, disponibile su oecd.org.
9. Per tali danni viene in rilievo l'art. 82 GDPR (reg. 27 aprile 2016, n. 679), che pone a carico del titolare del trattamento una responsabilità per colpa presunta (si v. Corte giust., 21 dicembre 2023, C-667/21, Krankenversicherung Nordrhein), ferma l'esenzione per le attività a carattere esclusivamente personale o domestico (art. 2, par. 2, lett. c).
10. Da ultimo, M.G. Iannicelli, Intelligenza artificiale e nuove esigenze di tutela: verso un regime di assicurazione obbligatoria, in Assicurazioni, 3/2026, passim, la quale propone di introdurre un obbligo assicurativo a carico dei deployer di sistemi ad alto rischio.
11. Cfr. Parlamento europeo, Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, 16 febbraio 2017, 2015/2103(INL), pp. 57-59, disponibile su europarl.europa.eu. Si v. inoltre A. La Torre, I robot fra responsabilità e assicurazione, in Assicurazioni, 3/2019, p. 323 ss.
12. Cfr. Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, 2019, p. 61 s., disponibile su europarl.europa.eu.
13. Cfr. Parlamento europeo, Raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 20 ottobre 2020, 2020/2014(INL), art. 1, par. 4 all., disponibile su europarl.europa.eu.
14. Cfr. Commissione europea, Proposta di direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale, COM(2022) 496 final, art. 5, par. 2, e considerando 31, ritirata dalla Commissione nel 2025.

Prima ancora che sull'opportunità di un obbligo, il problema si pone sul piano dell'assicurabilità, e richiede di stabilire se, allo stato, il rischio connesso all'impiego di agenti IA sia per il consumatore assicurabile. La risposta passa per la nozione di interesse.
Nell'assicurazione della responsabilità civile, l'interesse richiesto dall'art. 1904 c.c. coincide con l'interesse dell'assicurato a preservare il proprio patrimonio dall'obbligazione risarcitoria che possa sorgere a suo carico[15]. Esso sussiste, dunque, soltanto in capo a chi possa essere chiamato a rispondere del danno, e un'assicurazione della responsabilità del consumatore per i pregiudizi cagionati dall'agente avrebbe senso solo se tale responsabilità fosse configurabile. L'interesse, d'altra parte, va apprezzato al momento della conclusione del contratto, quando il sinistro è ancora futuro e incerto. Non occorre che la responsabilità dell'assicurato sia certa, ma è sufficiente che sia astrattamente configurabile, che esista cioè almeno un'ipotesi plausibile nella quale egli possa essere tenuto a risarcire un terzo.
Ciò che rileva, inoltre, è la responsabilità verso il danneggiato, non l'allocazione definitiva del costo del danno. Chi risponde verso il terzo ha interesse ad assicurarsi anche quando possa poi rivalersi su altri, perché resta esposto all'azione del danneggiato e al rischio di non recuperare quanto pagato, mentre l'assicuratore che lo abbia tenuto indenne subentra nei suoi diritti verso i terzi responsabili (art. 1916 c.c.). Il diritto positivo ne offre un esempio eloquente nell'art. 2054, comma 4, c.c., che rende il proprietario e il conducente responsabili anche dei danni derivanti da vizi di costruzione del veicolo, ferma la responsabilità solidale del produttore.
La domanda sull'assicurabilità del rischio si traduce così in una domanda sulla responsabilità, perché il consumatore ha interesse ad assicurarsi nella misura in cui l'ordinamento lo chiami a rispondere dei danni cagionati dall'agente che impiega.
Per verificare se e quando il consumatore possa essere chiamato a rispondere dei danni cagionati dall'agente, conviene muovere da un caso concreto. Si immagini che un consumatore, insoddisfatto di un acquisto online, incarichi l'agente di ottenere il rimborso dal venditore, una società che gestisce un negozio elettronico, e scopra in seguito che su un sito di recensioni è comparso, a suo nome, un giudizio che attribuisce al venditore pratiche scorrette mai avvenute, con un conseguente calo delle vendite.
La pubblicazione può dipendere da un difetto del sistema, come quando lo strumento di pubblicazione, per un errore di programmazione, rende pubblica una bozza dai contenuti inesatti che l'utente aveva scartato. Può discendere da un'istruzione dell'utente, imprudente se egli ha chiesto all'agente di denunciare pubblicamente una truffa che crede, a torto, di aver subito, soltanto vaga se si è limitato a chiedere di fare «tutto il necessario» per ottenere il rimborso, rimettendo all'agente la scelta dei mezzi. Può essere stata provocata da un terzo, che abbia inserito istruzioni occulte in una pagina consultata dall'agente nello svolgimento del compito. Oppure può essere il frutto di un'iniziativa del sistema che, senza alcun difetto, istruzione in tal senso o interferenza esterna, eccede il compito ricevuto, come quando l'agente, incaricato soltanto di inoltrare la richiesta di rimborso, decide di pubblicare la recensione per esercitare pressione sul venditore.
Nella realtà queste ipotesi possono intrecciarsi, e l'istruzione vaga segna già di per sé una zona di confine tra la condotta negligente dell'utente e l'autonomia del sistema. Distinguerle consente tuttavia di misurare su ciascuna i criteri di imputazione astrattamente applicabili, che conviene ora esaminare partitamente.

5. I CRITERI DI IMPUTAZIONE DELLA RESPONSABILITÀ

Per ricostruire la posizione del consumatore si prospettano due opzioni interpretative. Si può ritenere che egli risponda soltanto per colpa, e dunque per la propria condotta, oppure che gli siano imputate, in base a un criterio che prescinde dalla colpa, anche le conseguenze del funzionamento del sistema. Sullo sfondo resta la responsabilità del produttore, che non si sostituisce a quella del consumatore ma incide, come si vedrà, sull'allocazione definitiva del costo del danno.
La prima opzione interpretativa si fonda sull'art. 2043 c.c., espressione del principio generale del *neminem laedere*, che ricollega l'obbligo risarcitorio al fatto doloso o colposo del danneggiante. Nel caso del consumatore che impiega agenti IA, il profilo rilevante è quello della colpa perché il dolo, che fa dell'agente un mero strumento della sua volontà, non pone problemi peculiari di imputazione e resta comunque escluso dalla copertura assicurativa (art. 1917, comma 1, c.c.). Non gravando sul consumatore alcun obbligo di sorveglianza del sistema, la diligenza da lui esigibile va misurata sui soli criteri generali, e la colpa sarà ravvisabile quando il danno fosse prevedibile ed evitabile con l'ordinaria prudenza. L'accertamento della colpa è relativamente agevole quando l'istruzione impartita risulta imprudente, come quella di denunciare pubblicamente una truffa che il consumatore crede, a torto, di aver subito. Più incerta è l'ipotesi

15. Sull'interesse all'assicurazione si v., A. Donati, Trattato del diritto delle assicurazioni private, II, Il diritto del contratto di assicurazione. I principi generali del contratto di assicurazione, II, Milano, 1954, p. 187 ss.; M. Rossetti, Il diritto delle assicurazioni, I, Padova, 2011, p. 703 ss.; più di recente, M. Mazzola, L'interesse nel contratto di assicurazione. Teoria e problemi del tipo, Napoli, 2025.

dell'istruzione vaga. Rimettere all'agente una scelta è proprio ciò che giustifica il ricorso a un agente, e pretendere dall'utente istruzioni analitiche finirebbe per annullare i vantaggi della delega[16]. La colpa potrà semmai individuarsi in scelte organizzative più a monte, come l'aver concesso all'agente accessi più ampi di quanto il compito richiedesse o l'aver rinunciato a ogni conferma prima di operazioni irreversibili. Nelle altre ipotesi, invece, la colpa difficilmente sarà configurabile. Il consumatore non può conoscere né controllare il funzionamento interno del sistema, sicché il difetto, l'interferenza del terzo e l'iniziativa autonoma dell'agente sfuggono, di regola, alla sua sfera di prevedibilità.
Si è sostenuto che chi sceglie un sistema basato su tecniche di apprendimento automatico, capace di compiere atti non previsti né conosciuti, accetti consapevolmente il rischio che ne deriva, sicché la sua colpa, consistente nella scelta stessa del sistema, dovrebbe ritenersi presunta[17]. Per il consumatore, tuttavia, quell'alternativa non esiste, perché gli agenti oggi disponibili sono tutti basati su modelli di apprendimento automatico, e se la sola scelta di servirsene bastasse a fondare la colpa, la responsabilità per colpa si trasformerebbe in una responsabilità sostanzialmente oggettiva.
Sul terreno della colpa, dunque, l'interesse del consumatore ad assicurarsi esiste, ma resta circoscritto alle ipotesi in cui il danno discenda da una sua condotta imprudente. Occorre allora verificare se l'ordinamento offre un criterio di imputazione che attribuisce al consumatore anche le conseguenze del funzionamento del sistema, prescindendo dalla colpa. Un criterio siffatto, ove applicabile, non si affiancherebbe alla colpa soltanto per le ipotesi da questa lasciate scoperte, ma regolerebbe la posizione del consumatore in tutte le ipotesi considerate, rendendo superflua, anche quando egli sia stato imprudente, la prova della sua colpa.
Tra i criteri di imputazione diversi dalla colpa, alcuni possono essere esclusi con relativa sicurezza. La responsabilità per il fatto degli ausiliari (art. 2049 c.c.) presuppone il fatto illecito di un domestico o di un commesso, e dunque la condotta di un soggetto cui l'illecito possa essere imputato. L'opinione prevalente la ritiene perciò inapplicabile ai sistemi di IA, privi di soggettività[18]. La tesi contraria, che ne ammette l'applicazione analogica, è stata formulata con riguardo ai robot antropomorfi inseriti nell'attività d'impresa[19], e difficilmente si estende a un agente *software* privo di corpo fisico e impiegato per scopi personali. Neppure la responsabilità per l'esercizio di attività pericolose (art. 2050 c.c.) sembra attagliarsi al caso. La norma presuppone che la pericolosità sia propria dell'attività, e l'impiego di un sistema di IA non basta di per sé a renderla tale[20]; chi ne ammette l'applicazione, del resto, la fonda sul rischio d'impresa[21]. Gestire la corrispondenza, aggiornare un sito o effettuare acquisti non sono attività pericolose, né lo diventano per il fatto di essere affidate a un agente.
La seconda opzione fa leva sulla responsabilità per i danni cagionati da cosa in custodia (art. 2051 c.c.), che pone a carico di chi ha una cosa in custodia i danni da essa cagionati, salvo provi il caso fortuito. La responsabilità del custode non si fonda sulla violazione di un dovere di vigilanza, ma sul mero rapporto di fatto con la cosa, e il fortuito va inteso in senso oggettivo, come fattore estraneo alla sfera del custode, imprevedibile e inevitabile, idoneo a interrompere il nesso causale[22]. Applicata ai sistemi di IA, la norma coglie proprio i danni che derivano dal loro funzionamento autonomo. In tali casi, si è osservato, il danno è cagionato non con la cosa ma dalla cosa, perché deriva dal dinamismo che le è proprio e non da una condotta umana di cui essa sia lo strumento[23]. Né vale obiettare che la norma sarebbe pensata per cose prive di capacità decisionali, perché l'art. 2051 generalizza la regola dettata dall'art. 2052 per gli animali, la cui imprevedibilità non è certo inferiore a quella di un sistema programmato[24].
Resta tuttavia da stabilirsi chi sia il custode dell'agente IA. Custode, come si è visto, è chi esercita sulla cosa un potere di fatto, indipendentemente dalla titolarità giuridica. Si potrebbe obiettare che il consumatore non ha alcun potere sul funzionamento dell'agente, che si svolge sull'infrastruttura del fornitore e da questi è continuamente definito e aggiornato, e il gruppo di esperti riteneva in effetti più convincente imputare la responsabilità a chi fornisce in modo continuativo il supporto essenziale al funzionamento della tecnologia[25]. La responsabilità del custode, tuttavia, non presuppone la possibilità di controllare in ogni momento il funzionamento del sistema o di modificarne le condizioni di rischio e il controllo che il fornitore esercita sul funzionamento tecnico attiene piuttosto alla sua responsabilità come produttore. È il consumatore, invece, a decidere se e quando attivare l'agente, quali obiettivi assegnargli e quali

16. L'osservazione è formulata da M.S. Gal, N. Elkin-Koren, Algorithmic Consumers, in Harv. J.L. & Tech., 2/2017, p. 14 s.
17. Così E. Bocchini, La regolazione giuridica dell'intelligenza artificiale, Torino, 2024, p. 97 ss.
18. Cfr. A. Albanese, La responsabilità civile per l'uso di sistemi di intelligenza artificiale, in R. Bocchini (a cura di), Manuale di diritto privato dell'informatica, Napoli, 2023, p. 570 s.
19. Cfr. A. La Torre, op. cit., p. 333.
20. Cfr. A. Albanese, op. cit., p. 565 s.
21. Cfr. E. Bocchini, op. cit., p. 96 ss.
22. Ex multis, Cass., sez. un., 30 giugno 2022, n. 20943.
23. Cfr. A. Albanese, op. cit., p. 565 s.
24. Cfr. A. Albanese, op. cit., p. 565 s.
25. Cfr. Expert Group on Liability and New Technologies – New Technologies Formation, op. cit., p. 41 s.

accessi concedergli, e l'operatività del sistema resta subordinata a questa scelta[26]. Ed è lui a trarre vantaggio dal suo impiego, sicché è coerente con la *ratio* della norma che ne sopporti anche i rischi.
Qualificato il consumatore come custode, l'area della sua responsabilità si allarga sensibilmente. Quando il danno discende da un'istruzione imprudente, egli ne risponde senza che occorra provarne la colpa. Ma anche l'iniziativa con cui l'agente eccede il compito ricevuto non integra il caso fortuito, perché esprime proprio quel dinamismo intrinseco della cosa che la norma pone a carico del custode. Così, se l'agente incaricato di ottenere un rimborso moltiplica i solleciti fino a renderli molesti, o pubblica una recensione che attribuisce al venditore fatti non veri, ne risponde il consumatore, benché nessuno avesse chiesto all'agente di agire in quel modo. Lo stesso vale per il difetto, che è interno alla cosa e non costituisce un fattore esterno idoneo a interrompere il nesso causale. Per la circolazione di veicoli, del resto, il legislatore ha compiuto una scelta analoga, rendendo il proprietario e il conducente responsabili dei danni derivanti da vizi di costruzione del veicolo, in solido con il produttore (art. 2054, comma 4, c.c.). Più incerta è l'ipotesi dell'interferenza del terzo, che potrebbe integrare il fortuito, ma soltanto se imprevedibile e inevitabile. Ne risulta che l'interesse del consumatore ad assicurarsi si estende a quasi tutte le ipotesi considerate, con la sola eccezione, eventuale, dell'interferenza del terzo.
Resta la responsabilità del produttore, che per gli agenti coincide di regola con il fornitore del sistema. La direttiva sul risarcimento per danno da prodotti difettosi[27], da recepire entro il 9 dicembre 2026, include espressamente il *software* nella nozione di prodotto e, nella valutazione del difetto, tiene conto della capacità del prodotto di continuare ad apprendere dopo l'immissione sul mercato. L'ipotesi del difetto vi rientra senza difficoltà, e anche l'iniziativa con cui l'agente eccede il compito potrebbe esservi ricondotta, se si accoglie l'idea che sia difettoso il sistema progettato senza limiti adeguati a prevenirne evoluzioni incontrollate. La responsabilità del produttore, tuttavia, non si sostituisce a quella del consumatore. I due sono obbligati in solido verso il danneggiato (art. 2055 c.c.), e il difetto rileva nei rapporti interni, ai fini del regresso, nel quale l'assicuratore del consumatore potrà surrogarsi[28]. La responsabilità del produttore riguarda dunque l'allocazione definitiva del costo del danno, non l'esposizione del consumatore verso il terzo.
L'analisi conferma, in definitiva, che l'esistenza di un interesse assicurabile dipende dal regime di responsabilità applicabile. Per i danni da trattamento illecito di dati personali, la scelta è già compiuta dall'art. 82 GDPR, che espone il consumatore a una responsabilità per colpa presunta e fonda un interesse assicurabile in quasi tutte le ipotesi. Per gli altri pregiudizi, se ci si arrestasse alla colpa, il consumatore avrebbe interesse ad assicurarsi soltanto contro le conseguenze delle proprie istruzioni imprudenti. Qualificato invece come custode dell'agente, egli risponde in quasi tutte le ipotesi, e il suo interesse ad assicurarsi si estende di conseguenza, anche quando il costo del danno sia destinato a gravare in via definitiva sul produttore attraverso il regresso.

6. CONSIDERAZIONI CONCLUSIVE

Mentre il dibattito sull'opportunità di un obbligo assicurativo restava aperto, il legislatore italiano è intervenuto sulla responsabilità civile da IA per altra via. La legge 23 settembre 2025, n. 132 ha delegato il Governo a prevedere, nei casi di responsabilità civile, strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di IA e dei relativi obblighi individuati dall'*AI Act*. In attuazione della delega, il d.lgs. 9 settembre 2026, n. 160, in vigore dal 30 settembre 2026, ha introdotto alcuni strumenti processuali per le azioni di risarcimento del danno, contrattuale ed extracontrattuale, cagionato nell'utilizzo di un sistema di IA.
Il decreto, tuttavia, non interviene direttamente sui criteri di imputazione della responsabilità, che restano quindi affidati alla disciplina di diritto comune. Infatti, il preambolo richiama gli artt. 2050 e 2051 c.c., ma il decreto nulla dice circa il criterio concretamente applicabile. In altri termini, gli strumenti approntati dal decreto presuppongono che il responsabile sia stato già individuato.
È opportuno rilevare che il decreto introduce una presunzione, relativa, sulla sussistenza del nesso di causalità tra la violazione e il danno (art. 18). Questa, tuttavia, si applica unicamente in caso di violazione di uno o più obblighi previsti dall'*AI Act* (art. 16, comma 2). Ne deriva una tutela asimmetrica. Il danneggiato è agevolato quando agisce contro un'impresa gravata da obblighi regolatori, ma resta privo di qualsiasi agevolazione proprio nell'area in cui vi sono meno presidi di garanzia, vale a dire quella dell'uso personale degli agenti IA. D'altronde, ove si ritenesse che il criterio di imputazione della responsabilità del consumatore che impiega agenti IA è quello della colpa, la vittima

26. Cfr. A. Albanese, La prevenzione dei danni da utilizzo dell'intelligenza artificiale tra responsabilità civile e regole europee di risk management, in Europa dir. priv., 2/2025, p. 163.
27. Dir. 23 ottobre 2024, n. 2853.
28. Cfr. A. Albanese, La prevenzione dei danni da utilizzo dell'intelligenza artificiale tra responsabilità civile e regole europee di risk management, cit., p. 165 s.

si troverebbe a sopportare, di fatto, il rischio del funzionamento di un sistema che non controlla e del quale non trae alcun vantaggio.
Più rilevante, ai fini del presente lavoro, è la previsione di un'azione diretta nei confronti dell'impresa di assicurazione (art. 20). Chi intende agire può chiedere al presunto responsabile se sia assicurato, e questi deve rispondere entro trenta giorni indicando gli estremi della copertura. Il danneggiato può quindi rivolgersi direttamente all'impresa di assicurazione, nei limiti del massimale, convenendo in giudizio anche il responsabile come litisconsorte necessario. La norma non distingue tra professionisti e privati, e si applica dunque anche quando il convenuto sia un consumatore assicurato. Quando il convenuto è un consumatore, la portata pratica dell'azione diretta appare peraltro limitata. L'azione non amplia l'area della copertura, ma ne presuppone l'esistenza, e il decreto consente all'assicuratore di opporre al danneggiato le eccezioni contrattuali anteriori al sinistro (art. 20, comma 3). Sul mercato, tuttavia, non risultano ancora offerte, almeno in Italia, polizze specificamente destinate a coprire la responsabilità del consumatore per i danni cagionati dagli agenti IA. La copertura più prossima resta quella della responsabilità civile della vita privata, nota anche come «RC del capofamiglia», che tiene indenne l'assicurato dei danni involontariamente cagionati a terzi nella vita quotidiana, ma riguarda per lo più la morte, le lesioni personali e i danneggiamenti a cose o animali, lasciando perciò fuori gran parte dei pregiudizi che un agente IA può arrecare in ambiente digitale. Per sviluppare coperture adeguate, le imprese di assicurazione dovrebbero poter stimare il rischio, e dunque sapere anzitutto in quali casi il consumatore sia chiamato a rispondere. Finché il criterio di imputazione resta incerto, quella stima è preclusa, e con essa la possibilità di costruire un'offerta assicurativa.
Si è visto che la soluzione più convincente è quella della responsabilità da cosa in custodia, con regresso verso il produttore per i danni derivanti da malfunzionamento. Ma una soluzione interpretativa, per quanto argomentata, non offre la certezza di cui il mercato assicurativo ha bisogno per valutare il rischio. Occorrerebbe allora una norma che faccia per gli agenti IA ciò che l'art. 2054 c.c. fa per i veicoli. Una norma, cioè, che imputi a chi impiega l'agente le conseguenze del suo funzionamento, consentendogli di liberarsi soltanto provando il caso fortuito o che l'agente ha operato contro la sua volontà, come il proprietario del veicolo può fare quando la circolazione sia avvenuta contro la sua volontà. E che, sul modello del quarto comma dell'art. 2054, lo renda responsabile anche dei danni derivanti da difetti del sistema, in solido con il produttore, facendo salvo il regresso nei confronti di quest'ultimo.
L'esperienza della circolazione stradale suggerisce anche l'ordine in cui procedere. La regola che oggi si legge nell'art. 2054 c.c. risale alla legge sulla circolazione degli automobili del 1912[29], mentre l'obbligo di assicurare la responsabilità civile è stato introdotto soltanto nel 1969[30]. Prima è venuta la regola di imputazione della responsabilità, poi, a distanza di decenni e quando la diffusione dei veicoli lo ha reso necessario, l'obbligo assicurativo. Per gli agenti IA impiegati dai consumatori siamo, per così dire, ancora al 1912. Ciò che serve oggi non è un obbligo, che allo stato apparirebbe sproporzionato, ma una regola che stabilisca chi risponde. Su quella regola il mercato potrà costruire coperture volontarie adeguate ai danni tipici degli agenti, e solo alla luce della sua applicazione si potrà valutare, in futuro, se il rischio di insolvenza dei danneggianti giustifichi un passo ulteriore.

29. L. 30 giugno 1912, n. 739.
30. L. 24 dicembre 1969, n. 990.

AUTORITA DI REGOLAZIONE DEI TRASPORTO

DALLA TUTELA DEL PASSEGGERO ALLA REGOLAZIONE DELLA MOBILITÀ. IL CONSUMATORE 2030 E IL RUOLO DELL'AUTORITÀ DI REGOLAZIONE DEI TRASPORTI.

(di Federico Nespega[1])

La progressiva integrazione tra infrastrutture, servizi e dati sta modificando la struttura e il funzionamento dei mercati della mobilità e, con essi, le forme di tutela dell'utente. La digitalizzazione, lo sviluppo della mobilità multimodale e l'emersione di nuovi intermediari rendono sempre meno sufficiente una protezione costruita esclusivamente attorno al singolo contratto di trasporto e alla reazione al disservizio. In questa prospettiva, il contributo analizza l'evoluzione del ruolo dell'Autorità di regolazione dei trasporti verso il 2030, mettendo in luce la progressiva integrazione tra regolazione economica, qualità dei servizi e delle infrastrutture, diritti individuali, enforcement e risoluzione delle controversie. Particolare attenzione è dedicata alla mobilità multimodale e al coordinamento tra i diversi soggetti della regolazione, alle nuove asimmetrie connesse alla digitalizzazione, ai profili di accessibilità e inclusione e alla valorizzazione dei reclami quali strumenti di conoscenza del mercato, anche attraverso il supporto dell'intelligenza artificiale. Ne emerge una concezione della tutela consumeristica che non si esaurisce nella reazione alla patologia del rapporto, ma concorre alla stessa conformazione regolatoria del mercato: nella mobilità del 2030, la protezione del consumatore comincia – sempre più – prima del viaggio.

SOMMARIO: – 1. Dal passeggero al consumatore di mobilità – 2. La tutela del consumatore nella costruzione regolatoria del mercato – 3. Nuove asimmetrie nella mobilità digitale – 4. Dal reclamo alla regolazione anticipatoria – 5. Verso il 2030: l'ART tra efficienza del mercato e inclusione della mobilità.

1. Dal passeggero al consumatore di mobilità

Ragionare sul consumatore del 2030 nel settore dei trasporti richiede, anzitutto, di interrogarsi sulla trasformazione dell'oggetto stesso della tutela. Il paradigma tradizionale è costruito attorno alla figura del passeggero: un soggetto che acquista una prestazione di trasporto da un determinato operatore, lungo una tratta definita e mediante uno specifico modo di trasporto. A questa relazione corrisponde un sistema di diritti altrettanto riconoscibile, destinato a operare soprattutto quando l'esecuzione della prestazione diviene patologica: ritardo, cancellazione, mancata assistenza, inadeguatezza delle informazioni, necessità di rimborso o indennizzo.[2]

Questo modello rimane essenziale, ma non appare più sufficiente a descrivere l'esperienza contemporanea della mobilità. Il consumatore si muove sempre più frequentemente all'interno di un ecosistema nel quale infrastrutture fisiche, servizi di trasporto, piattaforme digitali, sistemi di prenotazione e pagamento, dati e algoritmi concorrono alla costruzione di un'unica esperienza di viaggio. La distinzione tra trasporto ferroviario, automobilistico, aereo, marittimo e mobilità urbana continua naturalmente ad assumere rilevanza sul piano giuridico e regolatorio; dal punto di vista dell'utente, tuttavia, essa tende a perdere centralità rispetto all'esigenza di raggiungere una destinazione attraverso una combinazione efficiente e accessibile di servizi.

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

2. Cfr., per il quadro unionale relativo ai settori sottoposti alla vigilanza ART, Regolamento (UE) 2021/782 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo ai diritti e agli obblighi dei passeggeri nel trasporto ferroviario (rifusione), in GUUE L 172 del 17 maggio 2021; Regolamento (UE) n. 181/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, relativo ai diritti dei passeggeri nel trasporto effettuato con autobus, in GUUE L 55 del 28 febbraio 2011; Regolamento (UE) n. 1177/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo ai diritti dei passeggeri che viaggiano via mare e per vie navigabili interne, in GUUE L 334 del 17 dicembre 2010.

È il passaggio dal passeggero al consumatore di mobilità.

La prospettiva del *Mobility as a Service* (MaaS) rappresenta la manifestazione più evidente di questa evoluzione: differenti servizi di mobilità vengono integrati in un'unica piattaforma digitale, attraverso la quale l'utente può ricercare, combinare, prenotare e pagare soluzioni di viaggio differenti.[3]

Il passaggio dal trasporto unimodale alla mobilità integrata non determina, tuttavia, una corrispondente semplificazione sul piano giuridico. Al contrario, alla semplificazione tecnologica dell'esperienza dell'utente può corrispondere una crescente complessità dei rapporti sottostanti.

Il diritto europeo dei passeggeri si è infatti sviluppato prevalentemente secondo una logica modale. Ferrovia, autobus, trasporto marittimo e aereo sono disciplinati da differenti sistemi normativi, costruiti attorno al singolo contratto e alla specifica modalità di trasporto.[4]

La letteratura dedicata al MaaS ha da tempo evidenziato la difficoltà di ricondurre a tale struttura una catena di mobilità nella quale il disservizio verificatosi durante un segmento possa produrre conseguenze sul segmento successivo, eventualmente gestito da un diverso operatore.[5]

La questione non è più soltanto teorica. La proposta di regolamento della Commissione europea del 29 novembre 2023 sui diritti dei passeggeri nei viaggi multimodali muove espressamente dalla constatazione che il quadro vigente non garantisce una tutela equivalente quando il viaggio sia composto dalla combinazione di differenti modi di trasporto. La Commissione individua, tra le criticità, l'insufficienza delle informazioni, le difficoltà nell'assistenza in caso di perdita delle coincidenze e l'incertezza circa i soggetti responsabili e le autorità competenti.[6]

Il relativo procedimento legislativo è tuttora in corso. A tale iniziativa si è affiancato, più recentemente, il pacchetto legislativo presentato dalla Commissione europea il 13 maggio 2026, volto a favorire una maggiore integrazione dei sistemi di prenotazione e distribuzione dei titoli di viaggio e a rafforzare la protezione dei passeggeri nell'ambito di servizi di trasporto effettuati da una pluralità di operatori. Il pacchetto si articola in tre proposte di regolamento, rispettivamente dedicate alla prenotazione multimodale, alla bigliettazione ferroviaria e alla modifica del regolamento (UE) 2021/782 con riferimento alla tutela dei passeggeri titolari di biglietti unici.[7]

L'intervento europeo assume particolare significato nella prospettiva qui considerata, poiché affronta una delle principali contraddizioni che caratterizzano l'evoluzione dei mercati della mobilità: mentre l'innovazione tecnologica consente di rappresentare e organizzare il viaggio come una prestazione progressivamente integrata, la sua concreta realizzazione continua a dipendere da una pluralità di operatori, infrastrutture, sistemi informativi e rapporti contrattuali, non sempre adeguatamente coordinati. La frammentazione dei sistemi di prenotazione e distribuzione, le difficoltà di accesso ai dati e la limitata interoperabilità delle piattaforme possono così tradursi in ostacoli all'effettiva fruizione dei servizi, incidendo non soltanto sulla libertà di scelta del consumatore, ma anche sulla possibilità di individuare con chiarezza le condizioni contrattuali applicabili e le garanzie riconosciute nelle diverse fasi del viaggio.[8]

In questa prospettiva, il pacchetto del 2026 manifesta una tendenza della regolazione europea a intervenire sulle condizioni strutturali di funzionamento del mercato, anziché limitarsi alla disciplina dei rimedi conseguenti all'inadempimento della prestazione di trasporto. L'obiettivo di rendere più agevole la ricerca, la comparazione e l'acquisto di soluzioni di viaggio integrate presuppone, infatti, la definizione di regole comuni nei rapporti tra operatori di trasporto, intermediari digitali e fornitori dei servizi di mobilità multimodale. L'accessibilità delle informazioni, la trasparenza nella presentazione delle offerte e l'interoperabilità dei sistemi assumono, in tal modo, una rilevanza direttamente consumeristica, concorrendo a determinare le condizioni nelle quali l'utente può esercitare una scelta effettivamente consapevole.

Particolare rilievo assume, inoltre, la dimensione istituzionale dell'intervento. La proposta relativa alla prenotazione multimodale contempla un sistema di cooperazione tra gli organismi nazionali responsabili dell'applicazione della

3. Sul fenomeno, ampiamente, E. Murati, Regulating Mobility as a Service (MaaS) in European Union. A Legal Analysis of Digitalization, Competition, and Multimodality, Springer, Cham, 2023, spec. pp. 21 ss., 151 ss. e 327 ss.

4. Per il settore ferroviario, v. Regolamento (UE) 2021/782, cit.; per il trasporto mediante autobus, Regolamento (UE) n. 181/2011, cit.; per il trasporto via mare e vie navigabili interne, Regolamento (UE) n. 1177/2010, cit. Il carattere settoriale dell'attuale sistema europeo è riconosciuto dalla stessa Commissione nell'Impact Assessment relativo alla proposta sui viaggi multimodali.

5. E. Murati, "Mobility-as-a-service (MaaS) digital marketplace impact on EU passengers' rights", in European Transport Research Review, 2020, 12, 62, pp. 1-14; Id., Regulating Mobility as a Service (MaaS) in European Union, cit., pp. 327-360.

6. Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo ai diritti dei passeggeri nel contesto di viaggi multimodali, COM(2023) 752 final, 29 novembre 2023, 2023/0436(COD), spec. Relazione introduttiva. Il procedimento legislativo risulta, alla data di redazione del presente contributo, ancora in corso.

7. Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prenotazione multimodale e che abroga il regolamento (CE) n. 80/2009, COM(2026) 231 final, 13 maggio 2026; Id., Proposta di regolamento del Parlamento europeo e del Consiglio sull'emissione di biglietti ferroviari, COM(2026) 232 final, 13 maggio 2026; Id., Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2021/782 per quanto riguarda la protezione dei passeggeri con biglietti unici, COM(2026) 233 final, 13 maggio 2026.

8. Cfr. Commissione europea, Commission Staff Working Document – Executive Summary of the Impact Assessment Report, SWD(2026) 301 final, 13 maggio 2026; M. Kiss, Passenger package: Towards seamless multimodal travel and stronger passenger rights in the EU, European Parliamentary Research Service, luglio 2026.

disciplina, con il coinvolgimento della Commissione europea nelle attività di coordinamento e di scambio delle informazioni e delle migliori pratiche. Tale previsione risponde all'esigenza di evitare che l'integrazione transnazionale dei servizi e delle piattaforme digitali si accompagni a una persistente frammentazione delle attività di vigilanza e applicazione delle regole. L'effettività della disciplina europea viene così a dipendere non soltanto dall'armonizzazione degli obblighi sostanziali, ma anche dalla capacità delle istituzioni competenti di assicurarne un'applicazione coerente, affrontando criticità che, per la loro stessa natura, possono oltrepassare i confini dei singoli ordinamenti nazionali. [9]
Questa evoluzione presenta significativi punti di contatto con la prospettiva delineata da Bassan nell'introduzione al presente volume, ove il superamento della frammentazione degli interventi pubblici è ricondotto all'esigenza di un «concerto regolatorio a due versanti», fondato, da un lato, sul coordinamento verticale e orizzontale tra autorità indipendenti e, dall'altro, sulla cooperazione tra autorità e mercato, considerato nella sua dimensione infrastrutturale, pubblica e privata. [10]
Nel settore della mobilità, la complementarità delle due dimensioni emerge con particolare evidenza: mentre la cooperazione tra Commissione europea e organismi nazionali competenti concorre ad assicurare un'applicazione coerente delle regole, il coinvolgimento degli operatori e dei soggetti responsabili delle infrastrutture fisiche e digitali costituisce una condizione essenziale per tradurre gli obiettivi regolatori in sistemi effettivamente interoperabili e accessibili. La tutela del consumatore viene così a dipendere non soltanto dall'armonizzazione delle disposizioni sostanziali, ma anche dalla capacità di coordinarne l'attuazione e l'enforcement, nel rispetto della specializzazione delle competenze settoriali.
La prospettiva del viaggio integrato, idealmente organizzabile dalla propria abitazione sino alla destinazione finale, non rappresenta dunque soltanto un obiettivo di innovazione dei servizi di mobilità. Essa esprime un'esigenza più ampia di integrazione delle condizioni di accesso al mercato, delle garanzie individuali e dei meccanismi istituzionali preposti alla loro applicazione. Il passaggio dal passeggero al consumatore di mobilità richiede – sostanzialmente – che alla progressiva unificazione dell'esperienza di viaggio corrisponda una maggiore capacità dell'ordinamento di governare la pluralità dei rapporti economici e giuridici che la rendono possibile.
Dati, servizi e infrastrutture non costituiscono più dimensioni separabili. È nella loro interazione che si forma la posizione del consumatore della mobilità.

1. La tutela del consumatore nella costruzione regolatoria del mercato

La trasformazione *de qua* consente di leggere sotto una luce diversa il ruolo dell'Autorità di regolazione dei trasporti. L'A.R.T. non nasce come autorità generalista di tutela del consumatore. L'art. 37 del decreto-legge 6 dicembre 2011, n. 201 le attribuisce funzioni di regolazione economica dei trasporti e dell'accesso alle relative infrastrutture, con l'obiettivo, tra l'altro, di garantire condizioni di accesso eque e non discriminatorie, metodologie tariffarie orientate all'efficienza, livelli adeguati di qualità dei servizi e condizioni minime di tutela degli utenti.[11] A tali attribuzioni si affiancano le competenze esercitate quale organismo nazionale responsabile dell'applicazione della disciplina europea sui diritti dei passeggeri nel trasporto ferroviario, con autobus e per mare e vie navigabili interne.[12]
È proprio la compresenza di queste funzioni a rendere l'ART un osservatorio particolarmente significativo dell'evoluzione della tutela consumeristica.
Nel mercato della mobilità, infatti, proteggere il consumatore non significa soltanto riconoscergli un diritto quando il rapporto con l'operatore è già entrato nella sua fase patologica. Una parte della tutela si realizza **prima ancora che il singolo rapporto di consumo abbia inizio**, attraverso la conformazione regolatoria del mercato.
La disciplina dell'accesso alle infrastrutture, i criteri per la determinazione dei canoni, l'individuazione di condizioni minime di qualità, la regolazione delle procedure di affidamento dei servizi pubblici e la costruzione di meccanismi incentivanti collegati alla qualità incidono sulle condizioni nelle quali il consumatore potrà successivamente esercitare la propria libertà di scelta e fruire del servizio.
Il trasporto pubblico costituisce, sotto questo profilo, un banco di prova particolarmente significativo. Nel giugno 2026 l'ART ha avviato, ai sensi dell'art. 37, comma 2, lett. a) e f), del d.l. n. 201/2011, un procedimento per la predi-

9. Cfr. Commissione europea, COM(2026) 231 final, cit., con particolare riferimento alle disposizioni concernenti la cooperazione tra organismi nazionali responsabili dell'applicazione del regolamento e al ruolo di coordinamento e supporto della Commissione europea.
10. F. Bassan, Il consumatore ibrido 2030, introduzione al presente volume, spec. § 1-12, ove il «concerto regolatorio a due versanti» è individuato nel coordinamento, verticale e orizzontale, tra autorità indipendenti e nella cooperazione tra autorità e mercato-infrastruttura, quali strumenti di integrazione della formazione delle norme, della loro esecuzione e dell'enforcement.
11. Art. 37, d.l. 6 dicembre 2011, n. 201, conv., con modif., dalla l. 22 dicembre 2011, n. 214, e successive modificazioni, recante la disciplina istitutiva e le competenze dell'Autorità di regolazione dei trasporti.
12. Cfr. Regolamento (UE) 2021/782; Regolamento (UE) n. 181/2011; Regolamento (UE) n. 1177/2010, cit., nonché la relativa disciplina nazionale di attuazione e sanzionatoria.

sposizione di nuove linee guida relative all'affidamento dei servizi di trasporto pubblico ferroviario e su strada.[13]
Il dato interessa la prospettiva consumeristica perché mostra come qualità ed efficienza del servizio possano essere incorporate già nella fase che precede la sua concreta erogazione all'utente. Occorre tuttavia considerare che tra l'intervento regolatorio dell'Autorità e l'effettiva fruizione del servizio si colloca l'attività delle amministrazioni e degli enti competenti all'organizzazione e all'affidamento dei servizi di trasporto pubblico. A questi ultimi spetta tradurre il quadro regolatorio, nell'ambito delle rispettive attribuzioni, in scelte concrete relative alla programmazione dei servizi, alla predisposizione delle procedure di affidamento, alla definizione degli obblighi di servizio pubblico e all'individuazione degli standard qualitativi da assicurare agli utenti.[14]
La fase di progettazione dell'affidamento assume, pertanto, una rilevanza direttamente consumeristica. La determinazione delle caratteristiche del servizio, dei livelli di accessibilità, degli obblighi informativi, degli indicatori di qualità e dei meccanismi di monitoraggio dell'esecuzione contrattuale concorre infatti a definire le condizioni nelle quali il consumatore potrà esercitare i propri diritti. In questa prospettiva, la qualità della regolazione non può essere valutata esclusivamente con riferimento all'adeguatezza delle prescrizioni adottate dall'Autorità, ma deve essere considerata anche in relazione alla loro effettiva traduzione negli atti di affidamento e nei successivi rapporti contrattuali.
Ne discende l'esigenza di valorizzare la capacità amministrativa e tecnica degli enti affidanti, la cui attività richiede competenze specialistiche, disponibilità di informazioni attendibili e risorse adeguate per la progettazione delle procedure, la definizione dei fabbisogni di mobilità e il controllo della qualità dei servizi. L'investimento nella capacità progettuale delle amministrazioni rappresenta, sotto questo profilo, una condizione per l'effettività della regolazione e, indirettamente, della tutela del consumatore. In assenza di adeguate risorse e competenze, anche un quadro regolatorio coerente rischia infatti di non tradursi in prestazioni rispondenti alle esigenze degli utenti, con il risultato di mantenere una distanza tra gli obiettivi della regolazione e la qualità concretamente sperimentata nell'utilizzo del servizio.[15]
La tutela del consumatore nei trasporti comincia, dunque, prima del viaggio e si sviluppa attraverso una sequenza di interventi che, dalla definizione delle regole alla progettazione e all'affidamento del servizio, giunge sino alla verifica della qualità effettivamente erogata. L'efficacia di tale sequenza dipende dalla capacità dei diversi soggetti coinvolti di tradurre gli obiettivi regolatori in condizioni concrete di accessibilità, affidabilità e qualità delle prestazioni.
Il fenomeno è ancora più evidente se si considera l'infrastruttura.
Nel settore ferroviario, con la delibera n. 116/2025, l'ART ha approvato meccanismi di premi e penalità sui livelli tariffari correlati alla qualità del servizio erogato dal gestore dell'infrastruttura ferroviaria nazionale.[16]
Nell'ottobre 2026 ha inoltre avviato il procedimento volto all'individuazione di indicatori di performance e criteri di qualità da inserire negli schemi dei contratti di programma tra il gestore dell'infrastruttura ferroviaria nazionale e il Ministero delle infrastrutture e dei trasporti.[17]
Ancora più immediato è il caso autostradale. Con la delibera n. 211/2025 l'Autorità ha concluso il procedimento concernente il contenuto minimo degli specifici diritti, anche di natura risarcitoria, esigibili dagli utenti nei confronti dei concessionari autostradali e dei gestori dei servizi erogati nelle pertinenze, disciplinando altresì il rimborso del pedaggio in presenza di limitazioni all'utilizzo dell'infrastruttura.[18]
Il passaggio è significativo.
L'infrastruttura cessa di essere soltanto un fattore produttivo o un oggetto della regolazione economica e diviene elemento capace di incidere direttamente sulla posizione giuridica dell'utente.
La tradizionale distinzione tra regolazione del mercato e tutela del consumatore tende, sotto questo profilo, ad attenuarsi. La *consumer protection* non opera soltanto come limite esterno al funzionamento del mercato, destinato ad attivarsi quando il rapporto tra professionista e consumatore diviene patologico; penetra, almeno in parte, nella stessa costruzione regolatoria del mercato.

13. ART, delibera 26 giugno 2026, n. 101, Avvio del procedimento per la predisposizione, ai sensi dell'art. 37, comma 2, lett. a) e f) del d.l. 201/2011, di Linee guida nel settore dei servizi di trasporto pubblico, in attuazione dell'art. 1, comma 6, della legge n. 190/2025.
14. Cfr. art. 37, comma 2, lett. a) e f), d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214; regolamento (CE) n. 1370/2007 del Parlamento europeo e del Consiglio, del 23 ottobre 2007, relativo ai servizi pubblici di trasporto di passeggeri su strada e per ferrovia; d.lgs. 23 dicembre 2022, n. 201, recante «Riordino della disciplina dei servizi pubblici locali di rilevanza economica».
15. Sul rapporto tra regolazione, infrastrutture e cooperazione tra autorità e mercato, v. F. Bassan, Il consumatore ibrido 2030, introduzione al presente volume, spec. § 12, ove il «concerto regolatorio a due versanti» è ricondotto anche alla necessità di assicurare coerenza tra formazione delle norme, loro esecuzione ed enforcement, valorizzando il circolo regolatorio e la regolazione partecipata.
16. ART, delibera 24 luglio 2025, n. 116, Approvazione delle misure per la definizione dei meccanismi di premi/penalità sui livelli tariffari correlati alla qualità del servizio erogato dal gestore dell'infrastruttura ferroviaria nazionale.
17. ART, delibera 1° ottobre 2026, n. 182, Individuazione degli indicatori di performance e dei criteri di qualità da inserire negli schemi di contratti di programma tra il gestore della infrastruttura ferroviaria nazionale e il Ministero delle infrastrutture e dei trasporti ai sensi dell'articolo 15, comma 5-bis, del d.lgs. 112/2015. Avvio del procedimento.
18. ART, delibera 2 dicembre 2025, n. 211, Misure concernenti il contenuto minimo degli specifici diritti, anche di natura risarcitoria, che gli utenti possono esigere nei confronti dei concessionari autostradali e dei gestori dei servizi erogati nelle pertinenze di servizio delle reti autostradali. Misure afferenti al rimborso del pedaggio in presenza di limitazioni all'utilizzo dell'infrastruttura.

Non si tratta, dunque, di descrivere un passaggio dell'ART da una regolazione *ex post* a una regolazione *ex ante*: l'Autorità dispone sin dall'origine di rilevanti strumenti regolatori preventivi. Il fenomeno più interessante consiste piuttosto nella **progressiva integrazione tra regolazione economica ex ante, tutela individuale, enforcement e strumenti di risoluzione delle controversie**, che concorrono, con tecniche differenti, alla protezione dell'utente.

2. Nuove asimmetrie nella mobilità digitale

L'integrazione tra infrastrutture, servizi e dati non elimina le tradizionali asimmetrie che caratterizzano il rapporto tra professionista e consumatore. Può, al contrario, generarne di nuove.

Nel mercato della mobilità digitale, la capacità dell'utente di conoscere e confrontare l'offerta dipende sempre più dal funzionamento di sistemi informativi e piattaforme che selezionano, ordinano e presentano le alternative disponibili. Il prezzo può assumere carattere dinamico; la visibilità delle offerte può dipendere dalle modalità attraverso le quali esse vengono ordinate; la possibilità stessa di combinare servizi diversi può essere condizionata dall'accesso ai dati e dall'interoperabilità tra sistemi.

Il MaaS porta quindi nel settore dei trasporti problematiche già emerse nei mercati digitali: accesso ai dati, ruolo dell'intermediario, trasparenza dell'interfaccia, possibilità di comparazione, trattamento differenziato degli operatori, allocazione della responsabilità.[19]

Non ogni forma di differenziazione tariffaria o di personalizzazione costituisce, naturalmente, una discriminazione. Né tali dinamiche possono essere indistintamente ricondotte al perimetro delle competenze dell'ART. Esse descrivono, tuttavia, il contesto nel quale la regolazione della mobilità sarà chiamata a operare e rendono necessario un crescente coordinamento tra disciplina dei trasporti, concorrenza, tutela dei consumatori, regolazione dei servizi digitali e protezione dei dati.

La tecnologia presenta – sotto questo profilo – una evidente ambivalenza: può ridurre le asimmetrie informative, facilitando comparazione, accesso e integrazione dei servizi, ma può al contempo trasferire l'asimmetria all'interno dell'architettura digitale attraverso la quale il consumatore accede al mercato.

La medesima ambivalenza emerge rispetto alla transizione ecologica.

La costruzione di un sistema di mobilità multimodale più efficiente costituisce una componente fondamentale della strategia europea di decarbonizzazione dei trasporti. La stessa proposta europea sui diritti dei passeggeri nei viaggi multimodali collega espressamente un'adeguata protezione del passeggero all'attrattività delle forme di trasporto collettivo e sostenibile.[20]

La transizione presenta tuttavia anche una dimensione distributiva. Digitalizzazione dei servizi, razionalizzazione delle reti, trasformazione delle strutture tariffarie e investimenti nelle infrastrutture possono produrre effetti differenti a seconda del territorio, dell'età, delle condizioni economiche e delle competenze digitali dell'utente. Una mobilità complessivamente più efficiente potrebbe, pertanto, risultare meno accessibile per chi vive nelle aree interne, per chi dispone di minori risorse economiche o per chi incontra difficoltà nell'utilizzo esclusivo di strumenti digitali.

Il tema assume particolare rilevanza con riferimento alle persone con disabilità o a mobilità ridotta, per le quali l'accessibilità non può essere valutata esclusivamente in termini di disponibilità formale del servizio, ma deve essere considerata rispetto alla sua concreta fruibilità. L'esistenza di un collegamento, infatti, non garantisce di per sé la possibilità di utilizzarlo, qualora permangano ostacoli nell'accesso alle infrastrutture, nella disponibilità dell'assistenza, nella fruizione delle informazioni o nell'utilizzo dei sistemi digitali di prenotazione e acquisto dei titoli di viaggio.[21]

La questione acquista ulteriore complessità nella mobilità multimodale, nella quale l'inaccessibilità di un singolo segmento, fisico o digitale, può compromettere la possibilità di completare l'intero itinerario. L'effettività della tutela richiede, invero, di considerare l'accessibilità quale componente strutturale della qualità del servizio, da integrare nelle scelte di organizzazione, affidamento e regolazione della mobilità, e non soltanto quale oggetto di misure correttive successive al verificarsi di un disservizio.[22]

---

19. Per una ricostruzione sistematica delle problematiche relative a data sharing, concorrenza e multimodalità nel MaaS, E. Murati, Regulating Mobility as a Service (MaaS) in European Union, cit., rispettivamente pp. 45-201, 203-323 e 325-360.
20. Commissione europea, COM(2023) 752 final, cit., Relazione, par. 1, ove la protezione del passeggero durante le perturbazioni del viaggio viene espressamente collegata alla maggiore attrattività della mobilità multimodale e collettiva.
21. Cfr. regolamento (UE) 2021/782 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo ai diritti e agli obblighi dei passeggeri nel trasporto ferroviario, spec. artt. 21-26; regolamento (UE) n. 181/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, relativo ai diritti dei passeggeri nel trasporto effettuato con autobus, spec. artt. 9-17; regolamento (UE) n. 1177/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo ai diritti dei passeggeri che viaggiano via mare e per vie navigabili interne, spec. artt. 7-15; regolamento (CE) n. 1107/2006 del Parlamento europeo e del Consiglio, del 5 luglio 2006, relativo ai diritti delle persone con disabilità e delle persone a mobilità ridotta nel trasporto aereo.
22. Cfr. direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi, spec. art. 2, par. 2, lett. c), relativo a determinati elementi dei servizi di trasporto passeggeri, nonché lett. f), relativa ai servizi di commercio elettronico; d.lgs. 27 maggio 2022, n. 82, recante «Attuazione della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi».

La prospettiva dell'accessibilità effettiva si collega, più in generale, all'esigenza di superare una rappresentazione uniforme del destinatario della regolazione. Il consumatore 2030 non può essere assunto come una figura astratta, tecnologicamente competente e omogeneamente collocata sul territorio, poiché le condizioni individuali e sociali incidono concretamente sulla possibilità di beneficiare dell'innovazione. L'efficienza della mobilità deve essere misurata, pertanto, anche rispetto alla sua capacità di garantire condizioni di accesso effettive, evitando che la crescente integrazione dei servizi si traduca nella formazione di nuove disuguaglianze.
La considerazione delle differenti condizioni di accesso ai servizi trova un ulteriore terreno di sviluppo nell'analisi degli effetti distributivi e intergenerazionali delle decisioni regolatorie. Così, in questa direzione, nel 2026 l'ART abbia avviato un percorso volto a integrare la **Valutazione di impatto generazionale (VIG)** nei propri strumenti di analisi e verifica dell'impatto della regolazione. La Relazione annuale 2026 dedica proprio a questo tema la propria parte prospettica, ponendolo in continuità con le precedenti riflessioni sulle nuove forme di mobilità e sull'intelligenza artificiale.[23]
L'introduzione della dimensione generazionale nell'AIR/VIR può essere letta come manifestazione di un'esigenza più ampia: misurare non soltanto gli effetti immediati della decisione regolatoria, ma anche quelli destinati a prodursi nel medio-lungo periodo.
Pertanto, regolazione anticipatoria non significa prevedere il futuro, ma incorporare nel processo decisionale gli effetti che le scelte compiute oggi possono produrre sull'accessibilità, sull'inclusione e sulla sostenibilità della mobilità di domani.

3. Dal reclamo alla regolazione anticipatoria

Il passaggio ad una tutela maggiormente preventiva emerge con particolare chiarezza se si considera il ruolo assunto dai reclami degli utenti nell'attività delle autorità di regolazione. Tradizionalmente, il reclamo costituisce anzitutto uno strumento di reazione individuale al disservizio, attraverso il quale il passeggero contesta l'inadempimento degli obblighi gravanti sull'operatore e richiede il riconoscimento delle garanzie previste dalla disciplina applicabile. Questa funzione rimane centrale nel sistema europeo dei diritti dei passeggeri, che attribuisce specifica rilevanza alle procedure di gestione dei reclami e all'intervento degli organismi nazionali responsabili dell'applicazione della normativa.
Occorre, tuttavia, distinguere il reclamo rivolto all'operatore, la segnalazione o il reclamo presentato all'autorità competente e gli strumenti di risoluzione non giurisdizionale delle controversie. Si tratta di istituti che, pur concorrendo alla tutela dell'utente, rispondono a finalità differenti: la gestione del reclamo da parte dell'operatore è diretta a ottenere una risposta alla contestazione individuale; l'intervento dell'autorità si inserisce nell'esercizio delle competenze pubblicistiche di vigilanza e, ove ne ricorrano i presupposti, sanzionatorie; la conciliazione mira invece alla composizione della controversia tra utente e operatore. Nell'esperienza dell'Autorità cui ci si riferisce, siffatte diverse dimensioni concorrono a delineare un sistema articolato di tutela, nel quale alle funzioni di vigilanza sull'applicazione della disciplina europea dei diritti dei passeggeri si affiancano strumenti di risoluzione alternativa delle controversie.
Un ruolo significativo è svolto, in particolare, dal Servizio conciliazioni ART, operativo attraverso la piattaforma ConciliaWeb, che consente agli utenti di accedere a una procedura telematica di risoluzione delle controversie nei settori e alle condizioni previsti dalla disciplina applicabile. Secondo i dati precedentemente diffusi dall'Autorità, al 30 giugno 2025 risultavano gestite 45.317 istanze, con circa sei milioni di euro di rimborsi riconosciuti agli utenti e una netta prevalenza delle controversie relative al trasporto aereo, pari a oltre il 97 per cento delle istanze considerate. Il ricorso allo strumento ha conosciuto un ulteriore incremento; tantoché al 30 settembre 2026 le istanze presentate attraverso il sistema avevano superato quota 60.000. Al di là della crescita quantitativa, che comunque assume la sua rilevanza, il dato testimonia la rilevanza assunta dagli strumenti di risoluzione alternativa delle controversie nella tutela dei passeggeri e conferma l'importanza di assicurare modalità di accesso semplici e concretamente fruibili, affinché la digitalizzazione della tutela non si traduca essa stessa in una nuova barriera per gli utenti.
Accanto alla funzione di tutela individuale, i reclami possono assumere una rilevanza conoscitiva per l'attività del regolatore. Le informazioni acquisite nell'esercizio delle funzioni istituzionali di esame dei reclami e di vigilanza, considerate in forma aggregata, possono infatti evidenziare la reiterazione di determinati disservizi, la loro concentrazione in specifici ambiti territoriali o temporali, la persistenza di carenze informative e l'emersione di problematiche comuni a una pluralità di operatori. Il reclamo assume così una dimensione ulteriore rispetto alla singola vicenda individuale, concorrendo alla conoscenza delle condizioni effettive di funzionamento del mercato e alla valutazione dell'effettività delle regole poste a presidio dei servizi.

23. ART, Relazione annuale 2026 al Parlamento, Torino, 22 settembre 2026, Parte I; v. altresì ART, delibera 17 settembre 2026, n. 181, Valutazione di impatto generazionale e regolazione dei settori di competenza dell'Autorità. Avvio di una call for input propedeutica alla revisione del regolamento AIR/VIR approvato con delibera n. 54/2021.

Questa funzione conoscitiva non costituisce una novità introdotta dall'impiego dell'intelligenza artificiale, ma rappresenta una potenzialità già insita nell'attività istituzionale di acquisizione e valutazione dei reclami. L'innovazione tecnologica può piuttosto rafforzarne le capacità operative, rendendo più agevole l'elaborazione di grandi quantità di informazioni e l'individuazione di ricorrenze difficilmente rilevabili attraverso modalità esclusivamente manuali.
In tale contesto si colloca la call esplorativa avviata dell'Autorità già nel corso del 2026 per la realizzazione di un *Proof of Concept* finalizzato alla sperimentazione di soluzioni tecnologiche basate sull'intelligenza artificiale per la verifica della coerenza dei reclami dei passeggeri. L'iniziativa riguarda, in particolare, la fase preliminare di verifica documentale e classificazione dei reclami acquisiti attraverso il Sistema Telematico di acquisizione reclami (SiTe). [24] La sperimentazione così si inserisce nell'ambito di una funzione già appartenente all'attività istituzionale dell'Autorità, tantoché l'elemento innovativo non risiede nell'attribuzione di nuove competenze, ma nella possibilità di utilizzare strumenti tecnologici a supporto delle operazioni preliminari di analisi e organizzazione delle informazioni.
Occorre, peraltro, distinguere le finalità direttamente riconducibili alla sperimentazione dalle ulteriori prospettive che potrebbero derivare dall'evoluzione degli strumenti di analisi. La verifica preliminare della coerenza dei reclami non equivale all'automatizzazione della loro valutazione giuridica, né implica necessariamente l'impiego di sistemi predittivi nell'attività regolatoria. La possibilità di valorizzare le informazioni acquisite per individuare criticità ricorrenti e orientare successive valutazioni dell'Autorità rappresenta, piuttosto, una prospettiva di sviluppo che richiede adeguati presupposti organizzativi, metodologici e giuridici. La qualità e la rappresentatività dei dati, la verificabilità dei risultati, la trasparenza delle metodologie impiegate e la supervisione umana costituiscono, in questo senso, condizioni essenziali affinché l'utilizzo degli strumenti algoritmici rafforzi, anziché indebolire, l'effettività della tutela.
Il passaggio concettuale rimane tuttavia rilevante; le informazioni acquisite nell'esercizio delle funzioni di vigilanza e tutela possono contribuire anche alla valutazione dell'efficacia delle regole esistenti e all'individuazione di eventuali esigenze di intervento. Si delinea così un possibile circuito di retroazione tra regolazione, comportamento degli operatori, esperienza degli utenti, acquisizione delle informazioni e successiva valutazione regolatoria. Tale dinamica presenta significativi punti di contatto con la prospettiva del *circolo regolatorio* richiamata da Bassan nell'introduzione al presente volume, nella quale il rapporto tra autorità e mercato non si esaurisce nell'applicazione unidirezionale delle prescrizioni, ma assume una dimensione progressivamente partecipativa e conoscitiva. [25]
Nel settore dei trasporti, la valorizzazione delle informazioni provenienti dai reclami può rappresentare un ulteriore elemento di questo processo, contribuendo a ridurre la distanza tra la qualità del servizio prevista dalla regolazione e quella effettivamente sperimentata dagli utenti.
È in tale prospettiva che può essere individuata una delle evoluzioni più interessanti della funzione delle autorità indipendenti verso il 2030, corrispondente non tanto al superamento della distinzione tra regolazione ed enforcement, ma piuttosto al rafforzamento della loro complementarità attraverso una più sistematica conoscenza degli effetti prodotti dalle regole sul funzionamento del mercato.

4. Verso il 2030: l'ART tra efficienza del mercato e inclusione della mobilità

Il consumatore del 2030 sarà sempre meno soltanto il passeggero di un singolo vettore e sempre più l'utente di un ecosistema complesso di mobilità, nel quale infrastrutture fisiche e digitali, operatori economici, piattaforme tecnologiche e sistemi informativi concorrono alla realizzazione di un'esperienza di viaggio progressivamente integrata. La sua tutela non potrà, pertanto, essere confinata alla relazione bilaterale con il vettore né al momento patologico del disservizio, ma dovrà estendersi alle condizioni strutturali che rendono possibile l'accesso e la fruizione dei servizi.
È in questa trasformazione che il ruolo dell'Autorità di regolazione dei trasporti assume particolare interesse. La varietà degli strumenti attraverso i quali l'Autorità interviene sull'organizzazione e sul funzionamento dei mercati dei trasporti mostra come la tutela del consumatore possa essere perseguita non soltanto mediante il riconoscimento di diritti individuali e la predisposizione di rimedi successivi al disservizio, ma anche attraverso la definizione preventiva delle condizioni di accesso, qualità ed efficienza dei servizi. Non si tratta di trasformare l'ART in un'autorità generalista dei consumatori né di sovrapporne le competenze a quelle attribuite ad altre autorità indipendenti. Si tratta, piuttosto, di riconoscere che, nei mercati regolati contemporanei, la distinzione tra regolazione economica e tutela del consumatore, pur conservando il proprio rilievo sul piano delle attribuzioni istituzionali, tende ad attenuarsi sul piano degli effetti prodotti dalle decisioni regolatorie. La qualità della tutela dipende anche dalla qualità della costruzione del mercato.

24. Autorità di regolazione dei trasporti, Call esplorativa per la realizzazione di un Proof of Concept relativo all'impiego di soluzioni di intelligenza artificiale per la verifica della coerenza dei reclami dei passeggeri, aprile 2026.
25. F. Bassan, Il consumatore ibrido 2030, introduzione al presente volume, spec. § 12, ove il «circolo regolatorio» è descritto quale processo di interazione tra mercato e autorità, attraverso il quale le pratiche e le conoscenze maturate nell'esperienza economica possono concorrere alla definizione e all'evoluzione degli standard regolatori. Sul rapporto tra circolo regolatorio, regolazione partecipata e concerto regolatorio a due versanti, v. ivi.

In questa direzione assume rilevanza la progressiva integrazione dei servizi di mobilità, che richiede non soltanto regole coerenti, ma anche forme efficaci di coordinamento tra i diversi livelli di regolazione e di cooperazione con gli operatori economici e i soggetti responsabili delle infrastrutture. L'effettività della tutela dipende, inoltre, dalla capacità delle amministrazioni e degli enti affidanti di tradurre le prescrizioni regolatorie in scelte concrete di organizzazione dei servizi, standard qualitativi verificabili e adeguati strumenti di controllo. La crescente interdipendenza dei mercati rende così evidente che l'efficacia della regolazione non può essere valutata esclusivamente in relazione al contenuto delle regole, ma deve essere considerata anche rispetto alle condizioni istituzionali e amministrative che ne consentono l'attuazione.

Al tempo stesso, l'efficienza del sistema non può essere disgiunta dalla sua effettiva accessibilità. Digitalizzazione, multimodalità e sostenibilità possono ampliare le possibilità di scelta e migliorare la qualità della mobilità, ma possono anche determinare nuove asimmetrie e forme di esclusione, soprattutto quando le caratteristiche dei servizi e delle infrastrutture non tengano adeguatamente conto delle differenti condizioni territoriali, economiche e individuali degli utenti. L'accessibilità, anche per le persone con disabilità o a mobilità ridotta, non rappresenta pertanto un elemento accessorio rispetto agli obiettivi di efficienza, ma concorre a definirne il significato in una prospettiva consumeristica. La sfida verso il 2030 sarà quella di assicurare che l'innovazione tecnologica si traduca in un effettivo ampliamento delle possibilità di mobilità, evitando che alla crescente integrazione dei servizi corrispondano nuove disuguaglianze nelle condizioni della loro fruizione.

Un ulteriore profilo riguarda la capacità della regolazione di valorizzare le informazioni provenienti dal funzionamento concreto del mercato. I reclami degli utenti, le attività di vigilanza e gli strumenti di analisi dei dati possono contribuire a individuare criticità ricorrenti e a valutare l'effettività delle prescrizioni esistenti, alimentando un processo di progressivo adattamento delle regole alle trasformazioni dei servizi. L'impiego dell'intelligenza artificiale può rafforzare questa dimensione conoscitiva, senza sostituire le valutazioni giuridiche e amministrative riservate all'Autorità. La regolazione anticipatoria non implica il superamento delle tradizionali funzioni di vigilanza ed enforcement, ma la possibilità di valorizzarne le risultanze anche ai fini della prevenzione delle criticità e del miglioramento delle condizioni di funzionamento del mercato.

Il passaggio dalla tutela del passeggero alla regolazione della mobilità non comporta, perciò, il superamento dei tradizionali diritti individuali, ma il loro inserimento in un sistema nel quale strumenti regolatori, rimedi individuali e conoscenza del mercato concorrono alla protezione dell'utente. La considerazione degli effetti di lungo periodo delle decisioni regolatorie, cui si collega anche la riflessione avviata dall'Autorità sulla Valutazione di impatto generazionale, contribuisce ad ampliare ulteriormente l'orizzonte temporale della tutela, collegando le scelte presenti alle condizioni di accessibilità, sostenibilità e qualità dei servizi futuri.

La domanda sul consumatore 2030 può allora essere rovesciata. Non si tratta soltanto di chiedersi quali diritti dovranno essere riconosciuti all'utente nel 2030, ma quali decisioni regolatorie debbano essere assunte oggi perché quei diritti possano essere effettivamente esercitati domani.

Nel mercato della mobilità del 2030, proteggere il consumatore significherà non soltanto riconoscergli un rimedio dopo il disservizio, ma soprattutto costruire, prima del viaggio, le condizioni regolatorie affinché quel disservizio possa essere prevenuto, il mercato rimanga accessibile e l'innovazione tecnologica si traduca in un effettivo ampliamento delle possibilità di mobilità.

È così, "in questo senso di marcia al 2030" prospettico, che la regolazione dei trasporti può essere letta come una forma avanzata di tutela del consumatore.

AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE (ARERA)

ARERA AL FRONTE. IL "CONSUMATORE 2030", TRA POLICRISI E MONITORAGGIO CONTINUO

(di Cristiana Lauri)

SOMMARIO: 1. Premessa: il 2030 come orizzonte regolatorio. 2. una regolazione alla prova della policrisi. 3. Energia elettrica e gas: mercati e reti. 4. I settori ambientali: acqua, rifiuti e telecalore. 5. Tecnologie abilitanti e rischi emergenti. 6. Tutela, enforcement e governance. 7. Conclusioni e raccomandazioni.

1. Premessa: il 2030 come orizzonte regolatorio

Interrogarsi sul rapporto tra *Authorities* e consumatori con lo sguardo rivolto al 2030 significa, per i settori regolati da ARERA, misurarsi con una data rilevante da molteplici punti di vista. Il 2030 è l'orizzonte degli Obiettivi di Sviluppo Sostenibile dell'Agenda ONU, dei principali target europei in materia di decarbonizzazione ed economia circolare[1] e, non da ultimo, dell'apertura alla concorrenza della distribuzione elettrica[2]. Esso rappresenta, inoltre, il traguardo intermedio del mandato settennale della quinta Consiliatura dell'Autorità, insediatasi il 1° gennaio 2026, il cui primo Quadro strategico copre il quadriennio 2026-2029.[3]

La strategia di ARERA verso il 2030 prosegue un percorso già avviato, secondo il quale l'Autorità accompagna il passaggio da un consumatore da *proteggere* a un consumatore capace di *agire*: un soggetto che, secondo le parole del Presidente, «non subisce il mercato, bensì lo usa» e partecipa alla transizione energetica attraverso strumenti come l'autoconsumo, le comunità energetiche e la domanda flessibile[4]. La stessa Autorità riconosce, tuttavia, lo iato esistente tra questo orizzonte e la realtà della fase attuale. È infatti fondamentale, nell'attuale contesto di "ibridazione" – tra Stati e imprese, tra pubblico e privato e della stessa "matrice regolatoria" – che i legislatori non sbilancino le loro scelte sulla presunta "capacità aumentata" dell'utilizzatore-consumatore[5], rinunciando a spazi di esercizio di sovranità, giocoforza erosi da poteri privati emergenti in grado di disegnare la creazione dei prodotti accessibili sul mercato e il loro uso.

È proprio tale iato, letto alla luce delle crisi che attraversano i settori regolati e delle trasformazioni tecnologiche in corso, a costituire l'oggetto delle considerazioni che seguono.

2. Una regolazione alla prova della policrisi

1. Sul versante della decarbonizzazione, il quadro europeo fissa al 2030 una riduzione netta delle emissioni di gas a effetto serra di almeno il 55% rispetto ai livelli del 1990, nella prospettiva della neutralità climatica al 2050 (Regolamento (UE) 2021/1119, «Normativa europea sul clima»). A tale obiettivo si affiancano: una quota di energia da fonti rinnovabili pari ad almeno il 42,5% del consumo finale lordo, cui si aggiunge un obiettivo indicativo ulteriore del 2,5% (Direttiva (UE) 2023/2413, c.d. RED III); una riduzione dell'11,7% del consumo di energia finale rispetto alle proiezioni dello scenario di riferimento 2020 (Direttiva (UE) 2023/1791); una riduzione del 62% rispetto al 2005 delle emissioni dei settori soggetti all'EU ETS (Direttiva (UE) 2023/959) e, per i settori non ETS, del 43,7% per l'Italia (Regolamento (UE) 2023/857, c.d. Effort Sharing); l'obbligo di edifici di nuova costruzione a emissioni zero dal 2030 (dal 2028 per quelli pubblici), unitamente a una riduzione di almeno il 16% del consumo medio di energia primaria del parco residenziale rispetto al 2020 (Direttiva (UE) 2024/1275). A livello nazionale, il PNIEC 2024 prevede una quota di rinnovabili del 39,4% sui consumi finali lordi e del 63,4% nel settore elettrico. In materia di economia circolare, l'obiettivo di preparazione per il riutilizzo e riciclaggio dei rifiuti urbani è fissato al 60% entro il 2030, dopo il 55% al 2025 e prima del 65% al 2035 (Direttiva 2008/98/CE, come modificata dalla Direttiva (UE) 2018/851, art. 11). È inoltre previsto il riciclaggio del 70% dei rifiuti di imballaggio, con obiettivi specifici per materiale, tra cui il 55% per la plastica (Direttiva 94/62/CE, come modificata dalla Direttiva (UE) 2018/852; obiettivi ora confermati dal Regolamento (UE) 2025/40). Dal 2030 vige il divieto di collocare in discarica i rifiuti idonei al riciclaggio, e le discariche non potranno accogliere più del 10% dei rifiuti urbani entro il 2035 (Direttiva 1999/31/CE, come modificata dalla Direttiva (UE) 2018/850). Il Piano d'azione per l'economia circolare (COM(2020) 98 final) indica infine l'obiettivo programmatico di raddoppiare, entro il 2030, il tasso di utilizzo circolare dei materiali.

2. La scadenza delle concessioni di distribuzione elettrica, fissata al 31 dicembre 2030 dal d.lgs. n. 79/1999, è stata rimessa in discussione dal meccanismo di proroga introdotto dalla legge di bilancio 2025 (L. 30 dicembre 2024, n. 207, art. 1, commi 50 e ss.), che consente ai concessionari di ottenere, previa approvazione di piani straordinari di investimento pluriennali e versamento di un corrispettivo, una rimodulazione della durata della concessione per un periodo non superiore a vent'anni. Sul punto si vedano ARERA, documento per la consultazione 5 giugno 2025, 238/2025/R/eel, e AGCM, segnalazione AS2079 del 30 aprile 2025.

3. La Relazione annuale 2026, la prima del nuovo Collegio, è stata presentata a Parlamento e Governo il 1° luglio 2026. Cfr. inolre ARERA, Quadro strategico 2026-2029 dell'Autorità di Regolazione per Energia Reti e Ambiente, documento per la consultazione 244/2026/A del 9 luglio 2026, con termine per le osservazioni fissato al 15 settembre 2026; le audizioni periodiche degli stakeholder si sono svolte a Roma il 10 e l'11 settembre 2026

4. Relazione annuale sullo stato dei servizi e sull'attività svolta. Presentazione del Presidente, Roma, 1° luglio 2026.

5. F. Bassan, L'era ibrida. Sovranità e democrazia tra poteri pubblici e imprese tech, Rubbettino, 2026.

Nei settori regolati da ARERA particolarmente evidente è la compresenza di crisi interconnesse che si rafforzano reciprocamente, fino a produrre effetti che travalicano le singole componenti. Tale scenario di *policrisi* si articola almeno lungo quattro direttrici[6].

Anzitutto, sul piano geopolitico ed energetico. Se il 2025 è stato un anno di consolidamento dopo la crisi dei prezzi, il primo trimestre del 2026 ha registrato una nuova impennata delle quotazioni del gas sui mercati europei. Il Prezzo Unico Nazionale (PUN)[7] medio del 2025 si è attestato a 115,9 €/MWh (+7% sul 2024), il valore più elevato tra le principali borse europee, a fronte dei 61,1 €/MWh della Francia e dei 65,3 €/MWh della Spagna[8]: tale differenziale, riconducibile alla forte dipendenza della generazione dal gas, pesa tanto sui bilanci delle famiglie quanto sulla competitività del sistema produttivo.

Rileva poi la crisi climatica, che si manifesta con maggiore evidenza nel settore idrico, dove la scarsità della risorsa non è più un'emergenza episodica ma, come afferma l'Autorità, «una condizione strutturale da governare», peraltro in un più ampio quadro di fragilità territoriale e di concause sul piano ambientale. La stessa crisi sanitaria contemporanea rappresenta una proiezione di una più ampia crisi ecosistemica, in cui il rischio sanitario emerge come rischio strutturalmente relazionale, generato all'interno di sistemi socio-ecologici complessi e adattativi lungo catene causali che attraversano indistintamente ambiente, animali, esseri umani, sistemi produttivi e modelli di consumo[9]. Dal punto di vista sociale, le reiterate tensioni sui prezzi hanno ampliato l'area della vulnerabilità economica, rendendo i bonus sociali un presidio stabile e non più straordinario.

Non da ultimo, senz'altro baricentrica in una considerazione di sistema, è una crisi di *governance*, legata alla frammentazione dei livelli di competenza che caratterizza soprattutto i servizi ambientali ma anche alla menzionata "ibridazione" tra soggetti pubblici e privati, che soggiace ai mercati e alle regole.

La risposta regolatoria a questo scenario segna il passaggio da una logica emergenziale, prevalente nel biennio 2022-2023, a una logica di intervento strutturale. Ne sono espressione l'istituzione di un'Unità di Vigilanza Energetica, deputata al monitoraggio quotidiano dei prezzi all'ingrosso e al dettaglio con un canale diretto verso Governo, Parlamento e istituzioni europee, e l'indicazione del disaccoppiamento tra prezzo dell'energia elettrica e prezzo del gas come direttrice permanente dell'azione dell'Autorità, unitamente al rafforzamento della sorveglianza REMIT in coordinamento con ACER[10]. Manipolazioni o abusi sul mercato all'ingrosso rischiano infatti di tradursi in prezzi più alti in bolletta, determinando l'urgenza del tema in una fase di prezzi volatili come l'inizio del 2026.

3. Energia elettrica e gas: mercati e reti

Sul versante dei mercati all'ingrosso, la sfida al 2030 coincide con l'integrazione di una quota crescente di fonti rinnovabili. Il raggiungimento dell'obiettivo non appare però di scontata portata se si considera che, come mostrato dalla Relazione annuale, nell'ambito di una domanda italiana soddisfatta per l'85% dalla produzione nazionale netta e per il restante 15% dal saldo con l'estero, rispetto al 2024 si assiste a un'inversione di tendenza con le rinnovabili, che coprono il 48% del mix, in diminuzione (-1,5%) e il termoelettrico in ripresa (+5,2%). Nello specifico, a crescere sono state la generazione da gas naturale (aumentata del 7%) e quella fotovoltaica (del 25%) mentre eolico e idroelettrico hanno segnato un calo rispettivamente del 3% e del 21%.

L'adozione del Testo Integrato del Dispacciamento Elettrico (TIDE)[11] ha aperto i servizi di bilanciamento a tutte le risorse – accumuli, carichi flessibili, aggregati distribuiti – in condizioni di neutralità tecnologica, e il percorso proseguirà con il superamento graduale del PUN e la piena applicazione dei prezzi zonali.

Per i consumatori la transizione verso segnali di prezzo territorialmente differenziati solleva questioni distributive che meritano di essere monitorate e, se necessario, accompagnate da misure dedicate.

Il secondo fronte è quello delle reti. Il ciclo di investimenti, osserva l'Autorità, «non è destinato a ridursi»: generazione distribuita, elettrificazione dei consumi e adattamento climatico richiedono infrastrutture più capienti e resilienti. La transizione verso la Regolazione per Obiettivi di Spesa e di Servizio (ROSS), il testo unico delle connessioni – con misure contro la saturazione virtuale della rete – e la promozione di soluzioni *non-wire* e di *grid-enhancing technologies* rispondono all'interrogativo di fondo che interessa direttamente i consumatori: chi sostiene il costo della transizione

6. Cfr. WORLD ECONOMIC FORUM, Global Risks Report 2023, Ginevra, 2023.
7. Il PUN (Prezzo Unico Nazionale) è il prezzo di riferimento dell'energia elettrica all'ingrosso in Italia. Si forma sulla borsa elettrica gestita dal GME (Gestore dei Mercati Energetici), nel Mercato del Giorno Prima (MGP), e viene calcolato per ogni ora del giorno.
8. Relazione annuale 2026, Stato dei servizi, Volume 1. Per le imprese, il prezzo finale dell'energia elettrica risulta superiore del 24,1% rispetto alla media dell'Area euro.
9. E. Scotti, Digital one health. un'analisi giuridica, in Ambientediritto, 2026.
10. Regolamento (UE) n. 1227/2011 (REMIT), come modificato dal Regolamento (UE) 2024/1106. Sul disaccoppiamento si veda anche la riforma europea del market design: Direttiva (UE) 2024/1711 e Regolamento (UE) 2024/1747.
11. **Delibera ARERA 25 luglio 2023, n. 345/2023/R/eel.**

infrastrutturale[12].
A ciò si aggiungono le nuove competenze in via di attribuzione: il decreto legislativo che designa ARERA quale autorità nazionale di regolazione per l'idrogeno è prossimo alla finalizzazione, e potrebbe seguire l'estensione della regolazione al trasporto e allo stoccaggio della CO_2.
Nel gas, la sfida è governare il progressivo ridimensionamento del vettore senza compromettere la sicurezza degli approvvigionamenti né generare costi non recuperabili a carico degli utenti.
Nel mercato retail la tensione tra obiettivi e realtà appare ancor più evidente. A due anni dal superamento del servizio di Maggior Tutela per i clienti domestici non vulnerabili, l'Autorità constata che nel mercato libero di piccola taglia «si scambia prevalentemente fiducia nel marchio dell'operatore, non *commodity*», che i differenziali tra le offerte scelte e quelle più efficienti restano elevati e che le decisioni di acquisto sono in larga parte svincolate dalla convenienza effettiva.
La riforma della bolletta entrata in vigore nel luglio 2025, il rafforzamento del Portale Offerte e l'aggiornamento del Codice di condotta commerciale mirano a colmare questa asimmetria, ma il banco di prova più atteso sarà il passaggio al mercato libero, previsto nel marzo 2027, dei clienti ancora serviti nel Servizio a Tutele Graduali.

4. I settori ambientali: acqua, rifiuti e telecalore

Nei settori ambientali la regolazione non opera su mercati liberalizzati ma su sistemi in cui la tariffa rappresenta lo strumento strutturale cardine per finanziare gli investimenti. Ne deriva un *trade-off* permanente tra accessibilità economica del servizio e sua qualità, che la regolazione è chiamata a comporre tenendo conto di profonde disuguaglianze territoriali.
Il servizio idrico è il settore in cui il cambiamento climatico si manifesta con maggiore immediatezza. Le perdite di rete si attestano mediamente al 42,5%, con punte più elevate nel Mezzogiorno; nel 2024 oltre un milione di residenti nei capoluoghi di provincia ha subito misure di razionamento; l'Italia è il primo Paese dell'Unione per prelievo di acqua a uso potabile, con 411 litri per abitante al giorno. Al tempo stesso, la regolazione ha prodotto risultati tangibili: la spesa per investimenti è passata da poco più di un miliardo di euro nel 2012 a oltre sei miliardi nel 2025, e nel quarto periodo regolatorio la spesa programmata ammonta a circa 28 miliardi.
Il Metodo Tariffario Idrico MTI-4 introduce l'indicatore "M0-Resilienza idrica", che per la prima volta incorpora nella regolazione il rapporto tra domanda e disponibilità della risorsa, in coerenza con la Strategia europea per la resilienza idrica[13].
È questo un settore in cui le incertezze sul piano della *governance* – soprattutto in alcune aree, come Campania e Sicilia – in particolare per quanto riguarda l'affidamento al gestore unico, genera effetti negativi sui consumatori utenti.
Nel ciclo dei rifiuti urbani la raccolta differenziata si avvicina al 70%, ma il tasso di riciclaggio si ferma al 52,3%, ancora distante dal 55% richiesto per il 2025 e dal 60% fissato per il 2030.[14]
L'adozione del Testo Integrato Corrispettivi Servizio Gestione Rifiuti (TICSER), primo riordino organico della tariffazione agli utenti dopo il d.P.R. 158/1999, apre la strada alla tariffazione puntuale secondo il principio «chi inquina paga», mentre il metodo tariffario MTR-3 disciplina il quadriennio 2026-2029.
L'esperienza del bonus rifiuti – uno sconto del 25% sulla TARI per le famiglie in disagio economico – ha tuttavia mostrato la complessità di attuare politiche uniformi in un sistema con circa 2.700 enti territorialmente competenti; di qui l'indicazione dell'Autorità in favore di Enti di governo d'ambito di dimensione almeno regionale.
Il telecalore, infine, è un settore in crescita strutturale – la volumetria allacciata è più che triplicata tra il 2000 e il 2024 – ma serve ancora circa il 3% delle utenze, concentrate per il 95% in cinque regioni del Nord. Inoltre, la competenza tariffaria, attribuita solo nel 2023, è ancora in costruzione: il metodo transitorio è stato prorogato di un anno e l'estensione del bonus sociale al settore, prevista dal d.l. n. 21/2026, dovrà essere definita nel dettaglio dall'Autorità.

5. Tecnologie abilitanti e rischi emergenti

La tecnologia attraversa trasversalmente tutti i settori regolati e si presenta, rispetto al consumatore, con una duplice valenza. Da un lato essa è la condizione stessa del consumatore attivo: contatori intelligenti, piattaforme di confronto delle offerte, integrazione tra Portale Offerte e Portale Consumi, sistemi di accumulo e di gestione della domanda consentono all'utente di conoscere i propri consumi, modularli e partecipare ai mercati[15]; dall'altro, la stessa infra-

12. Cfr. Terna, Pianificazione della rete elettrica, https://www.arera.it/fileadmin/allegati/operatori/pds/25/Pianificazione_della_rete_elettrica.pdf
13. Commissione europea, European Water Resilience Strategy, giugno 2025. Sul piano nazionale, l'Autorità ha avviato una collaborazione formale con le Autorità di Bacino Distrettuali in materia di pianificazione dell'uso della risorsa.
14. Direttiva 2008/98/CE, come modificata dalla Direttiva (UE) 2018/851, art. 11, par. 2.
15. Sul riconoscimento dei «clienti attivi» e delle comunità energetiche dei cittadini si veda la Direttiva (UE) 2019/944, artt. 15 e 16, e, per le comunità di energia rinnova-

struttura digitale moltiplica i rischi: pratiche commerciali aggressive, uso improprio dei dati personali nella fase di cambio fornitore, offerte dinamiche difficili da comprendere, esclusione di quanti non dispongono delle competenze o degli strumenti necessari.

Un ruolo specifico è riservato all'intelligenza artificiale, che il Quadro strategico affronta come tema trasversale a tutti i settori. L'Autorità la considera uno strumento fondamentale a supporto dell'*enforcement*, per rendere più sistematica e tempestiva l'individuazione di condotte scorrette. Tale prospettiva si inserisce in un quadro normativo ormai definito, che classifica come ad alto rischio i sistemi impiegati nella gestione delle infrastrutture critiche e nell'accesso ai servizi essenziali, e che impone anche alle amministrazioni requisiti di trasparenza e sorveglianza umana[16].

L'intelligenza artificiale è tuttavia anche un fattore di pressione sulle risorse che ARERA regola. L'Autorità ha segnalato la necessità di valutare l'impatto dei *data center* sul consumo di energia e di acqua, sollecitando uno sforzo congiunto che favorisca lo sviluppo di sistemi di produzione energetica sostenibile e di riuso della risorsa idrica[17].

È, questo, un tema destinato ad assumere crescente rilievo nei prossimi anni[18], poiché la domanda aggiuntiva generata da tali infrastrutture incide, in ultima analisi, sui costi di rete e sulla disponibilità delle risorse per gli altri utenti, oltre a contribuire in maniera decisiva alla c.d. "saturazione virtuale" delle reti[19]. Su altro fronte però, è necessario che il legislatore non perda l'occasione di delineare una disciplina – inclusi gli aspetti localizzativi – in grado di contribuire fruttuosamente alla diffusione dei *data center* sul territorio nazionale, presupposto per lo sviluppo applicativo dell'IA che sia realmente al servizio degli operatori del mercato e dei consumatori[20].

6. Tutela, enforcement e governance

Il lavoro svolto negli ultimi anni dalle Authority, in un clima di collaborazione con le Associazioni dei consumatori e con gli operatori di settore è confermato dati relativi alla tutela individuale, che confermano la maturazione del sistema: nel 2025 lo Sportello per il consumatore ha gestito quasi 787.000 chiamate e il Servizio Conciliazione circa 30.000 domande, consentendo di recuperare oltre 21 milioni di euro a favore degli utenti con un tasso di soddisfazione del 95%.

Rilevante è anche il percorso compiuto sul fronte del supporto sociale, laddove sono stati riconosciuti automaticamente circa 2,8 milioni di bonus elettrici e 1,7 milioni di bonus gas[21].

Per il quadriennio l'Autorità prospetta il potenziamento della conciliazione e delle Procedure Speciali Risolutive, la valutazione di un eventuale terzo livello decisorio per i casi non risolti in sede conciliativa e l'estensione della conciliazione obbligatoria al settore dei rifiuti. Le campagne informative saranno inoltre integrate in una strategia strutturata di *empowerment*, supportata da indagini demoscopiche sulla soddisfazione degli utenti e da pubblicazioni comparative sulla qualità dei servizi, anche con riferimento alla gestione dei reclami.

Rilevante è inoltre l'esplicito riconoscimento da parte dell'Authority che la tutela del consumatore non può essere esercitata «in solitudine». Fenomeni come il telemarketing aggressivo o l'uso improprio dei dati nella fase di cambio fornitore si collocano all'intersezione delle competenze di ARERA, AGCM, AGCOM e Garante per la protezione dei dati personali; di qui l'impegno a rafforzare la collaborazione istruttoria e le azioni di *enforcement* congiunto, atteso che «la frammentazione delle competenze, se non presidiata, si traduce in lacune di tutela».

Sul piano partecipativo, l'istituzione di un *Osservatorio della regolazione*, quale sede permanente di confronto con stakeholder, esperti e mondo della ricerca, offre alle Associazioni dei consumatori un ulteriore canale ulteriore di interlocuzione[22].

---

bile, alla Direttiva (UE) 2018/2001, art. 22.

16. Regolamento (UE) 2024/1689 (AI Act), Allegato III, punti 2 e 5; a livello nazionale, legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale. G. Sgueo, Punti di Vista sulla regolazione dei sistemi di intelligenza artificiale tra tutela della riservatezza e tutela dell'ambiente - La Commissione europea e il rischio inaccettabile, in Osservatorio sullo Stato Digitale, IRPA, 2025.

17. G. La Rosa-G. Delle Cave, Infrastrutture digitali e pianificazione del territorio: la localizzazione dei data center tra pubblica utilità e strategicità degli asset, in Ambientediritto, 2026; L. Pergolizzi, Il procedimento unico per la realizzazione dei Data Center, in Il Diritto Amministrativo, 2026.

18. I dati rilasciati dall'Osservatorio Data Center del Politecnico di Milano ("Dal rumore al valore: l'Italia come nuovo Data Center Hub europeo", gennaio 2026) rivelano che nel triennio 2023-2025 sono stati investiti in Italia 7,1 miliardi di euro nel settore, e per il periodo 2026-2028 si stimano ulteriori 25,4 miliardi di euro legati a 83 nuovi progetti annunciati da 30 aziende, il 72% dei quali riconducibile a nuovi operatori internazionali non ancora attivi in Italia.

19. Cui il legislatore fa specifico riferimento nel preambolo del d.l. 21/2026, Misure urgenti per la riduzione del costo dell'energia elettrica e del gas in favore delle famiglie e delle imprese, per la competitività delle imprese e per la decarbonizzazione delle industrie, nonché disposizioni urgenti in materia di risoluzione della saturazione virtuale delle reti elettriche e di integrazione dei centri di elaborazione dati nel sistema elettrico, dove si richiama la "straordinaria necessità e urgenza di introdurre misure finalizzate a favorire la risoluzione della saturazione virtuale delle reti elettriche e di integrazione dei centri di elaborazione dati nel sistema elettrico". Da ultimo v. Decreto MASE n. 291 dell'8 settembre 2026, nuove regole per la gestione e l'accesso alla capacità della rete nazionale.

20. Cfr. Disegno di legge n. 1821, art. 2, approvato dalla Camera dei deputati il 24 febbraio, trasmesso al Senato il 26 febbraio 2026; Regolamento delegato (UE) 2024/1364 della Commissione, del 14 marzo 2024, che integra la direttiva (UE) 2023/1791 del Parlamento europeo e del Consiglio istituendo un sistema comune dell'Unione per classificare la sostenibilità dei centri dati.

21. Relazione annuale 2026, Vol. 2, Attività svolta.

22. https://www.arera.it/autorita/osservatorio.

7. Conclusioni e raccomandazioni

La lettura congiunta della Relazione annuale e del Quadro strategico restituisce l'immagine di un regolatore consapevole che la propria efficacia, da qui al 2030, si misurerà sulla capacità di comporre le tensioni date dal descritto scenario di policrisi.

In primo luogo, quella tra investimenti e accessibilità: reti elettriche, resilienza idrica e impiantistica per i rifiuti richiedono risorse ingenti che, in larga parte, transitano per la tariffa. In secondo luogo, quella tra attivazione e vulnerabilità: il consumatore attivo rischia di coincidere con il consumatore già attrezzato, lasciando indietro chi non dispone di risorse economiche, competenze digitali o abitazioni adeguate. In terzo luogo, quella tra innovazione e inclusione: dati, flessibilità e intelligenza artificiale possono rafforzare la tutela, ma anche generare nuove asimmetrie.

In questa prospettiva, e in coerenza con la formula dell'Autorità secondo cui «equità di accesso alla transizione è, in fondo, la forma più concreta di tutela del consumatore nel tempo che viene», si possono formulare alcune raccomandazioni:

- accompagnare il passaggio dei clienti del Servizio a Tutele Graduali al mercato libero (marzo 2027) con un monitoraggio pubblico fondato su indicatori di esito, come ad esempio i prezzi effettivamente pagati, i tassi di cambio fornitore, e i reclami;
- definire un set comune di indicatori di *consumer outcome* per tutti i settori regolati, pubblicato con cadenza regolare, così da rendere comparabili tra loro i servizi regolati sotto il profilo della tutela;
- armonizzare *bonus* e strumenti di tutela sociale tra i diversi settori, valorizzando il meccanismo di riconoscimento automatico e superando le difficoltà di attuazione emerse nel settore dei rifiuti, per sua conformazione fortemente frammentato;
- introdurre criteri espliciti di equità distributiva nella transizione ai prezzi zonali e nella tariffazione delle reti, evitando che il costo della transizione ricada in misura sproporzionata sulle fasce e sui territori più fragili;
- sostenere programmi strutturati di alfabetizzazione energetica e ambientale, in *partnership* con le associazioni dei consumatori, volti a massimizzare l'utilizzo e l'efficacia degli strumenti informativi (bolletta, Portale Offerte, Portale Consumi);
- proseguire il percorso di consolidamento, anche attraverso protocolli operativi, del coordinamento con le altre Authorities, in particolare AGCM, AGCOM, Garante privacy e in via crescente, ACN;
- accompagnare l'impiego dell'intelligenza artificiale nell'*enforcement* con garanzie di trasparenza e di supervisione umana;
- nel lungo periodo, si renderà necessario valutare nella regolazione delle connessioni e delle tariffe l'impatto dei *data center* sulle risorse energetiche e idriche;

Il 2030 appare, esso stesso, come un orizzonte in crisi: l'instabilità del sistema richiede flessibilità degli strumenti in grado di generare, all'occorrenza, scelte e risposte immediate, ma anche di adattare il quadro delle regole tracciate in base alla concreta evoluzione degli sviluppi tecnologici, dei mercati e delle scelte di consumo.

Il potenziamento di un consumatore "a capacità aumentate" nei settori di competenza di ARERA rappresenta un obiettivo essenziale nel contesto di ibridazione che caratterizza gli spazi regolatori.

Affinché tale percorso non resti un'astrazione, occorrerà che la regolazione continui a misurarsi, anno dopo anno, e attraverso un monitoraggio capillare, con lo iato e le crisi che la separano dall'effettivo raggiungimento dei risultati attesi.

AUTORITA NAZIONALE ANTICORRUZIONE

SOVRANITÀ DIGITALE E CONTRATTI PUBBLICI: IL NUOVO PARADIGMA DEGLI AFFIDAMENTI *CLOUD* E *AI*

(di Serafina Piantedosi) [1]

La trasformazione digitale della P.A. rende il cloud computing e l'intelligenza artificiale sempre più rilevanti per l'esercizio delle funzioni pubbliche e per l'erogazione dei servizi ai cittadini. Con l'approvazione della proposta di regolamento europeo Cloud and AI Development Act (CADA), parte del più ampio Tech Sovereignty Package, diviene evidente come la sovranità tecnologica non possa più essere considerata una categoria esclusivamente politica o industriale, ma debba assumere rilievo concreto anche nella disciplina dei contratti pubblici. I livelli europei di assurance, le valutazioni del rischio, il valore aggiunto europeo, gli acquisti comuni, la Federazione europea del cloud nel settore pubblico incidono, infatti, sulle modalità con cui le stazioni appaltanti sono chiamate a definire i propri fabbisogni, predisporre i capitolati e selezionare i fornitori. Negli affidamenti tecnologici, infatti, la tutela del consumatore-cittadino passa anche dalla continuità del servizio, dalla protezione dei dati, dalla portabilità, dall'interoperabilità e dalla prevenzione delle dipendenze tecnologiche. Le infrastrutture digitali, pur rimanendo spesso invisibili al cittadino, condizionano ormai in modo decisivo l'esercizio dei diritti e l'affidabilità dei servizi pubblici. La sfida dei prossimi anni, quindi, sarà quella di trasformare la sovranità digitale da principio generale a pratica amministrativa.

SOMMARIO: 1. Sovranità digitale e infrastrutture immateriali: il Cloud and Ai Development Act. 2. Lo sviluppo di un ecosistema europeo del cloud e dell'IA 3. Gli affidamenti pubblici per cloud e intelligenza artificiale. 4. Le prospettive di vigilanza e il possibile ruolo di ANAC. 5. Conclusioni.

1. SOVRANITÀ DIGITALE E INFRASTRUTTURE IMMATERIALI: *IL CLOUD AND AI DEVELOPMENT ACT*.

La trasformazione digitale che ha interessato le pubbliche amministrazioni negli ultimi anni non può essere considerata come una semplice evoluzione degli strumenti utilizzati nello svolgimento dell'attività amministrativa. Il passaggio dalla carta al digitale, dalla comunicazione tradizionale alle piattaforme telematiche, dalle banche dati isolate a sistemi interoperabili, ha modificato profondamente l'organizzazione pubblica e le modalità attraverso cui cittadini e imprese accedono ai servizi.

La digitalizzazione dell'amministrazione rappresenta certamente un'occasione per agevolare le interazioni tra Stato e cittadini, per ridurre gli oneri burocratici e per velocizzare l'istruttoria dei procedimenti amministrativi, tuttavia, l'adozione di tecnologie sempre più avanzate espone l'amministrazione a nuove forme di vulnerabilità, dal momento che oggi il funzionamento di una parte consistente dei servizi pubblici dipende da dati, *software*, archivi digitali, servizi *cloud* e sistemi di intelligenza artificiale, che ormai costituiscono l'ossatura invisibile dei servizi pubblici contemporanei.

Come le strade, i ponti, gli ospedali, le reti energetiche e quelle di trasporto costituiscono le infrastrutture "materiali" che consentono di realizzare gli interessi pubblici dei cittadini, allo stesso modo, le infrastrutture "immateriali", come il *cloud*, le piattaforme, gli algoritmi, le reti e i *data center*, consentono il funzionamento della società digitale, con la conseguenza che la loro indisponibilità incide direttamente sui cittadini, sull'economia e sulla capacità delle istituzioni di adempiere alle proprie funzioni.

Garantire la sicurezza, l'accessibilità e la continuità di tali infrastrutture immateriali diventa perciò fondamentale per assicurare il buon andamento dell'amministrazione pubblica.

Per tali ragioni diviene fondamentale garantire la sovranità digitale sui dati, sui *software* e sulle infrastrutture tecnologiche di cui si avvalgono le istituzioni nazionali ed europee. Uno degli elementi centrali del dibattito sulla sovranità

1. 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.

digitale, infatti, è la necessità di individuare il modello ideale di *governance* delle piattaforme online e, più in generale delle infrastrutture digitali, un modello che dovrebbe essere volto a far fronte al "gigantismo" economico delle piattaforme e a eliminare gli eccessi delle logiche di accumulazione di dati personali e non personali, tipiche della *data economy* di cui sono protagoniste[2].

Infatti, la riflessione sulla sovranità digitale nasce proprio dalla preoccupazione degli effetti che possa avere la crescente concentrazione del potere tecnologico in capo ad un numero limitato di operatori privati, specie se extra-UE, dal momento che l'affermazione delle grandi piattaforme ha determinato nuove geometrie di potere, nelle quali soggetti privati possono incidere in modo significativo sulle condizioni di accesso ai servizi digitali e sull'utilizzo dei dati[3].

Da qui la necessità a livello europeo di una regolamentazione che consentisse di implementare la sovranità digitale.

La prospettiva della proposta di regolamento europeo denominata *Cloud and AI Development Act* (d'ora in avanti CADA)[4], quindi, è proprio quella di impedire gli affidamenti dei servizi *cloud* e IA ad un singolo fornitore extra-UE, al fine di evitare di creare una dipendenza che, in caso di interruzione del servizio, tensioni geopolitiche o variazione unilaterale delle condizioni contrattuali, possa tradursi in un problema di continuità operativa per servizi essenziali per i cittadini europei.

Per tali ragioni, il CADA, nel Titolo IV, intitolato "*Autonomy*", circoscrive il concetto di sovranità digitale nell'ambito dei contratti pubblici, stabilendo che essa non coincide con la sola tutela dei dati personali dei cittadini, ma comprende anche la sicurezza informatica, l'autonomia operativa, la possibilità di migrare da una soluzione tecnologica a un'altra, la capacità di prevenire forme di dipendenze tecnologiche irreversibili e di non subire passivamente le condizioni imposte da un operatore economico[5], per cui la sovranità digitale cessa di essere una formula astratta e diventa un parametro concreto, destinato ad informare le decisioni di acquisto delle pubbliche amministrazioni.

Queste ultime, infatti, quando affidano un servizio *cloud* o acquistano un sistema di intelligenza artificiale non si limitano ad acquisire una prestazione tecnica, ma compiono una scelta capace di incidere nel tempo sulla disponibilità delle informazioni, sulla sicurezza dei dati e sulla qualità dei servizi offerti alla collettività.

Pertanto, l'acquisto di servizi tecnologici non attiene più soltanto alla convenienza economica dell'appalto, ma riguarda l'efficienza dell'azione amministrativa e, in ultima analisi, la tutela del cittadino-consumatore, tutte le volte in cui si trovi ad accedere ad un servizio sanitario digitale, ad una piattaforma fiscale o previdenziale, ad un servizio di identità digitale. In tutte queste ipotesi occorre scongiurare le conseguenze di un'eventuale interruzione improvvisa del servizio o, più in generale, dalle eventuali inefficienze cagionate da una cattiva scelta contrattuale dell'amministrazione.

La proposta di regolamento CADA, dunque, mira a rendere la sovranità tecnologica un obiettivo concretamente perseguibile attraverso regole, criteri di valutazione, procedure di *audit* e strumenti di cooperazione. In tal modo, la sovranità digitale cessa di essere una formula astratta e diventa un parametro destinato ad incidere sulle decisioni di acquisto delle amministrazioni pubbliche[6].

2. LO SVILUPPO DI UN ECOSISTEMA EUROPEO DEL *CLOUD* E DELL'IA.

2. Così F. Rotolo, Le digital wars tra istanze di sicurezza nazionale e gigantismo delle piattaforme: che fine hanno fatto gli utenti? (Nota a Corte suprema Stati uniti d'America 17 gennaio 2025, TikTok Inc.), in Foro Ita., Anno CL n. 6 - giugno 2025, p. 301.

3. La Corte di giustizia dell'Unione europea nelle sentenze Kolin (Corte giust. 22 ottobre 2024, causa C-652/22, Foro it., 2025, IV, 82) e Qingdao (Corte giust. 13 marzo 2025, causa C-266/22, ForoPlus) ha precisato che nell'ambito del diritto dell'Unione europea, non esiste una disposizione generale che imponga l'esclusione automatica dalla gara degli operatori economici aventi sedi in paesi terzi non membri Ue per il solo fatto che non abbiano stipulato con l'Unione un accordo internazionale sugli appalti pubblici (AAP), per cui è la stazione appaltante che può valutare se debbano essere ammessi a una procedura di aggiudicazione di un appalto pubblico gli operatori economici di un paese terzo. Per tali ragioni, non esistendo un divieto assoluto in tal senso, anche gli operatori extra-UE operanti in ambito tecnologico potrebbero partecipare alle gare in materia di cloud e IA bandite da stazioni appaltanti di Paesi dell'UE. Sul punto si veda M. Buccarella, Operatori economici extra-Ue e appalti pubblici: riflessioni critiche a partire dall'impatto della saga "Kolin/Qingdao" sull'ordinamento italiano (Nota a Cons. Stato, sez. V, 2 maggio 2025, n. 3721), in Foro Ita., Anno CL, n. 6 -giugno 2025, p. 257 ss..

4. Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce un quadro di misure per rafforzare l'ecosistema europeo del cloud e dell'IA (regolamento sullo sviluppo del cloud e dell'IA), COM(2026) 502, 2026/0138 (COD).

5. Il CADA cerca di prevenire il fenomeno del c.d. "vendor lock-in" (o "blocco da fornitore") che origina una forma di dipendenza economica e tecnologica nella quale l'utilizzatore di un servizio digitale, una volta adottata la soluzione di uno specifico fornitore, incontra ostacoli tecnici, contrattuali, organizzativi o finanziari tali da rendere eccessivamente oneroso, complesso o rischioso il passaggio a un diverso operatore. Nel settore del cloud computing, il fenomeno si manifesta soprattutto quando dati, applicazioni, configurazioni e processi operativi risultano strettamente integrati nell'ecosistema proprietario del provider, rendendo difficoltose la portabilità, l'interoperabilità e la continuità operativa in caso di migrazione. La dipendenza da un unico fornitore, infatti, può rendere estremamente difficile il passaggio a soluzioni alternative, soprattutto quando i dati e i processi amministrativi sono costruiti intorno a standard proprietari o a strumenti non interoperabili. La conseguenza può essere un aumento dei costi di migrazione, l'impossibilità di accedere a tecnologie diverse e, nei casi più gravi, una concreta vulnerabilità della continuità del servizio. Sul punto si veda J. Opara-Martins, R. Sahandi, F. Tian, Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective, in Journal of Cloud Computing: Advances, Systems and Applications, (2016) 5:4.

6. La dottrina ha evidenziato come il modello europeo di sovranità regolatoria cerchi di distinguersi tanto dalla centralità delle grandi piattaforme private, tipica dell'esperienza statunitense, quanto dal controllo diretto e pervasivo dello Stato, caratteristico di altri modelli geopolitici. L'Unione europea tende, infatti, a costruire un modello fondato sulla tutela dei diritti, sulla trasparenza, sulla responsabilità degli operatori e sulla ricerca di un equilibrio tra innovazione, mercato e interesse pubblico. Cfr. F. Faini, Umanesimo digitale e sovranità regolatoria: il governo dell'intelligenza artificiale tra diritto europeo e nazionale, in federalismi.it, n. 35/2025, pp. 63 ss.; A. Bradford, The Brussels Effect. How the European Union Rules the World, Oxford University Press, Oxford, 2020; F. Rotolo, Le digital wars tra istanze di sicurezza nazionale e gigantismo delle piattaforme: che fine hanno fatto gli utenti?, cit..

Il CADA si inserisce nel più ampio percorso europeo volto a rafforzare la capacità dell'Unione europea di sviluppare e utilizzare tecnologie digitali avanzate.
La proposta di regolamento prende atto della crescente centralità del *cloud computing* e dell'intelligenza artificiale per il funzionamento dell'economia, della società e delle istituzioni pubbliche e individua nella disponibilità di infrastrutture digitali sicure, resilienti e sostenibili una condizione essenziale per l'autonomia strategica unionale.
Nel CADA si parte dal presupposto secondo cui la capacità europea di *data center* è ancora limitata e geograficamente concentrata, mentre il mercato dei servizi *cloud* è dominato da un numero ristretto di grandi fornitori non europei[7]. Tale dipendenza non produce soltanto effetti sul piano economico, ma espone le organizzazioni pubbliche e private a rischi concernenti l'accesso ai dati, la continuità operativa e la sottoposizione a discipline straniere con effetto extraterritoriale, che potrebbero essere in conflitto con i diritti fondamentali e la normativa dell'UE in materia di protezione dei dati.
Nel complesso, le misure presentate nella proposta gettano le basi per un ecosistema del *cloud* e dell'IA dell'UE resiliente e ad alte prestazioni e mirano a far sì che l'Europa non sia un mero consumatore di tecnologie digitali avanzate, bensì un polo di riferimento mondiale per infrastrutture digitali affidabili e sovrane, in grado di plasmare le norme e i mercati della prossima ondata tecnologica.
L'obiettivo, però, non è soltanto quello di sostenere un'offerta tecnologica europea più competitiva, ma anche di creare le condizioni affinché le amministrazioni possano effettuare scelte di approvvigionamento più informate, trasparenti e maggiormente orientate alla resilienza.
Il fulcro della proposta che assume maggior rilievo nell'ambito dei contratti pubblici è contenuto nel Titolo IV del CADA.
Il Capo I, Sezione I, istituisce un quadro europeo di sovranità per i servizi di *cloud computing*. L'art. 16 prevede, in particolare, quattro livelli di "*Union assurance*", i cui requisiti sono indicati nell'Allegato II della proposta. I prestatori di servizi *cloud* che intendano offrire le proprie soluzioni agli enti dell'Unione e agli organismi del settore pubblico dovranno dimostrare la conformità ai criteri previsti per il corrispondente livello di *assurance*. La rilevanza della disposizione è evidente. La sovranità del *cloud* non viene definita attraverso una clausola generale o una mera dichiarazione di principio, ma viene articolata in livelli graduati e sottoposti a forme di verifica. In questo modo, il concetto di *cloud* sovrano viene sottratto al rischio di rimanere una formula evocativa e viene ricondotto a requisiti suscettibili di accertamento.
La proposta distingue, sotto il profilo della procedura, il primo livello di *assurance* dai successivi. Per ottenere il riconoscimento del livello 1, il provider può svolgere un'autovalutazione di conformità e rendere pubblica una dichiarazione UE di conformità. Per i livelli 2, 3 e 4, invece, è previsto il ricorso a un *audit* indipendente da parte di soggetti terzi indipendenti[8]. Il sistema è completato dall'istituzione di un registro centrale dei servizi *cloud* riconosciuti, destinato a offrire alle amministrazioni un punto di riferimento per individuare le soluzioni conformi ai diversi livelli europei di garanzia.
Tale meccanismo risponde all'esigenza di rendere suscettibili di verifica gli elementi che compongono la sovranità tecnologica. Non è sufficiente, infatti, che un servizio *cloud* sia fisicamente localizzato all'interno dell'Unione, ma occorre considerare ulteriori elementi, quali l'assetto di controllo del fornitore, la disciplina applicabile all'accesso ai dati interessati, la sicurezza della catena di subfornitura, le misure eventualmente previste per garantire la continuità operativa, le condizioni di uscita dal contratto, anche al fine di evitare dipendenze tecnologiche. La sovranità è, dunque, un concetto complesso, che riguarda sia il luogo in cui si trovano le infrastrutture sia le condizioni giuridiche, organizzative e tecniche che ne regolano l'utilizzo.
La proposta attribuisce un ruolo centrale alle valutazioni del rischio. L'art. 29 prevede che gli Stati membri e gli enti dell'Unione effettuino valutazioni per determinare il livello di *assurance* richiesto in relazione alle diverse attività del settore pubblico. La scelta deve tenere conto della sensibilità, della criticità e della quantità dei dati personali e non personali trattati, della rilevanza dell'attività svolta dalla stazione appaltante e degli obblighi previsti dalla normativa europea di settore.
L'articolo 30 del CADA traduce tale valutazione in una regola di *procurement*. Le amministrazioni che acquistano servizi di *cloud computing* devono, come soglia minima, ricorrere a servizi che offrono un livello di affidabilità di livello 1 dell'Unione. Le amministrazioni aggiudicatrici, compresi i soggetti che agiscono per loro conto, le cui attività sono

7. Cfr. Considerando n. 4 del CADA.
8. I criteri relativi ai quattro livelli di affidabilità richiesti dell'Unione sono indicati nell'Allegato II del CADA e sono: livello 1 quando i dati sono trattati e conservati in infrastrutture situate nell'Unione; livello 2 quando i fornitori devono dimostrare l'indipendenza dai paesi terzi e la trasparenza sulla loro catena di fornitura di software; livello 3 quando i fornitori devono essere di proprietà e controllati dall'UE e soddisfare criteri aggiuntivi, come la cittadinanza del personale e la Commissione può riconoscere i fornitori di paesi terzi; livello 4 quando i fornitori hanno piena trasparenza e controllo sulla loro catena di fornitura del software e nessuna interferenza da un paese terzo.

state individuate come attività che contribuiscono al mantenimento dell'ordine pubblico e nei settori della sicurezza nazionale, della sicurezza interna, della gestione delle frontiere esterne, della difesa, della giustizia o dell'attività di contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, acquistano solo servizi di *cloud computing* che sono stati riconosciuti come servizi che offrono il livello di affidabilità 2, 3 o 4 dell'Unione.
Ne deriva una regolazione graduata, nella quale il livello di garanzia richiesto non dipende dalla generica natura pubblica del soggetto acquirente, ma dalla concreta criticità del servizio e delle informazioni trattate.
Il modello proposto appare coerente con un approccio basato sul rischio, ormai diffuso nella regolazione europea delle tecnologie digitali.
L'AI Act, il GDPR, la normativa in materia di cybersicurezza e le discipline sulla resilienza digitale mostrano, infatti, la tendenza del legislatore europeo a graduare obblighi e responsabilità in funzione dell'impatto delle tecnologie sui diritti, sulla sicurezza e sul corretto funzionamento dei mercati.
Il CADA, quindi, applica la medesima logica al *cloud computing*, individuando nella valutazione preventiva del rischio lo strumento attraverso cui rendere proporzionate le scelte delle amministrazioni.

3. GLI AFFIDAMENTI PUBBLICI PER *CLOUD* E INTELLIGENZA ARTIFICIALE.

Le disposizioni del CADA producono conseguenze rilevanti sulle modalità di progettazione e gestione degli affidamenti pubblici relativi al *cloud computing* e ai sistemi di intelligenza artificiale.
Il primo effetto consiste nel superamento della concezione dell'appalto tecnologico come semplice acquisizione di un servizio standardizzato, infatti, le stazioni appaltanti nella fase della redazione del capitolato tecnico non potranno limitarsi ad indicare genericamente il servizio di archiviazione, elaborazione o analisi dei dati, ma dovranno valutare quale livello di affidabilità sia richiesto per lo specifico servizio, se il trattamento riguardi dati sensibili o attività critiche, quali effetti deriverebbero da un'interruzione del servizio e quale grado di dipendenza dal fornitore risulti tollerabile.
La valutazione di sovranità, quindi, diventa parte integrante dell'istruttoria amministrativa e condiziona anche la fase successiva della redazione della documentazione di gara.
La seconda conseguenza del CADA sugli appalti tecnologici riguarda i documenti di gara, che dovranno contenere clausole specifiche volte a garantire la restituzione dei dati in formato aperto, l'obbligo di assistenza da parte del fornitore nell'attività di migrazione, la disponibilità del codice o delle configurazioni necessarie per il trasferimento dei dati, la disciplina dei costi di uscita, ma soprattutto l'indicazione dell'obbligo per il fornitore di garantire la continuità del servizio in caso di migrazione.
Un terzo profilo riguarda i criteri di aggiudicazione, dal momento che, sulla base dell'art. 32 della proposta di regolamento le stazioni appaltanti devono attribuire peso al "valore aggiunto europeo" ai fini della valutazione qualitativa delle offerte relative a servizi *cloud* e IA. Tale valore aggiunto può consistere nel contributo dell'offerta al rafforzamento della catena di fornitura digitale dell'UE, nell'integrazione di tecnologie europee, nello svolgimento nell'Unione delle attività di innovazione necessarie al servizio o nell'utilizzo di *software* o di componenti *hardware* progettati o prodotti in Europa. Sul punto, il Considerando 67 del CADA precisa che il criterio del valore aggiunto europeo deve restare proporzionato e subordinato alla centralità della qualità tecnica e del prezzo, per cui l'obiettivo di tale previsione non sembrerebbe essere quello di escludere aprioristicamente fornitori non europei, ma di consentire alle amministrazioni di considerare, in modo trasparente e controllabile, gli effetti delle proprie scelte sulla resilienza della filiera tecnologica europea.
Un'altra conseguenza di rilievo è la valorizzazione degli "acquisti comuni" da parte della Commissione europea, la quale può svolgere procedure di appalto per l'acquisto di servizi di centro dati, servizi di *cloud computing*, *software* e sistemi di IA per sé stessa e per soggetti dell'Unione e amministrazioni aggiudicatrici degli Stati membri, di più amministrazioni, al fine di ottenere condizioni più favorevoli, sfruttando il potere contrattuale derivante della domanda aggregata, anche tramite l'ausilio della *EuroCloud Federation*.
Quest'ultima viene istituita dall'art. 34 del CADA e rappresenta la Federazione europea del *cloud* nel settore pubblico, volta alla condivisione tra enti pubblici di servizi *cloud* e di *data center* sicuri, affidabili e resilienti, così da realizzare una cooperazione infrastrutturale pubblica.
Da tali previsioni emerge come il concetto di sovranità digitale applicato agli appalti pubblici non possa essere ridotto alla localizzazione geografica dell'infrastruttura, per cui la presenza di un *data center* nel territorio dell'Unione non garantisce, di per sé, che l'amministrazione conservi un controllo effettivo sul servizio o che i dati non siano esposti a pericoli di sicurezza.
Da questo punto di vista, dunque, la proposta CADA rappresenta un tentativo di tradurre la sovranità in un insieme di

requisiti verificabili, perché delinea un insieme di regole applicabili agli appalti tecnologici che richiedono una valutazione articolata da parte della stazione appaltante, che tenga conto di aspetti come il controllo del *provider*, i rapporti con eventuali subfornitori, le misure di sicurezza adottate, la normativa applicabile e le condizioni di continuità e reversibilità del servizio.
La sovranità tecnologica in tale prospettiva diventa, quindi, una condizione della fiducia del cittadino nelle istituzioni e della stessa effettività dei diritti esercitati attraverso gli strumenti digitali.
Il cittadino rappresenta, infatti, il destinatario ultimo di questa architettura, poiché egli, in quanto utente di servizi pubblici digitali, risente delle scelte compiute dall'amministrazione, siccome l'eventuale perdita di disponibilità di un servizio o l'impossibilità di accedere ad un documento o ad una prestazione derivanti da un affidamento inefficiente incidono sulla sua posizione giuridica, dal momento che la tutela del consumatore-cittadino passa anche attraverso le scelte di *procurement* della pubblica amministrazione.

4. LE PROSPETTIVE DI VIGILANZA E IL POSSIBILE RUOLO DI ANAC.

L'evoluzione del quadro europeo impone di interrogarsi sul ruolo che le Autorità amministrative indipendenti possano svolgere rispetto agli affidamenti per *cloud computing*, *data center*, piattaforme digitali e sistemi di intelligenza artificiale. La complessità della materia richiede, innanzitutto, di evitare la sovrapposizione delle competenze fra *Authorities*. Infatti, certamente ambiti quali la valutazione tecnica della sicurezza informatica, l'applicazione della normativa in materia di protezione dei dati personali, l'interoperabilità dei sistemi e la regolazione della concorrenza appartengono a sfere nelle quali operano soggetti istituzionali, nazionali ed europei, a tale scopo preposti, per cui non sarebbe corretto immaginare la trasformazione di ANAC in un'autorità tecnica del *cloud* o dell'intelligenza artificiale.
Il possibile contributo di ANAC, dunque, sarebbe da ricercare nell'attività di vigilanza, regolazione, e supporto alle stazioni appaltanti.
La digitalizzazione del ciclo di vita dei contratti pubblici e la centralità della Banca dati nazionale dei contratti pubblici (BDNCP) mostrano come la funzione dell'Autorità sia già strettamente collegata alle infrastrutture digitali che consentono la gestione delle gare e il controllo sulla fase esecutiva dell'appalto.
Alla luce del CADA, quindi, potrebbe essere opportuno sviluppare una vigilanza collaborativa specificamente rivolta agli affidamenti tecnologici ad alta criticità. In siffatte ipotesi non si tratterebbe di attribuire ad ANAC il compito di stabilire quale soluzione tecnologica sia tecnicamente migliore, né di sostituire le valutazioni delle autorità competenti in materia di cybersicurezza o dati personali, ma di verificare che l'amministrazione abbia svolto un'adeguata attività istruttoria, abbia individuato correttamente il livello di affidabilità richiesto, abbia considerato i rischi di dipendenza tecnologica e, infine, abbia tradotto tali elementi in requisiti di partecipazione alla gara chiari e proporzionati.
In questa prospettiva, ANAC potrebbe elaborare strumenti di supporto dedicati agli affidamenti per *cloud*, IA, *data center* e piattaforme pubbliche ad alta criticità. Tali strumenti potrebbero indicare gli elementi minimi che la stazione appaltante dovrebbe prendere in considerazione nella fase di programmazione e progettazione della gara. In tal modo, ad esempio, si potrebbero individuare i criteri di valutazione della criticità e il relativo livello di *assurance* richiesto, oppure indicare possibili clausole da inserire nei documenti di gara relative agli obblighi di portabilità e migrazione per il fornitore oppure clausole volte a garantire la continuità del servizio o la corretta gestione degli incidenti informatici.
L'utilità di tali indicazioni risiederebbe soprattutto nel rendere più omogenee le procedure delle amministrazioni e nel ridurre il rischio che la complessità tecnica si traduca in opacità amministrativa. Infatti, le stazioni appaltanti, specialmente quelle più piccole, possono incontrare notevoli difficoltà nella definizione dei capitolati per servizi *cloud* o sistemi di IA, per cui il ricorso a criteri guida, anche costruiti in collaborazione con le amministrazioni competenti, potrebbe favorire una maggiore consapevolezza delle scelte della stazione appaltante.
Un ulteriore ambito di intervento dell'Autorità potrebbe riguardare il monitoraggio degli appalti tecnologici, anche tramite la Banca dati nazionale dei contratti pubblici, al fine di verificare eventuali rinnovi ripetuti nei confronti dello stesso *provider* o casi di concentrazione di contratti in capo ad un numero ristretto di operatori. Un simile monitoraggio non dovrebbe trasformarsi in una limitazione automatica della libertà di scelta delle amministrazioni, ma potrebbe fungere da indicatore di rischio utile ad individuare tutte quelle ipotesi in cui la concorrenza risulti solo formale oppure l'amministrazione stia progressivamente perdendo la capacità di modificare le proprie scelte tecnologiche.
Infine, ANAC potrebbe stipulare dei Protocolli sul tema con l'AgiD, l'Agenzia per la cybersicurezza nazionale, il Garante per la protezione dei dati personali e l'Autorità garante della concorrenza e del mercato al fine di coordinare la propria attività in materia di contratti pubblici ed evitare sovrapposizioni con le altre autorità.
La possibile funzione di ANAC, quindi, dovrebbe essere letta non come una espansione indiscriminata di competenze, ma come contributo alla costruzione di un procedimento di acquisto più trasparente e consapevole. L'Autorità

potrebbe concorrere a garantire che le valutazioni di sovranità e resilienza non rimangano affidate a formule generiche, ma trovino una concreta traduzione nella documentazione di gara, nei criteri di aggiudicazione e nelle condizioni di esecuzione del contratto.

5. CONCLUSIONI.

Il *Cloud and AI Development Act* propone un mutamento significativo nel modo di intendere gli affidamenti pubblici per i servizi *cloud* e i sistemi di intelligenza artificiale. L'amministrazione che acquista tali servizi non acquisisce soltanto spazi di archiviazione o applicazioni *software*, ma sceglie l'infrastruttura attraverso la quale saranno organizzati dati, procedimenti e servizi per i cittadini. Le decisioni di acquisto dell'amministrazione, in tali ambiti, dunque, incidono sulla stessa attività amministrativa, sulla sicurezza delle informazioni, sulla continuità dei servizi e, in generale, sulla qualità dell'azione pubblica.

Il CADA tenta di rispondere a queste esigenze introducendo un quadro europeo di *assurance* per il *cloud computing* basato su livelli di garanzia, riconoscimento del *provider* e valutazione del rischio. Accanto a tali strumenti, la proposta di regolamento valorizza il ruolo del *procurement* come leva di politica industriale e di resilienza: le amministrazioni sono chiamate a considerare il "valore aggiunto europeo", a favorire l'innovazione, ad utilizzare gli acquisti comuni e a partecipare a forme di cooperazione infrastrutturale pubblica come la *EuroCloud Federation*.

La sovranità digitale, però, non deve essere interpretata come una deroga ai principi della concorrenza o come criterio volto ad escludere automaticamente operatori extra-UE. Essa richiede, piuttosto, di rendere visibili e valutabili gli elementi che spesso rimangono sullo sfondo degli affidamenti tecnologici: chi controlla il servizio, come sono gestiti i dati, quale sia il grado di indipendenza del *provider*, se l'amministrazione possa effettivamente migrare verso soluzioni alternative e quali garanzie esistano per la continuità del servizio.

In tale scenario, i contratti pubblici possono diventare uno strumento di costruzione di fiducia digitale, per cui la trasparenza, l'interoperabilità, la portabilità e la continuità operativa non costituiscono più aspetti marginali della progettazione tecnica, ma elementi essenziali per garantire che la tecnologia resti al servizio dell'amministrazione e della collettività.

La riflessione investe anche il ruolo delle autorità di vigilanza. Senza sovrapporsi alle competenze tecniche e regolatorie di altri soggetti, ANAC potrebbe contribuire a rendere la sovranità tecnologica un parametro verificabile nell'ambito degli appalti pubblici. Dalle infrastrutture "materiali" alle infrastrutture "immateriali", la vigilanza sugli appalti è chiamata a confrontarsi con una nuova dimensione dell'interesse pubblico: quella delle architetture digitali che, pur rimanendo spesso invisibili al cittadino, condizionano ormai in modo decisivo l'esercizio dei diritti e l'affidabilità dei servizi pubblici.

La sfida dei prossimi anni, dunque, sarà quella di trasformare la sovranità digitale da principio generale a pratica amministrativa. Ciò richiederà norme adeguate, competenze tecniche, cooperazione tra istituzioni e capacità di utilizzare il *procurement* non soltanto per acquistare tecnologia, ma per costruire un ecosistema digitale europeo più aperto, sicuro, interoperabile e meritevole della fiducia dei cittadini.

AUTORITà PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM)

COMUNICAZIONI ELETTRONICHE, MEDIA E AUDIOVISIVO NEL 2030: CONSUMATORI SEMPRE PIÙ CONNESSI, PERSONALIZZATI E VULNERABILI

(di Francesca Pellicanò e Rosaria Petti) [1]

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.

SOMMARIO: 1. Premessa (Rosaria Petti). 2. Dalla scarsità dei contenuti alla scarsità dell'attenzione (Francesca Pellicanò) 3. I principali profili di attenzione per i consumatori nel 2030 (Francesca Pellicanò); 4. Aspetti strategici (Francesca Pellicanò); Conclusioni: dal consumatore spettatore al consumatore "algoritmicamente mediato" (Francesca Pellicanò); .6. La tutela del consumatore nelle comunicazioni elettroniche (Rosaria Petti); 7. Le prospettive per AGCOM nel periodo 2026–2030 nel settore delle comunicazioni elettroniche (Rosaria Petti); 8. Quali conclusioni per le comunicazioni elettroniche? (Rosaria Petti)

1. Premessa (Rosaria Petti)

La progressiva trasformazione digitale dell'economia e della società sta producendo un mutamento strutturale nella posizione del consumatore nei mercati delle comunicazioni. La diffusione dell'intelligenza artificiale, la crescente centralità delle piattaforme digitali, l'evoluzione delle reti di comunicazione elettronica, la trasformazione dei modelli di fruizione dei contenuti audiovisivi, la personalizzazione algoritmica della pubblicità e dell'informazione stanno modificando non soltanto le modalità attraverso le quali gli utenti accedono ai servizi, ma anche le condizioni nelle quali maturano le proprie decisioni.

Nel prossimo triennio-quadriennio la tutela del consumatore sarà pertanto chiamata a confrontarsi con forme di asimmetria che non riguardano più esclusivamente le informazioni disponibili o le condizioni contrattuali, ma investono la stessa architettura degli ambienti digitali nei quali le scelte vengono compiute. Il consumatore è sempre più inserito in ecosistemi nei quali algoritmi, sistemi di raccomandazione, interfacce, meccanismi di profilazione e modelli di personalizzazione contribuiscono a determinare ciò che egli vede, acquista, sottoscrive e utilizza.

Il presente contributo intende analizzare le principali urgenze, tendenze ed esigenze suscettibili di incidere sulla posizione del consumatore nei settori riconducibili alle competenze dell'Autorità per le garanzie nelle comunicazioni (AGCOM), con particolare attenzione alle comunicazioni elettroniche, ai media audiovisivi e radiofonici, alle piattaforme online. Particolare rilievo viene attribuito all'intelligenza artificiale, alla personalizzazione algoritmica, alla contendibilità dei mercati, alla qualità della connettività, alla tutela dei minori alla trasformazione dei modelli di consumo audiovisivo e informativo, alla pubblicità digitale e alle nuove forme di vulnerabilità.

L'ipotesi sostenuta è che il paradigma tradizionale del "consumatore informato" debba progressivamente evolvere verso quello di un consumatore dotato di effettiva capacità di scelta, controllo e reversibilità delle proprie decisioni. La tutela regolatoria non può quindi limitarsi alla correttezza dell'informazione fornita *ex ante*, ma deve interrogarsi sulle condizioni tecnologiche, economiche e cognitive che determinano la formazione della scelta.

1. Le opinioni espresse da entrambe le autrici sono personali e non impegnano in alcun modo l'Autorità per le garanzie nelle comunicazioni.

2. Alla scarsità dei contenuti alla scarsità dell'attenzione *(Francesca Pellicanò)*

Immaginare come sarà il settore dei media e dell'audiovisivo nel 2030 significa, prima di tutto, prendere atto che la distinzione tradizionale tra televisione, piattaforme digitali, *social network*, servizi audiovisivi *on demand* e informazione *online*, al giorno d'oggi già labile, sarà sempre più sfumata. Il principale cambiamento dei prossimi anni non sarà infatti semplicemente tecnologico, ma strutturale: il consumo audiovisivo si sposterà definitivamente dalla logica del "palinsesto" alla logica dell'accesso permanente, personalizzato e intermediato dagli algoritmi.

Il consumatore del 2030 non sarà necessariamente un telespettatore, un abbonato a una piattaforma o un utente di un *social network*. Sarà, sempre più, un destinatario di contenuti audiovisivi che attraversano ecosistemi diversi, spesso senza che sia percepibile con chiarezza chi produca il contenuto, chi lo distribuisca, chi ne determini la visibilità e sulla base di quali criteri.

La trasformazione è già in atto: i dati più recenti dell'AGCOM [2] mostrano che, nel 2025, i principali servizi di video *on demand* a pagamento hanno raggiunto in Italia 15,8 milioni di utenti unici nel mese di dicembre, mentre, nello stesso mese, il tempo complessivamente trascorso sui principali siti di *video streaming* a pagamento ha raggiunto quasi 46 milioni di ore e, parallelamente, i servizi VOD gratuiti hanno raggiunto oltre 35 milioni di utenti unici. Questo processo non implica necessariamente la scomparsa della televisione tradizionale, ma, piuttosto, la sua trasformazione in una componente di un ecosistema più ampio, nel quale televisione lineare, *catch-up TV*, *streaming*, *social video*, piattaforme di condivisione e contenuti generati dagli utenti convivono e si alimentano reciprocamente.

La Direttiva SMAV [3] aveva già colto questa evoluzione, includendo nel proprio ambito i servizi di media audiovisivi, i servizi on demand, le comunicazioni commerciali e le piattaforme per la condivisione di video, proprio alla luce della convergenza tra comunicazioni elettroniche, editoria e Internet. Da qui al 2030, tuttavia, la convergenza sarà ancora più radicale.

Per decenni il problema principale della regolazione dei media è stato quello della scarsità: pochi canali, poche frequenze, pochi operatori e un'offerta necessariamente limitata. La società digitale ha ribaltato completamente questa impostazione, rendendo prevedibile che il problema del consumatore del 2030 sarà, al contrario, l'eccesso di contenuti. Infatti, l'offerta audiovisiva sarà potenzialmente illimitata, ma la capacità individuale di selezionare, comprendere e valutare i contenuti resterà ridotta. Di conseguenza, la risorsa scarsa non sarà più il contenuto, bensì l'attenzione dell'utente. In questo scenario assumeranno un ruolo decisivo gli algoritmi di raccomandazione: non sarà sufficiente che un contenuto sia disponibile, ma, piuttosto, sarà necessario che venga mostrato, suggerito, indicizzato e reso visibile. La scelta del consumatore dipenderà quindi, sempre più, da sistemi tecnologici che egli non controlla e spesso non comprende. Il Digital Services Act [4] ha già riconosciuto questa trasformazione, imponendo alle piattaforme obblighi di trasparenza sui principali parametri dei sistemi di raccomandazione e prevedendo, in determinati casi, la possibilità per gli utenti di modificare o influenzare tali parametri. Da qui al 2030 questa dimensione diventerà probabilmente uno dei principali terreni della tutela del consumatore audiovisivo.

La seconda grande trasformazione sarà determinata dall'intelligenza artificiale come infrastruttura dei media. L'AI non sarà soltanto uno strumento utilizzato per produrre film, serie, programmi o contenuti digitali, ma è legittimo ritenere che entrerà nell'intero ciclo di vita del prodotto audiovisivo: ideazione, scrittura, traduzione, doppiaggio, montaggio, generazione di immagini e voci, personalizzazione, raccomandazione, moderazione e distribuzione. Il confine tra contenuto autentico e contenuto sintetico diventerà progressivamente più difficile da percepire. La questione non riguarda soltanto i cosiddetti *deepfake*: il problema più ampio sarà quello della fiducia nel contenuto audiovisivo. Se immagini, voci e video potranno essere generati o manipolati con costi sempre più bassi, il consumatore dovrà poter comprendere se ciò che sta guardando è reale, modificato, ricostruito artificialmente o integralmente generato. L'AGCOM ha già individuato nell'intelligenza artificiale [5] una delle principali sfide future per i settori regolati, analizzandone le implicazioni per disinformazione, *deepfake*, diritto d'autore, educazione digitale, protezione dei minori e rapporto tra tecnica e diritto. Nel 2030, pertanto, la trasparenza sull'origine e sulle modalità di produzione dei contenuti potrebbe diventare una componente ordinaria della tutela dell'utente.

Un'altra tendenza destinata a consolidarsi sarà la crescente concentrazione dell'intermediazione, che porterà a un

2. Riportati nell'Osservatorio delle comunicazioni n. 1/2026, disponibile al link https://www.agcom.it/sites/default/files/documenti/osservatorio/AGCOM_Osservatorio%20n.1-2026_1.pdf (consultato in agosto 2026).
3. Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato
4. Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) https://eur-lex.europa.eu/IT/legal-content/summary/digital-services-act.html
5. Nel Rapporto sull'intelligenza artificiale 2026, disponibile al link https://www.agcom.it/comunicazione/avvisi/rapporto-intelligenza-artificiale-2026 (consultato nel luglio 2026).

mercato sempre più multipiattaforma. Infatti, il consumatore potrà avere accesso a un numero enorme di contenuti, ma attraverso un numero relativamente ristretto di grandi piattaforme tecnologiche e distributive. L'AGCOM rileva [6] già una presenza molto significativa dei grandi operatori internazionali nell'ecosistema digitale italiano, riportando che, nel dicembre 2025, quasi 44 milioni di utenti unici hanno navigato online e le principali piattaforme social hanno raggiunto decine di milioni di utenti.
La questione concorrenziale, dunque, non potrà essere separata da quella consumeristica. Per il consumatore, infatti, la concorrenza non consiste soltanto nel poter scegliere tra diversi fornitori, ma anche nella possibilità di accedere a contenuti diversi, confrontare offerte, cambiare piattaforma senza costi eccessivi, conservare le proprie preferenze e non essere catturato da un singolo ecosistema digitale.
Il consumatore del 2030 sarà quindi più libero nella scelta dei contenuti, ma potrebbe essere meno libero nella scelta dell'infrastruttura attraverso cui quei contenuti gli vengono offerti.

3. I principali profili di attenzione per i consumatori nel 2030 *(Francesca Pellicanò)*

Se questa è la traiettoria del settore, le questioni consumeristiche del prossimo quadriennio possono essere ricondotte ad almeno sei grandi aree.

3.0.1. La trasparenza dell'algoritmo e la libertà di scelta

La prima questione sarà quella della scelta effettiva. In un ambiente in cui l'offerta ammonta a migliaia di titoli, l'utente non sceglie realmente tra tutti i contenuti disponibili: sceglie tra quelli che la piattaforma decide di mostrargli. La personalizzazione può migliorare l'esperienza dell'utente, ma può anche creare forme di opacità e dipendenza: il rischio è che la personalizzazione si trasformi in una progressiva restrizione della *findability* dei contenuti e, pertanto, dell'orizzonte informativo e culturale.
La domanda "regolatoria" del futuro sarà quindi: quanto è realmente libero un consumatore che riceve un'offerta fortemente preselezionata da un algoritmo? Il problema assume una particolare rilevanza nell'informazione. Se il sistema di raccomandazione determina quali notizie, quali video e quali opinioni raggiungono l'utente, l'algoritmo diventa, anche se indirettamente, un soggetto capace di incidere sul pluralismo.
Il Regolamento EMFA sulla libertà dei media [7] ha significativamente rafforzato questa prospettiva, riconoscendo il diritto dei destinatari dei servizi di media ad accedere a una pluralità di contenuti editorialmente indipendenti e ponendo al centro del nuovo quadro europeo l'indipendenza e il pluralismo dei media.
Da qui al 2030 sarà pertanto necessario sviluppare una nozione di trasparenza algoritmica orientata al consumatore, non necessariamente fondata sulla divulgazione tecnica del codice, ma sulla comprensibilità dei criteri che determinano ciò che viene mostrato e ciò che rimane invisibile.

3.0.2. Il consumatore minore e la protezione dai rischi digitali

Il secondo profilo riguarda i minori: bambini e adolescenti sono già e saranno sempre più tra i principali consumatori di contenuti audiovisivi digitali. La protezione non potrà tuttavia essere limitata alla tradizionale classificazione dei programmi per fasce d'età. I rischi saranno più articolati: contenuti inappropriati, pubblicità comportamentale, *influencer marketing*, dipendenza dall'utilizzo, sistemi di raccomandazione, contenuti violenti o sessualmente espliciti, disinformazione e raccolta di dati.
Il Digital Services Act già prevede specifici obblighi per le piattaforme accessibili ai minori, imponendo misure appropriate e proporzionate per garantire un elevato livello di *privacy*, sicurezza e protezione e vietando, in determinate condizioni, la pubblicità basata sul *profiling* dei minori.
In Italia, inoltre, l'AGCOM ha avviato un percorso particolarmente significativo sulla verifica dell'età per l'accesso a contenuti pornografici. Nel 2025 sono state definite modalità tecniche tese a evitare che il sito o la piattaforma ricevano direttamente informazioni personali e sensibili dell'utente, attraverso un modello di verifica affidato a un soggetto terzo indipendente [8].
Questa esperienza offre un'indicazione importante per il futuro: la protezione del minore non può tradursi automati-

6. Nel già citato Osservatorio sulle comunicazioni 1/2026.
7. Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (Regolamento europeo sulla libertà dei media)https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L_202401083
8. Delibera n. 96/25/CONS "Modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai fini dell'accesso a determinati servizi forniti dai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, ai sensi dell'articolo 13-bis del decreto-legge 5 settembre 2023, n. 123 convertito con modificazioni dalla legge 13 novembre 2023, n. 159".

camente in una nuova raccolta generalizzata di dati personali. La sfida del 2030 sarà, quindi, quella di costruire sistemi di *age assurance* realmente efficaci, ma, al contempo, rispettosi della *privacy*, proporzionati e interoperabili.

3.0.3. Pubblicità, influencer e nuove forme di persuasione

Un terzo argomento sarà rappresentato dalla trasformazione della comunicazione commerciale. La distinzione tra contenuto editoriale e pubblicità sarà sempre meno evidente. *Product placement, branded content, influencer marketing*, pubblicità personalizzata, contenuti sponsorizzati e commercio integrato nelle piattaforme tenderanno a fondersi.
Il consumatore potrebbe quindi non essere sempre in grado di comprendere quando sta ricevendo un'informazione, quando sta assistendo a un contenuto di intrattenimento e quando sta subendo una sollecitazione commerciale.
L'intervento dell'AGCOM sugli *influencer è già particolarmente indicativo. Nel 2025 l'Autorità ha modificato le Linee guida già adottate nel 2024 e ha approvato un Codice di condotta per gli influencer*, con l'obiettivo di rafforzare trasparenza, riconoscibilità delle comunicazioni commerciali, tutela dei minori e protezione degli utenti [9]. Questa evoluzione si basa su una regola di fondo: la pubblicità deve essere riconoscibile anche quando assume la forma del contenuto.
Il problema sarà particolarmente complesso con l'intelligenza artificiale, che consentirà di costruire pubblicità iper-personalizzate, modificare immagini e voci e creare testimonial sintetici.
Il consumatore del 2030 dovrà quindi essere messo nella condizione di comprendere non soltanto "che cosa" gli viene comunicato, ma anche "perché" quel contenuto viene mostrato proprio a lui.

3.0.4. Il prezzo dell'accesso e la nuova economia degli abbonamenti

Un quarto tema sarà quello economico. La moltiplicazione delle piattaforme ha prodotto una moltiplicazione degli abbonamenti. Il consumatore può oggi sottoscrivere servizi audiovisivi differenti per cinema, serie televisive, sport, musica, informazione e altri contenuti, sempre più parcellizzati o tematici.
La libertà di scelta può quindi produrre un nuovo problema: la frammentazione dell'offerta.
Da qui al 2030 sarà necessario interrogarsi sulle modalità di acquisizione e cessazione degli abbonamenti, sulla trasparenza dei prezzi, sui rinnovi automatici, sulle modifiche delle condizioni economiche, sui pacchetti pubblicitari e sulle modalità di cancellazione.
Una particolare attenzione dovrà essere rivolta alle cosiddette pratiche di "dark pattern", attraverso le quali l'interfaccia può rendere semplice sottoscrivere un servizio e difficile interromperlo.
La tutela del consumatore audiovisivo dovrà pertanto evolvere da una concezione prevalentemente informativa a una concezione di *fairness by design*: l'architettura stessa del servizio dovrebbe essere costruita in modo da non ostacolare artificialmente le decisioni dell'utente.

3.0.5. Pluralismo, qualità dell'informazione e disinformazione

La quinta questione è probabilmente la più delicata. La regolazione dei media non può essere considerata soltanto una materia economica o consumeristica, stante l'imprescindibile funzione democratica assolta dai medesimi. Il consumatore è, infatti, anche cittadino e la qualità dell'informazione cui accede può influenzare le sue decisioni politiche, economiche e sociali.
Nel 2030 il problema della disinformazione sarà aggravato dalla capacità dell'intelligenza artificiale generativa di produrre rapidamente grandi quantità di contenuti apparentemente credibili.
Il rischio non sarà soltanto quello di incontrare una notizia falsa, ma, piuttosto, di entrare in un ambiente informativo nel quale diventa progressivamente impossibile distinguere il vero dal falso.
In questo contesto, il pluralismo non potrà essere misurato soltanto contando il numero di operatori presenti sul mercato. Sarà necessario considerare anche la pluralità effettivamente accessibile all'utente.
Il nuovo European Media Freedom Act muove proprio nella direzione di collegare il funzionamento del mercato dei media alla tutela dell'indipendenza editoriale e del pluralismo.
La tutela del consumatore del 2030 dovrà quindi comprendere anche un diritto a un ambiente informativo sufficientemente trasparente, diversificato e affidabile.

3.0.6. Accessibilità e inclusione

Infine, non va trascurata la dimensione dell'accessibilità.
La progressiva digitalizzazione dell'audiovisivo può creare nuove opportunità per le persone con disabilità, grazie a

9. Delibera n. 197/25/CONS "Modifiche alle linee guida di cui alla delibera n. 7/24/CONS e approvazione del codice di condotta rivolto agli influencer"

sottotitoli, audiodescrizioni, traduzione automatica, sintesi vocale e strumenti di personalizzazione. Inoltre, l'intelligenza artificiale potrà ridurre significativamente i costi di tali servizi.
Il rischio, tuttavia, è che il processo di innovazione si sviluppi in maniera disomogenea, affidandosi prevalentemente all'iniziativa dei singoli operatori, col rischio di tradursi, per alcuni casi, in interventi marginali e scarsamente incisivi, comportando che l'accessibilità rimanga una caratteristica opzionale anziché una componente strutturale del servizio.
Entro il 2030 sarà quindi opportuno considerare l'accessibilità non come un obbligo meramente tecnico, ma come una componente della qualità del servizio audiovisivo.

4. Aspetti strategici (Francesca Pellicanò)

La prospettiva del 2030 richiede di anticipare i problemi, evitando che la regolazione intervenga soltanto quando le nuove tecnologie sono già diventate infrastrutture consolidate, così come le problematiche ad esse correlate, anticipate nel precedente paragrafo.
La prima esigenza è quindi quella di passare da una regolazione prevalentemente reattiva a una regolazione maggiormente prospettica, trasversale e tecnologicamente neutrale. Le norme dovrebbero essere valutate non soltanto in relazione al comportamento del singolo operatore, ma considerando l'intera esperienza dell'utente: scoperta del servizio, registrazione, scelta dell'abbonamento, fruizione, personalizzazione, pubblicità, trattamento dei dati, modifica delle condizioni, reclamo e cessazione.
In altre parole, il consumatore dovrebbe essere seguito lungo l'intero ciclo di vita della relazione digitale.
Ciò induce ad affermare che i problemi del consumatore audiovisivo del 2030 non rientreranno più facilmente nei confini di una singola competenza. Un unico servizio potrà coinvolgere contemporaneamente profili di regolazione dei media, tutela dei consumatori, concorrenza, protezione dei dati personali, intelligenza artificiale, tutela dei minori, *copyright* e sicurezza digitale. La crescente intersezione tra queste materie rende necessario rafforzare il coordinamento tra autorità competenti, con l'obiettivo non di creare nuovi livelli burocratici, ma evitare che la frammentazione delle competenze abbia, come risultato, una frammentazione della tutela.
Un terzo fronte è quello delle competenze tecniche: per poter vigilare efficacemente sui sistemi di raccomandazione, sulla moderazione automatizzata, sui contenuti generati dall'AI e sulla pubblicità algoritmica, le Autorità dovranno disporre di competenze tecnologiche e strumenti adeguati, in quanto sarà sempre meno sufficiente verificare il contenuto finale di un programma e, piuttosto, occorrerà comprendere anche il sistema che ne determina la distribuzione. Ciò significa sviluppare capacità di *algorithmic auditing*, analisi dei dati, monitoraggio delle piattaforme e valutazione dei rischi sistemici.
In questa prospettiva, il ruolo dell'AGCOM come Digital Services Coordinator assume particolare rilievo, anche in relazione all'attuazione del Digital Services Act.
Inoltre, la trasparenza – non meramente formale – dovrà diventare uno dei principi cardine della regolazione al 2030. Informare il consumatore attraverso condizioni generali di decine di pagine o informative tecniche incomprensibili non equivale necessariamente a garantire una scelta consapevole.
Occorrerà sviluppare una trasparenza comprensibile e contestuale, attraverso informazioni brevi, chiaramente comprensibili e fornite nel momento in cui l'utente compie una scelta, che questa sia la sottoscrizione di un abbonamento, la pubblicità, i sistemi di raccomandazione, l'uso dell'intelligenza artificiale e la gestione dei dati.
Infine, la regolazione non potrà, da sola, risolvere tutti i problemi. Il consumatore del 2030 dovrà possedere nuove competenze: comprendere come funzionano gli algoritmi, riconoscere una comunicazione commerciale, individuare un contenuto sintetico, comprendere i meccanismi di personalizzazione e riconoscere le principali tecniche di manipolazione digitale.
L'educazione ai media (c.d. *media and digital literacy)*dovrà quindi assumere un ruolo centrale nelle politiche pubbliche. Non si tratta soltanto di insegnare a utilizzare le tecnologie: occorre insegnare a interpretarle criticamente.
Infine, occorrerà mantenere alta l'attenzione sul pluralismo e sulla diversità culturale.
La crescita delle piattaforme globali presenta indubbi vantaggi per il consumatore, ma può generare anche una progressiva omogeneizzazione dell'offerta. Uno spunto utile può provenire, ad esempio, dalle regole sulle opere europee e sui produttori indipendenti: nel 2025 l'AGCOM ha aggiornato il relativo regolamento[10], adeguandolo alle modifiche normative intervenute nel Testo unico. Il tema, tuttavia, dovrà essere ripensato in prospettiva 2030, non limitandosi a focalizzarsi solo sulla quantità di opere disponibili, ma anche visibilità effettiva, reperibilità e accessibilità dei contenuti europei e italiani. La questione della "*prominence*" diventerà pertanto sempre più importante. In un catalogo di

10. Delibera n. 70/25/CONS di modifica della delibera n. 424/22/CONS.

migliaia di titoli, infatti, essere formalmente presenti non significa necessariamente essere realmente visibili e accessibili al consumatore.

5. Conclusioni: dal consumatore spettatore al consumatore "algoritmicamente mediato" *(Francesca Pellicanò)*

Il settore dei media e dell'audiovisivo si avvia verso il 2030 caratterizzato da una contraddizione fondamentale. Da un lato, il consumatore avrà a disposizione una quantità di contenuti, servizi e possibilità di scelta mai sperimentata prima; dall'altro, proprio questa abbondanza renderà il consumatore sempre più dipendente dai sistemi tecnologici che selezionano, ordinano, raccomandano e monetizzano i contenuti.

Il problema centrale della regolazione futura non sarà quindi soltanto garantire che il consumatore possa scegliere, ma assicurarsi che egli possa scegliere in modo effettivamente libero, informato e consapevole.

Questo comporta un cambio di prospettiva: nel modello tradizionale la tutela dei consumatori audiovisivi si è concentrata soprattutto su contenuti illeciti o inappropriati, pubblicità, tutela dei minori, trasparenza contrattuale, qualità del servizio e accesso alle procedure di reclamo.

Nel modello del 2030 questi profili resteranno fondamentali, ma se ne aggiungeranno altri: trasparenza algoritmica, personalizzazione, AI generativa, deepfake, sistemi di raccomandazione, profilazione, influencer marketing, pluralismo digitale, interoperabilità, accessibilità e dipendenza dalle piattaforme.

La vera sfida sarà quindi quella di trasformare la tutela del consumatore da una tutela del contenuto a una tutela dell'ecosistema nel quale il contenuto viene prodotto, selezionato, distribuito e monetizzato.

È una trasformazione già inscritta nell'evoluzione normativa europea. La Direttiva SMAV ha esteso la prospettiva regolatoria oltre la televisione tradizionale, includendo servizi on demand e piattaforme di condivisione video; il Digital Services Act ha introdotto obblighi specifici per le piattaforme in materia di sistemi di raccomandazione, pubblicità e tutela dei minori; l'European Media Freedom Act ha posto il pluralismo e l'indipendenza editoriale al centro del nuovo quadro europeo: da qui al 2030 occorrerà dunque lavorare soprattutto su tre direttrici.

In primo luogo, rendere comprensibili le nuove forme di intermediazione. Il consumatore deve poter sapere perché vede un determinato contenuto, perché gli viene proposta una determinata pubblicità e quali elementi influenzano la sua esperienza audiovisiva.

In secondo luogo, proteggere i soggetti più vulnerabili. Minori, persone con ridotte competenze digitali e soggetti esposti a forme di manipolazione informativa dovranno essere destinatari di una tutela rafforzata, senza trasformare la protezione in una giustificazione per una raccolta indiscriminata di dati.

Infine, terzo ma non ultimo: preservare la possibilità di una scelta autentica. La concorrenza tra piattaforme, il pluralismo dei contenuti, la diversità culturale, l'accessibilità e la possibilità di cambiare servizio devono diventare elementi della stessa politica di tutela del consumatore.

Il consumatore del 2030 sarà, in definitiva, al contempo più potente e più fragile di quello di oggi. Più potente perché potrà accedere a un'offerta globale, personalizzata e praticamente illimitata; più fragile perché una parte crescente delle sue decisioni sarà mediata da sistemi che operano al di là della sua immediata comprensione.

La regolazione dei media e dell'audiovisivo dovrà quindi affrontare una sfida nuova: fare in modo che la personalizzazione non diventi manipolazione, che l'abbondanza non diventi opacità, che l'intelligenza artificiale non comprometta la fiducia e che la comodità delle piattaforme non si trasformi in dipendenza.

Se questo obiettivo sarà perseguito con sufficiente anticipo, il 2030 potrà rappresentare non soltanto il punto di arrivo della trasformazione digitale dei media, ma l'occasione per costruire un ecosistema audiovisivo nel quale innovazione e tutela dei consumatori procedano nella stessa direzione.

6. La tutela del consumatore nelle comunicazioni elettroniche *(Rosaria Petti)*

La trasformazione digitale, come ampiamente evidenziato, sta modificando in profondità la posizione del consumatore nei mercati delle comunicazioni. Tale cambiamento non coincide semplicemente con l'introduzione di nuove tecnologie o con la progressiva sostituzione dei canali tradizionali con quelli digitali. Esso investe, più radicalmente, le modalità attraverso le quali si formano la domanda, le preferenze e le decisioni individuali.

Per lungo tempo, la disciplina della tutela degli utenti e dei consumatori nei mercati delle comunicazioni si è fondata, in larga misura, sulla necessità di ridurre le asimmetrie informative tra operatori e utenti. Trasparenza delle condizioni contrattuali, chiarezza delle informazioni economiche, qualità dei servizi, possibilità di recesso e di cambiamento del fornitore hanno rappresentato alcuni degli strumenti attraverso i quali rendere effettiva la libertà di scelta del consumatore. Tale impostazione conserva tuttora la propria rilevanza, ma appare progressivamente insufficiente a descrivere

la complessità dell'ecosistema digitale contemporaneo.
La ragione è riconducibile al fatto che, nei mercati digitali, la scelta del consumatore non è più necessariamente il risultato di un processo nel quale egli individua autonomamente le alternative disponibili, le confronta e seleziona quella ritenuta più conveniente. Sempre più spesso, infatti, è l'ambiente digitale a determinare quali alternative siano visibili, in quale ordine vengano presentate, quali contenuti siano raccomandati, quali offerte siano pubblicizzate e quali informazioni ricevano maggiore attenzione. La decisione individuale si forma pertanto all'interno di un ambiente tecnologicamente mediato, nel quale algoritmi, sistemi di raccomandazione, interfacce, meccanismi di profilazione e tecniche di personalizzazione assumono un ruolo crescente.
Questa evoluzione presenta una particolare rilevanza per AGCOM. L'ambito di intervento dell'Autorità comprende infatti settori che costituiscono infrastrutture essenziali dell'esperienza digitale contemporanea: le comunicazioni elettroniche, i servizi media audiovisivi e radiofonici, le piattaforme online, l'informazione, la pubblicità e i servizi postali. La progressiva convergenza tra questi mercati rende inoltre sempre più difficile analizzarli separatamente. Il medesimo consumatore può essere, nel corso della stessa esperienza digitale, utente di una rete di comunicazione, abbonato a una piattaforma audiovisiva, destinatario di pubblicità personalizzata, fruitore di informazione, utilizzatore di un sistema di intelligenza artificiale e acquirente di beni attraverso un ambiente digitale.
Il periodo 2026–2030 appare, sotto questo profilo, particolarmente significativo. Le nuove discipline europee sull'intelligenza artificiale e sui servizi digitali entrano in una fase di progressiva attuazione e consolidamento, mentre la diffusione delle reti ad altissima capacità, la crescita dei servizi audiovisivi on demand e la trasformazione dei modelli di distribuzione dell'informazione stanno modificando rapidamente le abitudini degli utenti. La stessa nozione di servizio essenziale tende, inoltre, a trasformarsi: la connettività e l'accesso ai contenuti digitali sono divenuti condizioni sempre più rilevanti per la partecipazione economica e sociale, mentre nel settore postale la progressiva riduzione della corrispondenza tradizionale convive con la crescente centralità della logistica e dell'e-commerce.
In questo scenario, la questione fondamentale non consiste più soltanto nel chiedersi se il consumatore disponga delle informazioni necessarie per scegliere, ma se disponga delle condizioni effettive per esercitare una scelta autonoma. È questo, probabilmente, il principale interrogativo che accompagnerà l'evoluzione della tutela nei prossimi anni.
Tra i settori destinati a incidere maggiormente sulla posizione del consumatore nel prossimo quadriennio, quello delle comunicazioni elettroniche occupa una posizione peculiare. La ragione non risiede soltanto nella rilevanza economica dei servizi di telefonia e connettività, ma nel loro carattere sempre più infrastrutturale rispetto alla partecipazione degli individui alla vita economica e sociale.
La connessione alla rete non costituisce più, infatti, un servizio destinato prevalentemente alla comunicazione interpersonale o all'intrattenimento. Essa rappresenta una condizione abilitante per l'accesso all'informazione, all'istruzione, al lavoro, ai servizi pubblici, all'e-commerce, alla sanità digitale e, più in generale, alla cittadinanza digitale.
I dati più recenti di AGCOM mostrano chiaramente questa trasformazione infrastrutturale. A dicembre 2025 gli accessi alla rete fissa erano pari a circa 20,53 milioni; le linee FTTH avevano raggiunto il 34,1% degli accessi complessivi, con una crescita di circa 1,15 milioni di linee su base annua. Nello stesso periodo, l'83,9% delle linee risultava commercializzato con velocità pari o superiore a 100 Mbit/s, mentre le linee con capacità almeno pari a 1 Gbit/s rappresentavano il 35,9%. Parallelamente, il traffico dati medio giornaliero per linea broadband era salito a 10,34 GB, contro i 6,88 GB del 2021.
Questi dati non descrivono soltanto l'evoluzione tecnologica delle reti. Mostrano il progressivo aumento della dipendenza degli utenti dalla connettività e, conseguentemente, l'aumento del valore economico e sociale della sua qualità.

6.0.1. Dalla disponibilità della rete alla qualità dell'esperienza digitale (Rosaria Petti)

Una delle principali trasformazioni attese nel periodo 2026–2030 riguarda il passaggio dalla logica della copertura a quella della qualità effettiva dell'esperienza di connessione.
La diffusione della fibra e delle reti mobili di nuova generazione ha progressivamente elevato le aspettative degli utenti. Velocità di picco, ampiezza della copertura e disponibilità nominale del servizio costituiscono tuttavia soltanto una parte dell'esperienza percepita. Per il consumatore diventano sempre più rilevanti la stabilità della connessione, la latenza, la continuità del servizio, la congestione, la qualità della connessione indoor, la capacità della rete di sostenere contemporaneamente molteplici dispositivi e la rapidità con cui vengono risolti eventuali malfunzionamenti.
Il concetto di qualità del servizio è quindi destinato a diventare più complesso. Una connessione pubblicizzata come "ultraveloce" può produrre esperienze profondamente differenti a seconda del luogo, dell'orario, del dispositivo utilizzato e del tipo di applicazione. La distanza tra prestazione teorica e prestazione effettivamente sperimentata dal consumatore può pertanto diventare una delle principali fonti di asimmetria informativa.

AGCOM ha già progressivamente orientato la disciplina verso una rappresentazione più articolata della qualità. La revisione degli indicatori per i servizi da postazione fissa ha previsto, tra l'altro, la pubblicazione di informazioni relative alle velocità minima, massima e normalmente disponibile, rendendo tali informazioni parte integrante della trasparenza dell'offerta e, in determinate condizioni, della tutela contrattuale dell'utente.
Nel prossimo quadriennio sarà tuttavia necessario interrogarsi su un ulteriore passaggio: dalla qualità dichiarata alla qualità percepita.
Il consumatore non valuta una rete sulla base di un parametro tecnico isolato, ma sulla base della possibilità di svolgere efficacemente le attività che gli interessano. Una connessione è giudicata "valida" quando consente, ad esempio, di partecipare a una videoconferenza senza interruzioni, utilizzare servizi cloud, effettuare una videochiamata, fruire di contenuti audiovisivi ad alta definizione o utilizzare applicazioni interattive senza significative discontinuità.
La qualità percepita può quindi essere considerata una dimensione emergente della tutela dell'utente, destinata ad affiancare i tradizionali indicatori tecnici.
Questa prospettiva non implica l'abbandono degli indicatori oggettivi. Al contrario, richiede di collegarli maggiormente all'esperienza concreta. La sfida regolatoria consiste nel costruire un sistema nel quale la misurazione tecnica della rete possa essere tradotta in informazioni comprensibili sul servizio che il consumatore può realisticamente aspettarsi.
La qualità della connettività diventa così una questione di trasparenza sostanziale: non è sufficiente sapere quale sia la velocità massima teorica, ma occorre poter comprendere quale esperienza sia ragionevolmente associata all'offerta.
In questa prospettiva assume particolare rilevanza l'attività di misurazione sul campo. AGCOM ha proseguito anche nel 2026 l'aggiornamento degli strumenti di misurazione della qualità dei servizi mobili, prevedendo una specifica campagna di misure della qualità del servizio dati in mobilità. (AGCOM) Ciò mostra come la misurazione empirica della qualità rappresenti già un elemento importante dell'attività di tutela.
Nel prossimo futuro, tuttavia, potrebbe essere utile integrare sempre più questi strumenti con indicatori relativi all'esperienza dell'utente, ai reclami, alla frequenza dei disservizi e alla capacità di risoluzione dei problemi. La qualità potrebbe essere quindi interpretata come un fenomeno multidimensionale nel quale convergono prestazioni tecniche, continuità, assistenza e soddisfazione dell'utente.

6.0.2. La connettività come servizio essenziale (Rosaria Petti)

La crescente dipendenza dalla connettività pone inoltre una questione più generale relativa alla natura stessa del servizio.
La progressiva digitalizzazione delle relazioni economiche e sociali fa sì che l'interruzione della connessione possa produrre conseguenze significativamente diverse rispetto al passato. Un disservizio può impedire una comunicazione, ma può anche compromettere un'attività lavorativa, una lezione a distanza, una transazione economica, l'accesso a un servizio pubblico o la possibilità di utilizzare un dispositivo connesso.
La connettività tende quindi ad assumere caratteristiche proprie di un'infrastruttura essenziale. Ciò non significa necessariamente assimilarla giuridicamente ai servizi pubblici tradizionali, ma riconoscere che la sua affidabilità produce effetti che trascendono il rapporto bilaterale tra utente e operatore.
Da questo punto di vista, la resilienza delle reti diventerà una componente sempre più importante della tutela del consumatore. Il rischio di interruzioni dovute a guasti, eventi climatici estremi, sovraccarichi, incidenti informatici o altri fenomeni di natura sistemica introduce infatti una dimensione collettiva della qualità del servizio.
Il consumatore del prossimo quadriennio potrebbe pertanto attribuire alla continuità del servizio un valore non inferiore a quello della velocità o del prezzo. La resilienza della rete potrebbe diventare, di conseguenza, una vera e propria dimensione della qualità percepita.
Un ulteriore fattore destinato a incidere sulla posizione del consumatore riguarda la crescente complessità delle strutture tariffarie.
Il prezzo nominale rappresenta sempre meno, da solo, una misura adeguata del costo effettivo della connettività. Promozioni temporanee, sconti condizionati, servizi aggiuntivi, rateizzazione dei dispositivi, costi di attivazione, clausole legate alla permanenza e modifiche successive delle condizioni possono rendere difficile per l'utente determinare quanto effettivamente spenderà nel corso dell'intera relazione contrattuale.
Il problema assume particolare rilevanza in un contesto nel quale gli operatori tendono a proporre offerte sempre più personalizzate e convergenti. Telefonia mobile, connettività fissa, servizi audiovisivi, contenuti digitali, dispositivi e ulteriori prestazioni possono essere ricondotti a un unico rapporto commerciale. L'integrazione può produrre vantaggi di prezzo e di comodità, ma può anche aumentare la difficoltà di comparazione.

Il consumatore potrebbe quindi trovarsi di fronte a una forma di asimmetria informativa temporale: il costo realmente rilevante non è quello osservato al momento della sottoscrizione, ma quello sostenuto lungo l'intero ciclo di vita del contratto.
Una tutela effettiva richiede pertanto che l'utente possa comprendere non soltanto il prezzo iniziale, ma il costo totale atteso della relazione contrattuale.

6.0.3. Switching e libertà di uscita: bundle, convergenza e rischio di lock-in (Rosaria Petti)

La capacità di cambiare operatore rappresenta una delle condizioni fondamentali affinché la concorrenza possa produrre effetti favorevoli per il consumatore.
Non si tratta soltanto della possibilità giuridica di cambiare fornitore, ma della facilità effettiva del cambiamento. Un consumatore può disporre formalmente del diritto di recesso e incontrare, nella pratica, procedure complesse, tempi di attesa, informazioni frammentarie o difficoltà nel trasferimento del servizio.
La rilevanza di questo tema è confermata anche dalla recente attività di AGCOM: nel 2026 l'Autorità ha concluso un procedimento relativo al monitoraggio delle procedure di passaggio degli utenti su rete fissa e ha avviato un apposito tavolo tecnico.
La libertà di uscita deve quindi essere considerata una componente della qualità del mercato. Quanto più semplice è cambiare operatore, tanto maggiore è la pressione competitiva esercitata sugli operatori in termini di prezzo, qualità e innovazione.
La convergenza tra servizi rappresenta uno degli sviluppi più rilevanti dei mercati delle comunicazioni elettroniche. Il consumatore può beneficiare di un unico interlocutore, di una gestione integrata e di condizioni economiche potenzialmente più vantaggiose.
Tuttavia, quanto maggiore è il grado di integrazione dell'offerta, tanto più complessa può diventare la valutazione delle alternative.
Il fenomeno del lock-in merita pertanto particolare attenzione. La dipendenza dal fornitore può derivare non soltanto da vincoli contrattuali espliciti, ma anche dall'accumulo di servizi collegati, dalla perdita di vantaggi commerciali in caso di recesso, dall'utilizzo di dispositivi associati o dalla difficoltà di trasferire senza soluzione di continuità l'intero ecosistema di servizi.
La libertà di scelta deve quindi essere valutata in una prospettiva sostanziale. Se il consumatore può teoricamente cambiare operatore ma, per farlo, deve rinunciare a numerosi servizi o affrontare una procedura complessa, la sua libertà risulta significativamente ridotta.

6.0.4. Personalizzazione delle offerte e rischio di discriminazione (Rosaria Petti)

L'impiego crescente dei dati e dell'intelligenza artificiale potrebbe trasformare ulteriormente le modalità attraverso le quali vengono costruite le offerte di comunicazione elettronica.
La personalizzazione può produrre vantaggi significativi: un operatore può proporre a ciascun utente un servizio coerente con i suoi effettivi consumi, evitando prestazioni non necessarie. Tuttavia, la possibilità di costruire offerte sempre più granulari solleva interrogativi sulla trasparenza dei criteri utilizzati.
La personalizzazione potrebbe riguardare non soltanto il contenuto dell'offerta, ma anche il prezzo, gli incentivi, le promozioni o le condizioni di rinnovo. In tale scenario diventa più difficile per il consumatore sapere se l'offerta ricevuta rappresenti una condizione generale o sia stata costruita sulla base della sua storia di consumo, delle sue caratteristiche o della sua propensione a cambiare fornitore.
Si apre così un possibile nuovo fronte della tutela: quello della personalizzazione economica.
Anche il rapporto tra consumatore e operatore è destinato a cambiare radicalmente. Chatbot e sistemi di intelligenza artificiale stanno progressivamente sostituendo alcune funzioni tradizionalmente svolte dagli operatori umani.
L'automazione può ridurre i tempi di attesa e rendere disponibile l'assistenza in qualsiasi momento. Ma proprio nei casi più complessi, l'assenza di un interlocutore umano può trasformarsi in un ostacolo all'esercizio dei diritti.
AGCOM ha già riconosciuto la centralità di questa questione. La disciplina adottata con la delibera n. 255/24/CONS mantiene il canale telefonico con operatore umano come modalità obbligatoria di assistenza e introduce specifici standard qualitativi, oltre a rafforzare la tracciabilità dei reclami.
La possibilità di ottenere una risposta automatica non coincide quindi necessariamente con la possibilità di ottenere una soluzione. Nel prossimo quadriennio, la qualità dell'assistenza potrebbe diventare una componente sempre più importante della posizione competitiva degli operatori e della tutela dell'utente.
La qualità della connettività deve infine essere considerata insieme alla sua accessibilità economica.

Il rischio non sarà soltanto quello di un divario tra chi dispone e chi non dispone di una connessione, ma di un divario tra utenti che possono permettersi connessioni ad alta qualità e utenti costretti a utilizzare servizi più limitati.
La differenza potrebbe diventare particolarmente significativa con la crescente diffusione di applicazioni che richiedono elevate capacità di banda, bassa latenza e connessioni affidabili. Se la qualità della connessione determina sempre più la qualità dell'accesso a servizi economici, culturali e sociali, l'accessibilità economica diviene una componente sostanziale della partecipazione digitale.
La tutela del consumatore dovrà quindi confrontarsi con una tensione crescente tra innovazione tecnologica e inclusione.
Le trasformazioni descritte suggeriscono l'opportunità di affiancare agli indicatori tradizionali di mercato e di qualità una nuova generazione di indicatori centrati sulla posizione effettiva dell'utente.
Un possibile Consumer Connectivity Index potrebbe prendere in considerazione, oltre al prezzo, almeno cinque dimensioni: qualità effettiva della connessione, affidabilità, facilità di switching, trasparenza del costo complessivo e accessibilità economica.
Un simile approccio consentirebbe di spostare il baricentro dell'analisi dal singolo contratto alla relazione complessiva tra consumatore e mercato.
La posizione dell'utente potrebbe così essere valutata non soltanto sulla base della convenienza di una determinata offerta, ma in funzione della possibilità di scegliere tra alternative, modificare la propria decisione, ricevere un servizio di qualità e far valere i propri diritti.

7. Le prospettive per AGCOM nel periodo 2026–2030 nel settore delle comunicazioni elettroniche *(Rosaria Petti)*

Alla luce delle dinamiche descritte, il prossimo quadriennio potrebbe richiedere ad AGCOM un progressivo rafforzamento degli strumenti di osservazione e analisi dei comportamenti dei consumatori.
Una prima esigenza riguarda la costruzione di una conoscenza più sistematica degli effetti degli algoritmi. La regolazione dei mercati digitali richiede infatti di comprendere non soltanto le caratteristiche dei servizi, ma anche le modalità attraverso le quali essi vengono presentati e utilizzati.
Una seconda direttrice riguarda la misurazione della contendibilità. Indicatori relativi ai costi di uscita, alla facilità di switching, alla portabilità e alla comprensibilità delle offerte potrebbero contribuire a rappresentare meglio la posizione effettiva dell'utente rispetto agli operatori.
Una terza esigenza riguarda la qualità della connettività. La crescente rilevanza infrastrutturale delle reti suggerisce di affiancare agli indicatori tecnici tradizionali misure capaci di cogliere la qualità effettivamente sperimentata dagli utenti. La posizione del consumatore dovrebbe essere valutata considerando congiuntamente prestazioni tecniche, continuità del servizio, accessibilità economica, qualità dell'assistenza e possibilità di cambiare fornitore.
Una quarta direttrice riguarda le nuove forme di vulnerabilità. La regolazione potrebbe trarre beneficio da strumenti capaci di identificare non soltanto categorie astratte di utenti vulnerabili, ma situazioni concrete nelle quali l'utente risulta maggiormente esposto a manipolazione, esclusione o perdita di controllo.
Infine, appare sempre più importante una funzione di anticipazione. La velocità dell'innovazione rende difficile intervenire esclusivamente sulla base di fenomeni già consolidati. L'attività di monitoraggio, la ricerca interdisciplinare, la collaborazione con università e centri di ricerca e l'analisi prospettica delle tecnologie emergenti possono diventare componenti essenziali dell'attività regolatoria.
La stessa evoluzione dell'attività dell'Autorità nel settore delle comunicazioni elettroniche mostra questa tendenza. L'attenzione alla qualità dei servizi, alla trasparenza tecnica, all'assistenza clienti, alle procedure di passaggio e all'analisi dei mercati evidenzia una progressiva integrazione tra tutela dell'utente e funzionamento competitivo dei mercati.

8. Quali conclusioni per le comunicazioni elettroniche? *(Rosaria Petti)*

Il prossimo triennio-quadriennio sarà caratterizzato da una trasformazione della posizione del consumatore che appare destinata a essere più profonda di quella prodotta dalla semplice digitalizzazione dei servizi.
L'intelligenza artificiale, gli algoritmi di raccomandazione, le piattaforme, la personalizzazione, i nuovi modelli di abbonamento, la trasformazione dell'informazione, la pubblicità integrata nei contenuti, l'evoluzione delle reti e la digitalizzazione della logistica stanno modificando le condizioni stesse nelle quali il consumatore esercita la propria libertà di scelta.
Il principale elemento di discontinuità risiede nel fatto che una parte crescente della decisione viene trasferita dall'utente all'ambiente tecnologico nel quale egli opera. L'algoritmo seleziona, ordina, raccomanda e personalizza; la piat-

taforma organizza l'accesso; l'intelligenza artificiale interpreta la richiesta e formula la risposta; l'interfaccia orienta il comportamento; il modello di abbonamento rende ricorrente la relazione economica.
Nel settore delle comunicazioni elettroniche questo fenomeno assume una particolare rilevanza. La connessione costituisce ormai un'infrastruttura attraverso la quale si esercitano una pluralità di attività economiche e sociali. La posizione dell'utente non dipende quindi soltanto dal prezzo dell'offerta, ma dalla qualità effettiva della connessione, dalla sua affidabilità, dalla trasparenza delle condizioni, dalla possibilità di cambiare operatore, dalla qualità dell'assistenza e dall'accessibilità economica.
La crescente diffusione della fibra e delle reti ad alta capacità, accompagnata dall'aumento del traffico dati, conferma che la connettività è destinata ad assumere un ruolo sempre più centrale nell'esperienza quotidiana degli utenti. Ne consegue che la qualità della connettività non può essere considerata esclusivamente una questione tecnica: essa rappresenta una componente della posizione economica e sociale del consumatore.
La stessa nozione di qualità è destinata a evolvere. Accanto alla velocità nominale dovranno assumere crescente rilievo la continuità, la latenza, la resilienza, l'affidabilità e la qualità percepita. In questo senso, la regolazione della qualità può diventare uno dei principali strumenti attraverso i quali tradurre l'evoluzione tecnologica in una tutela effettiva dell'utente.
Più in generale, la tradizionale figura del consumatore informato deve essere ripensata. Informazione e trasparenza restano condizioni necessarie, ma non sono più sufficienti. La tutela effettiva richiede che l'utente disponga della possibilità concreta di comprendere, confrontare, scegliere, modificare, interrompere e contestare.
Il consumatore del prossimo futuro sarà dunque, prima ancora che un consumatore "informato", un consumatore autonomo, assistito ma non sostituito dalla tecnologia, personalizzato ma non manipolato, connesso ma non escluso, protetto ma anche capace di esercitare concretamente i propri diritti.
Per AGCOM ciò implica una progressiva evoluzione del paradigma regolatorio: dalla tutela del singolo atto di consumo alla tutela dell'intero ecosistema della scelta. È all'interno di questo ecosistema che si giocherà, nei prossimi anni, l'effettiva posizione del consumatore nei mercati delle comunicazioni.
La sfida del periodo 2026–2030 non sarà pertanto soltanto quella di assicurare mercati innovativi, competitivi e tecnologicamente avanzati. Sarà quella di garantire che l'innovazione non produca nuove forme di asimmetria tali da rendere meramente formale la libertà di scelta.
In ultima analisi, la qualità della regolazione potrà essere misurata anche dalla capacità di assicurare che, in un ambiente sempre più governato da algoritmi e sistemi automatizzati, il consumatore rimanga effettivamente titolare della decisione che lo riguarda.

AUTORITÀ NAZIONALE PER LA CYBERSICUREZZA (ACN)

IL BENE DI CONSUMO COME OGGETTO DI SICUREZZA NAZIONALE.

Competenze, limiti e spazi di intervento dell'ACN nell'orizzonte 2030

(di Michela Mastrantonio)

SOMMARIO: 1 Introduzione. Il nuovo oggetto della sicurezza – 2. Orizzonte 2030: i rischi emergenti – 3. I limiti della competenza e il contenuto della funzione anticipatoria – 4. I possibili spazi di intervento dell'ACN – 5. Conclusioni

1. Introduzione. Il nuovo oggetto della sicurezza

L'Agenzia per la cybersicurezza nazionale negli ultimi anni ha visto crescere in modo rapido il perimetro delle proprie attribuzioni. Alla sua funzione originaria di autorità nazionale NIS si è aggiunta quella di autorità di vigilanza per i sistemi di intelligenza artificiale; inoltre, per effetto della legge di delegazione europea 2025, l'Agenzia ha assunto il ruolo di riferimento nell'attuazione nazionale del regolamento sulla ciberresilienza[1].

Sul piano sovranazionale, nell'arco di due mesi l'Unione europea ha adottato due programmi riferiti al medesimo orizzonte temporale: il 19 novembre 2025 la Commissione ha approvato l'Agenda dei consumatori 2030, quadro strategico quinquennale articolato su quattro priorità, fra cui l'equità digitale; il 20 gennaio 2026 ha presentato il pacchetto sulla cibersicurezza, che comprende la revisione del regolamento di settore, una proposta di semplificazione delle notifiche e il rafforzamento del mandato operativo dell'agenzia europea[2]. I due documenti, pur esplicitamente mossi dal raggiungimento di obiettivi in parte sovrapponibili, non contengono rinvii reciproci. La politica dei consumatori nasce dal mercato interno e ragiona per contratti, pratiche commerciali e rimedi individuali attivati dall'interessato; la sicurezza cibernetica nasce dalla protezione delle infrastrutture e ragiona per soggetti obbligati, notifiche e continuità dei servizi essenziali. Nel lessico della prima la persona compare come consumatore, parte di un rapporto asimmetrico; nel lessico della seconda, la persona compare come cittadino, destinatario di iniziative di consapevolezza.

Le due prospettive hanno convissuto senza attriti fintanto che i prodotti di consumo sono stati considerati esclusivo appannaggio della disciplina consumeristica. A ben vedere, il cumulo di competenze in capo all'ACN presentato in apertura colloca oggi presso un'unica amministrazione le tre leve che incidono sulla condizione di sicurezza del prodotto di consumo: la certificazione, la sorveglianza del mercato e l'analisi della minaccia. In altre parole, l'approccio tradizionale organizzato per settori di competenza sembra, quindi, destinato a cessare nel breve periodo, in considerazione del nuovo ruolo che il bene di consumo è destinato ad assumere in qualità di superficie di attacco nazionale.

Interrogarsi sul consumatore del 2030 dal punto di vista dell'Agenzia, dunque, significa domandarsi che cosa accade quando una tecnica di protezione costruita per interessi collettivi si trova ad avere per oggetto beni di consumo, tipicamente oggetto di interessi individuali. Di conseguenza, la sfida per l'ACN consiste nel valutare se e a quali condizioni il modello di intervento, imposto dalle caratteristiche dei rischi di cybersicurezza e dalle esigenze della loro gestione, possa essere calibrato o ripensato rispetto ai rischi sistemici annunciati dal recente assetto normativo e dalle dinamiche di mercato: quelli che derivano dallo sviluppo delle nuove tecnologie e dal conseguente ampliamento della superficie di attacco del Paese.

1. Decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109, artt. 5 e 7; d.lgs. 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555; regolamento (UE) 2019/881 e d.lgs. 3 agosto 2022, n. 123, art. 4, quanto alla certificazione; legge 23 settembre 2025, n. 132, artt. 20 e 24, e relativi decreti legislativi di adeguamento approvati in esame definitivo il 4 agosto 2026, quanto alla vigilanza del mercato sui sistemi di intelligenza artificiale; legge 17 marzo 2026, n. 36 (legge di delegazione europea 2025), artt. 15-17, quanto alla ciberresilienza dei prodotti, ai servizi di sicurezza gestiti e alla solidarietà cibernetica.

2. Commissione europea, Agenda dei consumatori 2030, 19 novembre 2025, articolata in quattro priorità fra le quali l'equità digitale, con l'annuncio di una proposta di *Digital Fairness Act*; il pacchetto sulla cibersicurezza del 20 gennaio 2026 comprende la proposta di revisione del regolamento (UE) 2019/881, COM(2026) 11, e la proposta di direttiva di semplificazione e allineamento, COM(2026) 13.

2. Orizzonte 2030: i rischi emergenti

L'orizzonte del 2030 risponde alla convergenza di scadenze già fissate. Il portafoglio europeo di identità digitale dovrà essere reso disponibile entro il dicembre 2026 e accettato dai soggetti privati operanti in settori regolati entro il dicembre 2027[3]; il regolamento sulla ciberresilienza dei prodotti si applica nel corpo principale dei propri obblighi dall'11 dicembre 2027, con anticipazione degli obblighi di segnalazione all'11 settembre 2026[4]; le disposizioni sui sistemi di intelligenza artificiale ad alto rischio produrranno effetti fra il dicembre 2027 e l'agosto 2028[5]; la transizione alla crittografia post-quantistica dovrà coprire i casi d'uso ad alto rischio entro il 2030[6].

Poiché il ciclo che intercorre tra la formulazione di una proposta europea e la sua piena attuazione si estende generalmente per cinque o sei anni, le scelte non assunte oggi sono destinate a produrre effetti oltre l'orizzonte temporale considerato. Il 2030 rappresenta, pertanto, sia il primo momento in cui sarà possibile osservare gli effetti complessivi delle misure adottate, sia l'ultimo rispetto al quale le decisioni assunte oggi possono ancora risultare efficaci. L'esame congiunto delle scadenze già definite, degli atti di indirizzo politico e delle dinamiche di mercato consente di delineare fin d'ora i potenziali rischi destinati ad assumere rilievo nel prossimo quadriennio nel settore della cybersicurezza.

L'introduzione del portafoglio europeo di identità digitale determinerà la concentrazione in un'unica credenziale di funzioni essenziali per l'accesso a servizi bancari, sanitari e amministrativi. Sebbene il portafoglio e i relativi prestatori siano sottoposti a specifici requisiti di sicurezza e vigilanza, la disciplina non sembra assicurare un analogo presidio dell'apparato (in particolare, dello smartphone e del sistema operativo) su cui il portafoglio è installato. Ne deriva un possibile disallineamento tra la sicurezza certificata dell'applicazione e quella della piattaforma che la ospita: la compromissione o l'obsolescenza di una popolazione di dispositivi potrebbe infatti compromettere, su larga scala, l'accesso a servizi essenziali, senza che l'apparato sia formalmente qualificato come componente dell'infrastruttura di identità digitale né che sia individuato un soggetto responsabile del suo livello di sicurezza. Il rischio di cybersicurezza consiste, pertanto, nella possibilità che una vulnerabilità della piattaforma tecnologica sottostante si trasformi in un rischio sistemico per l'intero ecosistema dell'identità digitale.

La diffusione di agenti AI capaci di comparare offerte, negoziare e concludere acquisti per conto dell'utente modifica la struttura del rapporto di consumo, poiché l'atto negoziale e l'eventuale pagamento vengono eseguiti da un sistema autonomo sulla base di istruzioni generali e di contenuti acquisiti durante l'interazione. Il rischio più insidioso non consiste nell'errore dell'agente, ma nella manipolazione del suo comportamento mediante istruzioni ostili inserite nei dati o nei contenuti che esso elabora, una vulnerabilità comunemente ricondotta al fenomeno della prompt injection. Queste istruzioni possono indurre l'agente ad adottare decisioni o a compiere operazioni diverse da quelle volute dall'utente, pur utilizzando credenziali e strumenti legittimamente autorizzati. Una dinamica di questo tipo -- oltre a mettere in crisi i tradizionali criteri di imputazione della responsabilità -- presenta una potenziale dimensione sistemica: poiché una medesima istruzione ostile può essere replicata su tutti gli utenti dello stesso modello o servizio, un'unica vulnerabilità può produrre simultaneamente acquisti fraudolenti, divulgazioni di dati o pagamenti indebiti su larga scala[7].

Il rischio di effetti di massa si manifesta anche nell'ambiente domestico connesso, in cui la crescente integrazione di dispositivi digitali trasferisce su una pluralità di apparati di uso quotidiano funzioni rilevanti per la sicurezza, la privacy e l'accesso a servizi essenziali. Entro il 2030 l'abitazione connessa sarà composta da numerosi dispositivi digitali, spesso amministrati da utenti privi delle competenze necessarie per assicurarne la protezione. Questi apparati saranno soggetti a regimi normativi differenti, concernenti rispettivamente la sicurezza dei prodotti con elementi digitali, la protezione dei dati e, per i veicoli, i requisiti di omologazione. La frammentazione dei quadri regolatori e delle relative autorità di controllo può generare difficoltà di coordinamento. In questo ambito, un ulteriore importante rischio riguarda il patrimonio di dispositivi già installati. Il regolamento sulla ciberresilienza, infatti, troverà piena applicazione

3. Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.
4. Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).
5. Regolamento (UE) 2024/1689, i cui obblighi di trasparenza di cui all'art. 50 si applicano dal 2 agosto 2026; il regolamento (UE) 2026/1744 ha differito al 2 dicembre 2027 e al 2 agosto 2028 l'applicazione delle sezioni 1, 2 e 3 del capo III relative ai sistemi ad alto rischio.
6. Raccomandazione (UE) 2024/1101 dell'11 aprile 2024; NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, giugno 2025, che fissa alla fine del 2026 l'avvio della transizione, al 2030 la copertura dei casi d'uso ad alto rischio e al 2035 la transizione completa.
7. Il quadro normativo europeo non sembra ancora intercettare pienamente questo rischio. Gli obblighi di trasparenza applicabili agli agenti destinati ai consumatori, secondo l'AI Act, operativi dal 2 agosto 2026, presuppongono infatti un destinatario umano in grado di comprendere l'informazione e di reagire alla manipolazione; risultano quindi poco incisivi quando l'istruzione ostile è rivolta direttamente alla macchina. Ne emerge un'asimmetria regolatoria: mentre i sistemi di intelligenza artificiale impiegati in contesti professionali o istituzionali possono essere soggetti a presidi più intensi, gli agenti destinati a effettuare acquisti e autorizzare pagamenti per conto di un'ampia platea di consumatori restano sottoposti a obblighi più limitati.

dal dicembre 2027 e riguarderà principalmente i prodotti immessi sul mercato successivamente a tale data o sottoposti a modifiche sostanziali. Ne resterà quindi in larga parte escluso il parco domestico preesistente, che potrebbe essere privo di requisiti di sicurezza uniformi, di un periodo di supporto dichiarato e di canali adeguati alla gestione e alla segnalazione delle vulnerabilità. Il rischio consiste nella permanenza, all'interno delle abitazioni, di dispositivi insicuri ma ancora connessi e funzionalmente rilevanti, senza che esista un obbligo generalizzato di aggiornamento, sostituzione o dismissione né una chiara responsabilità per il loro stato di sicurezza[8].

Adottando un'ulteriore prospettiva, che sempre riguarda l'ambito di competenza dell'ACN, lo sviluppo repentino delle tecnologie ha ormai compromesso su larga scala il presupposto umano su cui si fondano molti meccanismi di sicurezza: la capacità di riconoscere l'autenticità della comunicazione ricevuta. Le tecnologie generative consentono, infatti, di replicare con elevata precisione voce, immagine, linguaggio e contesto relazionale della vittima, sfruttando anche dati personali già esposti in precedenti violazioni. Il phishing continua a rappresentare il principale vettore di accesso iniziale, mentre le campagne di ingegneria sociale risultano sempre più frequentemente assistite dall'intelligenza artificiale[9].

Il rischio di cybersicurezza non consiste, pertanto, solo nell'aumento delle frodi individuali, ma nella progressiva perdita di efficacia del comportamento diligente dell'utente come presidio di sicurezza. I tradizionali criteri fondati sulla riconoscibilità del falso e sulla possibilità di evitare il danno mediante un'attenzione ordinaria presuppongono infatti che la persona possa distinguere il contenuto autentico da quello contraffatto. Quando la falsificazione diviene tecnicamente indistinguibile e può essere prodotta su larga scala, questo presupposto viene meno: anche un utente diligente può essere indotto a comunicare credenziali, autorizzare operazioni o installare un software malevolo.

Un ultimo aspetto merita attenzione. Il consumatore del 2030 non sarà esposto soltanto ai rischi del proprio tempo. Gli insiemi informativi la cui riservatezza deve durare decenni sono già stati raccolti da chi dispone di risorse sufficienti per conservarli in attesa di poterli decifrare e nessuna misura successiva riduce il valore di ciò che è già stato acquisito. La raccomandazione europea del 2024 e la tabella di marcia elaborata dal gruppo di cooperazione istituito dalla disciplina sulle reti fissano al riguardo una progressione precisa, con avvio della transizione alla crittografia post-quantistica entro la fine del 2026, copertura dei casi d'uso ad alto rischio entro il 2030 e transizione completa entro il 2035.

Il criterio di priorità adottato in quella progressione è la criticità del detentore. Applicato agli insiemi riferiti alle persone, esso conduce a un esito che genera preoccupazione. Un archivio sanitario privato, un servizio di analisi genetica, una piattaforma che conservi anni di comunicazioni personali non costituiscono infrastrutture critiche e non compaiono in alcuna lista di priorità, pur custodendo dati la cui vita utile riservata supera l'intero orizzonte della transizione. Il criterio misura l'importanza di chi detiene, non la durata dell'interesse alla riservatezza di ciò che è detenuto: due grandezze che coincidono nella maggior parte dei casi e divergono radicalmente proprio nei dati riferiti alle persone.

3. I limiti della competenza e il contenuto della funzione anticipatoria

Nessuno dei profili descritti è stato attribuito all'Agenzia in ragione della posizione del consumatore e la circostanza spiega tanto l'ampiezza quanto i limiti della competenza che ne risulta.

Dove la scelta del singolo, consapevole o meno, ricade unicamente su chi la compie, il problema è di equilibrio contrattuale e di informazione e appartiene alla tutela consumeristica. Dove essa concorre ad alimentare la superficie d'attacco collettiva, il problema diventa sicurezza nazionale e l'intervento pubblico trova un fondamento che prescinde dalla protezione della parte debole.

Alcuni dei profili esaminati, pur rilevanti nell'ambito della sicurezza cibernetica, sono stati attribuiti dall'ordinamento ad altre istituzioni. Ciascuna delle autorità richiamate dispone di una via d'accesso individuale. Il reclamo all'autorità di protezione dei dati, la segnalazione all'autorità antitrust, l'esposto all'autorità di vigilanza sul settore bancario non sono soltanto strumenti di tutela della posizione soggettiva del singolo: sono canali attraverso i quali l'amministrazione riceve, in via continua e non sollecitata, informazioni sulla realtà che vigila. La funzione conoscitiva è un effetto della funzione di tutela e ne è inseparabile. L'Agenzia non dispone di alcun canale di questo tipo[10]. Il suo sistema è costruito sulla notifica e la notifica proviene da chi è tenuto a effettuarla. Nel 2025 lo CSIRT Italia ha trattato 2.729

8. Gli strumenti offerti dal diritto dei contratti e dalla disciplina generale sulla sicurezza dei prodotti non sembrano colmare tale lacuna. Il primo rimedio presuppone l'iniziativa dell'acquirente, che dovrebbe riconoscere la cessazione degli aggiornamenti come difetto di conformità e attivarsi per ottenere tutela; il secondo opera in via residuale e può arretrare rispetto alle discipline settoriali, senza assicurare una copertura effettiva del parco già installato. Ne deriva il rischio di una regressione della protezione: proprio nel passaggio al nuovo regime, la tutela dei consumatori rispetto ai prodotti connessi preesistenti potrebbe risultare meno incisiva di quella precedentemente assicurata.

9. ENISA, Threat Landscape 2025, ottobre 2025.

10. La scelta ha una ragione precisa: un canale rivolto al pubblico genererebbe aspettative di tutela individuale che un'amministrazione di sicurezza non può soddisfare e che altre sedi già presidiano con strumenti appropriati. Ne discende però la conseguenza che il riparto, considerato solo come distribuzione di competenze, non lascia apprezzare: l'unica amministrazione dotata delle competenze tecniche per accertare la sicurezza di un prodotto o di un sistema è anche l'unica priva di qualsiasi rapporto con chi quel prodotto lo utilizza.

eventi cibernetici e 615 incidenti con impatto confermato, diramando quasi 47.000 comunicazioni di allertamento[11]. Ciascuna di quelle comunicazioni ha per destinatario un'organizzazione, perché un'organizzazione ha un referente, un recapito e l'obbligo di dare seguito. Si conosce dunque ciò che qualcuno ha il dovere di riferire e si conosce nella forma in cui il dovere impone di riferirlo. La soglia di significatività conferma la geometria. L'incidente è misurato sull'interruzione del servizio, sulle perdite operative e sull'estensione della compromissione presso il soggetto notificante. Ne consegue che una violazione che esponga alcuni milioni di persone a una campagna di frode successiva non viene valutata e ritenuta di minore rilievo: non entra nella categoria, poiché non degrada alcuna prestazione presso chi la subisce. La grandezza "esposizione della popolazione" non è sottopesata nel sistema di misurazione vigente: ne è del tutto assente. Il punto di ingresso unico per le notifiche, gestito dall'agenzia europea secondo il principio della segnalazione singola e della condivisione multipla, interviene sul modo in cui la notifica è resa e sulla circolazione successiva dell'informazione, non sulla definizione di ciò che deve essere notificato[12]. A ben vedere, la medesima caratteristica che ha reso praticabile questo modello di protezione – la costruzione degli obblighi e dei flussi attorno a soggetti organizzati e identificabili – è ciò che oggi impedisce di osservare il lato della domanda. Un'amministrazione che conosce ciò che i soggetti obbligati sono tenuti a riferirle, misura la significatività degli eventi sull'impatto ai servizi e interviene sui prodotti a valle della loro immissione sul mercato può, così strumentata, reagire più rapidamente. Non può anticipare. La competenza dell'ACN quindi deve tenere conto di cosa l'Agenzia non deve fare (che è un limite di riparto) e di cosa non è in condizione di fare (che è un limite di strumentazione). La funzione anticipatoria, nella materia qui considerata, si compone di quattro elementi: (i) misurare l'esposizione della popolazione come parametro di riferimento, e non come effetto derivato di incidenti occorsi presso soggetti obbligati; (ii) conoscere la composizione e la diffusione del parco installato prima che un fenomeno lo attraversi, anziché ricostruirle dopo; (iii) individuare i punti di leva che raggiungono popolazioni ampie di apparati attraverso un numero ridotto di soggetti già vigilati, e nell'esercitarvi la vigilanza con gli strumenti ordinari; (iv) assumere posizione sulla qualificazione dei fenomeni emergenti prima che il primo episodio la determini di fatto.

4. I possibili spazi di intervento dell'ACN

La disciplina applicabile ai profili di rischio sopra richiamati esiste, è di recente formazione e in più punti tecnicamente avanzata; lacune e criticità sono certamente presenti, ma tuttora oggetto di esame nelle sedi competenti. Ciò che ne limita l'efficacia non è quindi la formulazione, bensì, in alcuni casi, il tempo della sua attuazione e, in altri, il ritardo nell'attribuire rilevanza a fenomeni già in atto: tempi che non coincidono con quelli di maturazione dei rischi. In questa divergenza si colloca la possibile iniziativa dell'Agenzia, che non postula un mutamento della sua natura, ma un adattamento della sua postura.

Il possibile piano di intervento in funzione preventiva si articola in due ordini di attività.

Il primo ha natura conoscitiva e incide su ciò che l'Agenzia è in grado di osservare. Non consiste nell'acquisire dati che essa non possiede, bensì nell'ampliare i parametri di osservazione, così da far emergere grandezze che il perimetro attuale non restituisce: l'esposizione della popolazione, la composizione del parco di apparati in uso, la diffusione effettiva dei prodotti. Sono grandezze non ricostruibili a posteriori, e destinate a fondare le decisioni successive. Il secondo ha natura prescrittiva e incide su ciò che i soggetti vigilati sono tenuti a fare. Si esprime in qualificazioni giuridiche, condizioni d'uso e criteri di priorità: non produce conoscenza, ma determina il regime applicabile a fenomeni prossimi a manifestarsi. Alcuni interventi rientrano per intero nei poteri già attribuiti all'Agenzia; altri consistono in posizioni che essa può sostenere nelle sedi europee ove i tavoli di confronto sono ancora aperti. In nessun caso la difficoltà risiede nella carenza di strumenti giuridici, bensì nell'assenza di una determinazione sul loro impiego.

Con riferimento al primo dei due ordini di intervento (quello di natura conoscitiva), non si tratta di acquisire dati di cui l'Agenzia non dispone, bensì di riconoscere il valore di quelli di cui è già in possesso. Gli indirizzi di *phishing* trattati dallo CSIRT, le credenziali individuali esposte e rilevate nel monitoraggio, la loro distribuzione geografica, la maggiore vulnerabilità che alcune categorie di soggetti manifestano rispetto ad altre: isolatamente considerati, costituiscono elementi della risposta operativa quotidiana e in essa si esauriscono; considerati congiuntamente e con continuità, integrano una misura dell'esposizione della popolazione, di cui nessun documento di programmazione dà conto. Da questo riconoscimento discende una conseguenza immediata sulla struttura dei flussi informativi. Le soglie di significatività degli incidenti sono attualmente commisurate all'interruzione del servizio e alle perdite operative

11. ACN, Relazione annuale al Parlamento 2025, Roma, 2026.

12. Proposta di Digital Omnibus del 19 novembre 2025, che introduce con un nuovo art. 23-bis della direttiva (UE) 2022/2555 il punto di ingresso unico per le notifiche, gestito da ENISA secondo il principio della segnalazione singola e della condivisione multipla. Quanto ai criteri di significatività attualmente vigenti, regolamento di esecuzione (UE) 2024/2690 della Commissione.

presso il soggetto notificante. Ne consegue che una violazione che esponga alcuni milioni di persone a una successiva campagna di frode non è soltanto valutata come meno rilevante, ma esula del tutto dalla fattispecie, non degradando alcuna prestazione presso chi la subisce. Introdurre un criterio fondato sul numero dei soggetti esposti vale a ricondurre nella sfera di conoscibilità dell'amministrazione eventi che attualmente ne restano fuori. L'Agenzia potrebbe dunque rideterminare il proprio punto di osservazione. Per l'intera fase di costruzione del sistema nazionale di cybersicurezza questo punto è stato l'infrastruttura, e la scelta era congrua, poiché i beni di consumo non ne facevano parte. Quella condizione è venuta meno: il dispositivo personale, l'apparato domestico connesso, il veicolo costituiscono oggi superfici di attacco del Paese, e attraverso l'impresa individuale e la microimpresa entrano nelle filiere che il sistema è chiamato a proteggere. All'estensione del perimetro da proteggere deve corrispondere l'estensione del perimetro osservato. Il parco domestico offre la verifica più immediata di questo assunto. Nelle abitazioni italiane si trovano decine di milioni di apparati di cui non è nota né la consistenza per modello, né la versione di programma eseguita, né la durata residua degli aggiornamenti. Una porzione consistente di quel parco, tuttavia, non appartiene ai soggetti che hanno comprato il prodotto e/o il servizio: l'apparecchiatura terminale fornita in comodato dall'operatore di comunicazione elettronica, unico dispositivo permanentemente esposto su rete pubblica nella maggioranza delle abitazioni, appartiene a un soggetto già vigilato, che la amministra da remoto e vi appone il proprio marchio. Qualificare questa base installata come parte potenziale della superficie di attacco nazionale consente di esigere dall'operatore ciò che attualmente non gli è richiesto: l'inventario degli apparati per modello e versione, l'intervallo fra la disponibilità di una correzione e la sua distribuzione al parco, la data di cessazione del supporto per ciascun modello. Sul piano della sicurezza, milioni di apparati sono raggiunti attraverso poche decine di interlocutori, senza istituire alcun rapporto con i cittadini. Sul piano conoscitivo, l'inventario delle flotte è allo stato il solo censimento del parco domestico nazionale materialmente conseguibile. È in questa prospettiva che assume rilievo dirimente la disponibilità di una rappresentazione periodica di questi dati in forma aggregata. Non si tratta di un adempimento documentale: una rappresentazione continua dell'esposizione consente di intervenire prima che il danno assuma una dimensione sistemica, e di concentrare il monitoraggio sulle aree geografiche, sulle categorie di prodotto e sui gruppi di individui maggiormente esposti. Questo approccio consente di ridurre la finestra temporale tra l'attacco e l'intervento riparatore, con l'effetto di limitare l'entità del danno.

La logica qui rappresentata non è nuova: coincide con quella della *software bill of materials* (SBOM), la distinta dei componenti software che il regolamento sulla ciberresilienza impone al fabbricante di redigere. La SBOM elenca i componenti di cui il prodotto si compone, in formato leggibile da macchina, e va mantenuta aggiornata per l'intero periodo di supporto; non è soggetta a pubblicità, ma è fornita alle autorità di sorveglianza del mercato su richiesta. La ratio dell'obbligo è nota: accertata la vulnerabilità di un componente diffuso, la difficoltà non risiede nella correzione, bensì nella localizzazione. Conoscere la composizione di un sistema e la collocazione dei suoi elementi riduce sensibilmente l'intervallo fra la rilevazione del fatto e l'intervento. Applicare la medesima logica al contesto informativo significa costruire, per il territorio nazionale, ciò che la SBOM costruisce per il singolo prodotto[13].

Poiché dal dicembre 2027 l'autorità di sorveglianza del mercato per i prodotti connessi è in Italia l'Agenzia, essa si troverà fra i pochi soggetti in condizione di conoscere la composizione dell'oggetto collocato nell'abitazione. Ne resteranno prive tanto la persona che quell'oggetto ha acquistato, quanto le autorità che ne tutelano la posizione, non legittimate a richiederla. È l'unico profilo nel quale l'amministrazione strutturalmente estranea al lato della domanda ne è invece l'unica osservatrice possibile.

In un sistema così congegnato l'impiego dell'intelligenza artificiale si configura come imprescindibile, non quale innovazione bensì quale condizione di praticabilità: la correlazione continua di flussi eterogenei riferiti a decine di milioni di apparati non è operazione eseguibile con mezzi organizzativi ordinari. L'Agenzia è del resto già orientata in questa direzione. Nell'ambito dell'investimento 1.5 «Cybersecurity» del Piano nazionale di ripresa e resilienza, di cui è soggetto attuatore, essa ha destinato risorse proprie all'analisi predittiva delle minacce e all'acquisizione di un sistema di calcolo ad alte prestazioni, espressamente riferito al monitoraggio centralizzato della minaccia cibernetica, anche mediante impiego di strumenti di intelligenza artificiale e di apprendimento automatico[14]. Il monitoraggio centralizzato

13. L'obbligo trae origine da una vicenda determinata. Il 9 dicembre 2021 fu resa pubblica una vulnerabilità della libreria Log4j --- componente di registrazione degli eventi largamente diffuso nelle applicazioni scritte in linguaggio Java --- che consentiva l'esecuzione di codice da remoto e alla quale fu attribuito il punteggio di gravità massimo. La correzione fu disponibile nell'arco di pochi giorni; l'individuazione dei sistemi interessati richiese invece settimane e in numerosi casi non fu conseguita, poiché la libreria non era di norma installata direttamente, ma incorporata in altri componenti a loro volta integrati nei prodotti finali. Molte organizzazioni non furono in grado di stabilire se il proprio software la contenesse. L'episodio, unitamente alla compromissione di SolarWinds del 2020, determinò il passaggio della distinta dei componenti da buona pratica raccomandata a requisito vincolante: la proposta di regolamento sulla ciberresilienza fu presentata nel settembre 2022 e il testo definitivo, all'allegato I, parte II, punto 1, impone al fabbricante di identificare e documentare i componenti del prodotto, anche mediante redazione di una distinta in formato di uso corrente e leggibile da macchina.

14. Investimento 1.5 «Cybersecurity», Missione 1, Componente 1 del Piano nazionale di ripresa e resilienza, a titolarità del Dipartimento per la trasformazione digitale e di cui l'Agenzia è soggetto attuatore, con dotazione di 623 milioni di euro. Sul piano europeo, la Commissione ha adottato il 7 luglio 2026 il Piano d'azione in materia di cybersicurezza e intelligenza artificiale, COM(2026) 577 final, che prevede fra l'altro una capacità europea di valutazione dei modelli e un quadro di accesso strutturato alle capacità

ha per destinatari le amministrazioni e i soggetti rientranti nel perimetro degli obblighi, ed è costruito, coerentemente, sulla medesima geometria descritta in precedenza. La rappresentazione dell'esposizione delle famiglie non postulerebbe una capacità diversa da quella: postulerebbe di rivolgerla a un oggetto diverso. Anche in questo caso, dunque, ciò che difetta non è lo strumento, bensì la determinazione sul suo impiego.

Gli strumenti di intelligenza artificiale e di analisi automatizzata rilevano sotto un ulteriore profilo, in cui la funzione conoscitiva si esercita non sul lato della domanda ma su quello dell'offerta: l'analisi dei prodotti immessi sul mercato restituisce la composizione del parco che le famiglie acquisteranno e, al tempo stesso, orienta la sorveglianza che su quei prodotti dovrà esercitarsi. La disciplina europea definisce poteri e procedure, non l'intensità del controllo, che resta rimessa all'autorità nazionale. Il controllo documentale, condotto sui fascicoli tecnici, è organizzabile in tempi brevi, ma, attestandosi la conformità della generalità dei prodotti mediante valutazione interna del fabbricante, accerta l'esistenza di dichiarazioni anziché la sicurezza dei beni. Il controllo sostanziale, fondato sull'acquisizione dei prodotti sul mercato e sulla prova di laboratorio, costituisce l'unico segnale idoneo a orientare la condotta del fabbricante in un mercato nel quale l'acquirente è privo di ogni elemento di valutazione. Esso postula tuttavia capacità di non rapida acquisizione: l'attrezzatura dei laboratori e il reclutamento di profili di ingegneria del prodotto seguono, nell'amministrazione pubblica, tempi non comprimibili. Ne discende che il numero dei prodotti sottoponibili a prova resterà, in ogni caso, una frazione minima di quelli immessi sul mercato.

È qui che l'analisi automatizzata del programma installato e della distinta dei componenti assume rilievo. Essa non sostituisce la prova di laboratorio, che permane necessaria e scarsa, e non accerta la sicurezza di alcun prodotto; consente però di condurre uno scrutinio preliminare su popolazioni ampie e di rilevarne i caratteri ricorrenti. Ne deriva un duplice effetto: la selezione dei prodotti sui quali condurre la prova, che è il passaggio oggi mancante fra un criterio di priorità e le risorse disponibili, e una rappresentazione della composizione dei beni destinati alle abitazioni che nessuna rilevazione presso le famiglie potrebbe restituire.

Con riferimento al secondo ordine di intervento (quello di tipo prescrittivo), si tratta di indagare non ciò che l'Agenzia può fare, bensì gli ambiti in cui il suo intervento produce effetto. È questione di selezione: le aree in cui il rischio maturerà non coincidono con quelle su cui gli strumenti esistenti sono calibrati.

A differenza delle attività conoscitive, questi interventi non richiedono capacità nuove: si esercitano mediante scelte, non mediante mezzi, stabilendo come un fatto vada qualificato o a quale condizione un servizio possa essere reso. Ne discende la caratteristica che li contraddistingue: il rinvio di determinate scelte non lascia la questione aperta, la risolve in altro modo. La qualificazione che l'amministrazione non assume sarà determinata dal primo episodio che si presenterà sul mercato; la condizione che non viene posta sarà determinata dall'assetto che si consoliderà altrove.

Due ambiti illustrano queste dinamiche, accomunati dal fatto che in entrambi la vigilanza ordinaria non produce effetto, seppure per ragioni opposte. Nel primo, quello degli agenti AI, il controllo esiste ma è rivolto all'oggetto sbagliato, poiché l'accertamento del corretto funzionamento del programma non intercetta il rischio che si vuole evitare. Nel secondo, quello del dispositivo che ospita l'identità digitale, il controllo non esiste affatto, non appartenendo l'apparato ad alcun soggetto vigilato.

Più nello specifico, non è possibile rendere sicuro un agente prescrivendogli ciò che non deve fare. L'istruzione legittima e quella ostile transitano sul medesimo canale, il linguaggio naturale, e il sistema non dispone di un criterio interno atto a distinguerle: un divieto formulato in quel medium è una regola espressa in un linguaggio padroneggiato dall'attaccante non meno che da chi l'ha formulata. I presidi che resistono sono quelli esterni al modello, operanti sul perimetro di ciò che l'agente può raggiungere: credenziali circoscritte al singolo compito, elenchi chiusi degli strumenti invocabili e delle destinazioni raggiungibili, limiti di importo e di numero delle operazioni, segregazione dell'ambiente di esecuzione, conferma umana obbligatoria per le operazioni irreversibili. Tali presidi resistono in quanto non rimessi al discernimento dell'agente: operano anche ove questi sia stato persuaso per intero.

L'oggetto della sorveglianza, in tale ambito, non è dunque il comportamento del programma, bensì il perimetro delle sue autorizzazioni. Ed è precisamente l'inventario che la distinta dei componenti, estesa ai sistemi addestrati dalle linee guida adottate in sede G7 nel maggio 2026[15], è chiamata a enumerare: i modelli incorporati e le loro versioni, i componenti di recupero delle informazioni, gli strumenti esterni invocabili, i canali attraverso i quali il sistema riceve contenuti in fase di esecuzione. La logica permane quella della distinta, applicata ai permessi anziché ai componenti.

La medesima tecnica prescrittiva si presta a un impiego più diretto, nella forma della condizione d'uso, di cui il portafoglio europeo di identità digitale costituisce l'esempio. La disciplina di prodotto impone al fabbricante di dichiarare

avanzate di intelligenza artificiale per finalità di cibersicurezza, elaborato con ENISA.

15. G7 Cybersecurity Working Group, Software Bill of Materials for AI – Minimum Elements, 12 maggio 2026, elaborato con il contributo dell'Agenzia. La distinta dei componenti relativa ai prodotti è invece requisita vincolante ai sensi dell'allegato I, parte II, punto 1, del regolamento (UE) 2024/2847, circoscritto alle dipendenze di primo livello; l'atto di esecuzione con cui la Commissione può specificarne formato ed elementi, previsto dall'art. 13, par. 24, non è stato ancora adottato.

la durata degli aggiornamenti, ma nulla dispone sugli usi consentiti dopo la scadenza; la disciplina dell'identità certifica la soluzione di portafoglio, ma assume come dato lo stato di sicurezza del dispositivo che la ospita. Subordinare la validità della piattaforma ospite alla permanenza del sistema operativo entro il periodo di supporto dichiarato converte un'informazione che l'ordinamento già impone di produrre in una condizione verificabile dal servizio medesimo. Costituisce l'unica via per raggiungere un terminale che nessuno è in grado di regolare, senza porre obblighi in capo alla persona; e il relativo costo va dichiarato anziché taciuto, poiché comporta che un apparato ancora funzionante cessi, a un dato momento, di poter essere impiegato ai fini dell'identità digitale.

Nell'ambito dell'attività dell'Agenzia entro l'orizzonte del 2030 si colloca un tema non riconducibile ad alcuna delle due categorie sopra rappresentate: la consapevolezza, funzione originaria che l'Agenzia esercita senza intermediazione e che un recente episodio impone di riconsiderare. Fra il 12 e il 15 settembre 2026 Revolut ha reso noto di aver trasmesso a soggetti non autorizzati i dati di circa seicentottanta clienti, comprensivi di numeri di conto, indirizzi di residenza e documenti di identità[16]. Non vi è stata alcuna violazione dei sistemi. Gli attaccanti si sono avvalsi di un indirizzo istituzionale italiano compromesso e hanno formulato richieste che l'istituto era tenuto a evadere, trattandole alla stregua di ordinarie richieste dell'autorità: secondo quanto dichiarato dalla società, esse provenivano da un dominio governativo verificato e recavano valida autenticazione tecnica.

Due circostanze rendono l'episodio istruttivo. La prima è che destinataria dell'inganno non è stata una persona negligente, bensì la struttura professionale di un intermediario vigilato, dotata di procedure dedicate. La seconda è che le verifiche non hanno mancato di funzionare: hanno restituito esito corretto, poiché il mittente era effettivamente un indirizzo governativo autentico. Non si tratta dunque di un controllo eluso, ma di un controllo superato per il tramite di un canale legittimo. Se la verifica fallisce dove è organizzata, specializzata e obbligatoria, non è ragionevole attendersi che il singolo consegua un risultato migliore. Ne discende una conseguenza sul contenuto dell'istruzione, prima ancora che sulla sua intensità. Chiedere al consumatore di riconoscere l'inganno è pretesa che la verosimiglianza dei nuovi attacchi ha reso impraticabile; ciò che può essergli richiesto è la consapevolezza del grado di sofisticazione raggiunto e l'adozione delle procedure che ne limitano l'effetto. Si tratta di una funzione che l'atto istitutivo già attribuisce all'Agenzia, e che va esercitata con maggiore rigore e con destinatari più circoscritti, comprese le imprese di minori dimensioni, allo stato prive di quelle procedure.

La transizione alla crittografia post-quantistica costituisce il caso limite dell'intera logica sin qui rappresentata, in cui l'Agenzia opera da tempo e in posizione non marginale[17]: qui l'intervento precede non soltanto il danno, ma la manifestazione stessa della minaccia. La minaccia non si è manifestata, né è certo il momento in cui si manifesterà. È tuttavia verosimile che, non appena sarà disponibile un elaboratore quantistico di potenza sufficiente, gli algoritmi asimmetrici che assicurano la riservatezza delle comunicazioni, l'autenticità delle firme e l'affidabilità dell'identità digitale cesseranno di offrire protezione. La criticità principale attiene oggi al criterio di priorità. La progressione ordina gli interventi secondo la criticità del soggetto detentore: criterio congruo rispetto alle infrastrutture, ma che diviene discutibile ove applicato agli insiemi informativi riferiti alle persone. Un archivio sanitario privato, un servizio di analisi genetica, una piattaforma che conservi anni di comunicazioni personali non costituiscono infrastrutture critiche e non compaiono in alcuna lista di priorità, pur custodendo dati la cui riservatezza deve permanere oltre l'intera durata della transizione. Il criterio idoneo a correggere questo esito non è estraneo al quadro europeo. La dichiarazione congiunta del gennaio 2025 raccomanda espressamente di redigere la tabella di marcia considerando la sensibilità e il periodo di protezione delle informazioni, e ciò proprio al fine di mitigare il rischio delle condotte di conservazione in attesa di decifratura. Esso non trova però riscontro nella progressione operativa, che continua a ordinare per criticità del detentore. Lo scarto non corre dunque fra il quadro europeo e ciò che qui si propone, bensì fra la raccomandazione e la sua attuazione; ed è su tale scarto che conviene intervenire finché le tabelle di marcia nazionali sono in formazione, poiché il loro consolidamento converte in revisione ciò che oggi costituirebbe un'impostazione.

5. Conclusioni

L'esercizio condotto in queste pagine non ha carattere prognostico. Le date sono pubblicate, gli obblighi sono vigenti ancorché ad applicazione differita, le tecnologie considerate esistono già e non richiedono, per produrre gli effetti

16. Comunicazioni della società rese pubbliche fra il 12 e il 15 settembre 2026; sull'accaduto risultano in corso verifiche della Polizia postale, dell'Agenzia per la cybersicurezza nazionale e della Banca d'Italia.

17. Documento informativo dell'Agenzia "Crittografia post-quantum e quantistica. Preparazione alla minaccia quantistica", luglio 2024; dichiarazione congiunta "Transitioning to Post-Quantum Cryptography", sottoscritta dall'Agenzia unitamente alle omologhe europee su iniziativa dell'ufficio federale tedesco per la sicurezza informatica, gennaio 2025, che istituisce il sottogruppo del Gruppo di cooperazione NIS incaricato di elaborare la tabella di marcia coordinata e raccomanda di considerare la sensibilità e il periodo di protezione delle informazioni; linee guida dell'Agenzia sulle funzioni crittografiche, da ultimo aggiornate nel giugno 2026; documento "Preparing for the Post-Quantum Era: A Call to Action", elaborato in seno al Gruppo di lavoro G7 sulla cybersicurezza su proposta dell'agenzia francese e negoziato nel primo semestre del 2026 con il contributo dell'Agenzia.

descritti, alcuna discontinuità rispetto allo stato attuale. L'unico elemento propriamente prospettico è la loro convergenza: discipline elaborate in tempi diversi, per finalità diverse e prive di reciproco coordinamento, si troveranno entro un quadriennio a insistere sulla medesima persona e sui medesimi oggetti. Guardare al 2030 non significa, dunque, immaginare che cosa accadrà, ma trarre le conseguenze di ciò che è già stabilito nelle norme e osservabile sui mercati. Questa lettura restituisce, più che una previsione sul rischio, un'immagine dell'amministrazione che di quel rischio dovrà rispondere. L'Agenzia giungerà al 2030 titolare di un insieme di competenze che nessun atto ha inteso riconoscere come tale: la certificazione, la vigilanza sui sistemi di intelligenza artificiale e la sorveglianza sui prodotti con elementi digitali le sono state attribuite per ragioni tecniche distinte, ciascuna plausibile nel proprio contesto, e la loro somma consegna all'Agenzia il bene di consumo come oggetto di sicurezza nazionale. Non si tratta di un'estensione rivendicata, ma di un esito che non ha ancora ricevuto una qualificazione istituzionale.

È da qui che discende la particolare condizione descritta nelle pagine precedenti: l'unica amministrazione che possiede le competenze tecniche per accertare la sicurezza di un prodotto è anche l'unica priva di qualsiasi rapporto con chi quel prodotto lo usa; la caratteristica che ha reso praticabile l'intero modello – costruire gli obblighi attorno a soggetti organizzati e identificabili – è la stessa che oggi impedisce di osservare il lato in cui il rischio si produce. Non vi è alcun difetto di diligenza: vi è una strumentazione costruita per un perimetro che si è nel frattempo esteso.

Ne deriva che la domanda utile non riguarda ciò che accadrà, bensì ciò che verrà deciso e quando. Le scelte esaminate – ampliare il punto di osservazione, qualificare i fenomeni prima che il primo caso li qualifichi di fatto, subordinare l'uso di un servizio a un presupposto verificabile – non richiedono poteri nuovi e hanno per contenuto una determinazione, non un mezzo. Queste stesse scelte hanno però tempi di maturazione che le collocano nel periodo corrente e non in quello in cui produrranno effetti.

Ciò che resta genuinamente incerto, dunque, non appartiene al futuro tecnologico ma a quello amministrativo. La domanda, che non può essere rivolta al legislatore, è se l'Agenzia giungerà a quelle date avendo determinato il modo di esercitare le funzioni che le sono state attribuite, oppure avendole soltanto ricevute.

La difficoltà qui descritta non nasce da un difetto di produzione normativa, che è stata abbondante, né da un'inerzia degli apparati che hanno assorbito in pochi anni un carico attuativo senza precedenti; nasce dal fatto che la persona è osservata da ciascuna istituzione secondo la categoria che le è propria (interessato, contraente, pagatore, utente, titolare d'impresa, cittadino) e da nessuna nella sua interezza, mentre i rischi che la riguardano attraversano quelle categorie senza riconoscerle. È la medesima separazione che le due agende europee richiamate in apertura riproducono a un livello superiore e che l'esercizio condotto ha inteso rendere visibile. Riconoscere questa separazione non risolve il problema del riparto, che ha ragioni solide e che nessuna riforma settoriale correggerebbe utilmente; ne costituisce però il presupposto affinché le decisioni assunte nel prossimo quadriennio non risultino, nel 2030, coerenti ciascuna con la propria premessa e complessivamente insufficienti.

GLI AUTORI e COLLABORATORI

Curatore:

Fabio BASSAN
Professore ordinario di Diritto internazionale e Diritto dell'Unione europea presso l'Università degli Studi Roma Tre. Autore di numerose monografie e saggi scientifici, svolge attività di ricerca prevalentemente nei settori della regolazione dei mercati, della tutela dei consumatori e del diritto delle nuove tecnologie.

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.

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.

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

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

Sara PERUGINI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionaria dell'Autorità Garante della Concorrenza e del Mercato.

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

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

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

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

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

Serafina PIANTEDOSI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionaria presso l'Autorità Nazionale Anticorruzione e avvocata.

Francesca PELLICANÒ
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionaria di ruolo dell'Autorità per le Garanzie nelle Comunicazioni.

Rosaria PETTI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionaria di ruolo presso l'Autorità per le Garanzie nelle Comunicazioni e avvocata.

Michela MASTRANTONIO
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre. Funzionaria presso l'Autorità per le Garanzie nelle Comunicazioni e avvocata.

Associazioni di Consumatori

ADICONSUM

ADOC

ADUSBEF

ASSOCIAZIONE CONSUMATORI ACP
consumo lavoro cittadinanza

URT

ASSOUTENTI

Casa del Consumatore

Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti

CITTADINANZATTIVA

CODACONS

CODICI
Centro per i Diritti del Cittadino

CONFCONSUMATORI APS

ICONSUMATORI
Federazione di Associazioni di Consumatori

LEGA CONSUMATORI

MOVIMENTO CONSUMATORI

MOVIMENTO DIFESA del Cittadino

Associazioni di Imprese

AIRU
associazione italiana riscaldamento urbano

asstra
IMPRESE IN MOVIMENTO

CENTROMARCA
Associazione Italiana dell'Industria di Marca

netcomm
IL COMMERCIO DIGITALE ITALIANO

FEDERDISTRIBUZIONE
Imprese. Retail. Futuro.

federfarma

UPA

UTILITALIA
imprese acqua ambiente energia

Imprese

ALLEANZA ASSICURAZIONI

autostrade per l'Italia

mediolanum BANCA

EDISON

FERROVIE DELLO STATO ITALIANE

INTESA SANPAOLO

iren

Opella.

Posteitaliane

TIM

Istituzioni

UNIONCAMERE

CONSUMERS' FORUM

Consumers' Forum è un'associazione indipendente e unica in tutta Europa che dal 1999 riunisce importanti associazioni di consumatori, istituzioni, numerose imprese industriali e di servizi e loro rappresentanze. L'Associazione si pone come luogo di confronto sui diritti dei consumatori e favorisce il "dialogo aperto" tra le parti, promuovendo politiche di sostenibilità consumeristica, con l'obiettivo di costruire un mercato più giusto ed equilibrato e migliorare la qualità di vita dei cittadini.

Consumers' Forum
Via degli Scipioni,8 00192 Roma RM
tel.06-39725486 fax 06-39887519
segreteria@consumersforum.it
www.consumersforum.it

consumforum
@ConsumForum
consumersforumtv
consumers'-forum