10

COLLANA DEL
DIPARTIMENTO
DI ECONOMIA
AZIENDALE

A cura di

MADDALENA RABITTI, FABIO BASSAN

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

Il ruolo delle autorità indipendenti

Roma TrE-Press
2025

Roma Tre
Università degli Studi Roma Tre
Dipartimento di Economia aziendale

COLLANA DEL DIPARTIMENTO DI ECONOMIA AZIENDALE

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

2 *Sindacati in un mondo globale*
Giampiero Bianchi

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

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

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

6 *Profili ragionieristici della contabilità nazionale*
Claudio Columbano

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

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

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

Università degli Studi Roma Tre
Dipartimento di Economia Aziendale

10

COLLANA DEL DIPARTIMENTO
DI ECONOMIA AZIENDALE

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

Il ruolo delle autorità indipendenti

A cura di

MADDALENA RABITTI, FABIO BASSAN

RomaTrE-Press
2025

Collana del Dipartimento di Economia Aziendale
Direttore
Alberto Pezzi

Coordinamento editoriale
Gruppo di Lavoro *Roma TrE-Press*

Impaginazione e cura editoriale
teseo editore Roma teseoeditore.it

Elaborazione grafica della copertina
MOSQUITO mosquitoroma.it

Roma, luglio 2025
ISBN: 979-12-5977-497-2

http://romatrepress.uniroma3.it

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

Collana del Dipartimento di Economia Aziendale

Editorial Policy e descrizione dello scopo della Collana

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

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

La collana accoglie contributi monografici e collettanee.

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

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

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

Consumerism 2024

AUTORI

Andrea AGUGGIA
Dottorando di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma.

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 di Roma Tre.

Marco CAPPAI
Dottore di ricerca in «Mercati, impresa e consumatori» e assegnista di ricerca in Diritto amministrativo presso l'Università degli Studi Roma Tre. Abilitato alle funzioni di Professore universitario di Seconda Fascia nel Settore Concorsuale di diritto amministrativo.

Andrea CARRISI
Ricercatore di Diritto dell'Economia presso l'Università degli Studi "Magna Graecia" di Catanzaro e dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi Roma Tre.

Federico M. GABRICCI
Dottorando di Ricerca in «Mercati, impresa e consumatori» presso l'Università degli Studi di Roma Tre.

Cristiana LAURI
Dottore di ricerca in «Mercati, impresa e consumatori» presso l'Università di Roma Tre, assegnista di ricerca presso l'Università di Macerata e abilitata al ruolo di Professore di Seconda Fascia del Settore Concorsuale di diritto amministrativo.

Federico NESPEGA
Dottorando 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.

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

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

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

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

Maddalena RABITTI
Professore Ordinario di Diritto dell'Economia e componente del collegio dei docenti del dottorato di ricerca in «Mercati, impresa e consumatori» presso l'Università di Roma Tre.

Consumerism 2024

Indice

L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti

Maddalena Rabitti e Fabio Bassan

Sommario. 1. L'AI Act – 2 L'applicazione in Italia: il DDL 1146 – 3. La ricerca Consumerism 2024 – 4. Ipotesi per una collaborazione

1 L'AI Act

Il Regolamento europeo sull'intelligenza artificiale (AI ACT, Regolamento 1689 pubblicato il 13 giugno 2024, d'ora in avanti il "Regolamento") pone l'Unione europea all'avanguardia della regolazione di frontiera sui sistemi di intelligenza artificiale.

Nonostante la velocità dell'evoluzione tecnologica sia decisamente maggiore di quella del legislatore, una regolazione 'per principi' consente di definire il perimetro di gioco e le regole di base. In questa direzione si è mosso il legislatore europeo, riuscendo però solo in parte nell'intento. Per quanto sia certamente migliorabile, il Regolamento è una base su cui costruire l'evoluzione di un welfare europeo continentale che si avvalga dei sistemi di intelligenza artificiale.

Per quanto qui interessa, il Regolamento definisce:

– regole armonizzate per l'immissione sul mercato, la messa in opera e l'uso dei sistemi di IA;
– una classificazione dei sistemi di IA in base ai livelli di rischio (rischio inaccettabile, alto rischio, rischio modesto, rischio specifico per la trasparenza);
– un divieto delle pratiche di IA contrassegnate come inaccettabili (art. 5),
– requisiti specifici e procedure particolari per i sistemi di IA classificati ad alto rischio con i conseguenti obblighi per gli utilizzatori, a tutela soprattutto dei diritti fondamentali;
– regole di trasparenza per i sistemi di IA a 'rischio medio', in cui l'interesse tutelato è quello del mercato;

– regole di trasparenza specifica per alcuni sistemi di IA;
– regole armonizzate specifiche per l'immissione sul mercato di modelli di IA per uso generale;
– modalità di identificazione di possibili rischi sistemici che potrebbero discendere dai sistemi di IA per finalità generali, intendendo per rischio sistemico la possibilità che l'uso dell'IA possa conseguire un impatto significativo sul mercato interno con effetti reali o prevedibili su salute, sicurezza e diritti fondamentali;
– misure a sostegno dell'innovazione, con particolare attenzione alle PMI e alle start up;
– una disciplina sulla governance dell'IA, sul monitoraggio e sulla vigilanza del mercato.

Il Regolamento definisce anche la governance della disciplina, sul piano unionale (artt. 64-69) e nazionale (art. 70).

Lo strumento del regolamento era necessario, in applicazione del principio di proporzionalità, poiché una direttiva, anche di massima armonizzazione, non avrebbe raggiunto l'obiettivo di applicazione immediata di una disciplina che, già nel tempo della sua approvazione, è diventata meno idonea ad affrontare le dinamiche di un mercato in forte evoluzione (un esempio: l'AI generativa al momento in cui il regolamento è stato proposto dalla Commissione non era ancora disponibile sul mercato di massa). In secondo luogo, il Regolamento era lo strumento più idoneo (forse, necessario) per costituire immediatamente l'Ufficio per l'Intelligenza Artificiale presso la Commissione europea, che accentra i poteri in materia di vigilanza sui sistemi di intelligenza artificiale (tra l'altro: monitora l'efficace attuazione del regolamento, può chiedere documentazione sui modelli di IA, valuta la conformità del fornitore dei modelli di IA agli obblighi previsti dal regolamento, può richiedere l'accesso al modello stesso, indaga sui rischi sistemici).

Proprio però perché lo strumento utilizzato è un regolamento UE, i contenuti della norma sono generali, sotto almeno tre profili.

Il primo: per l'applicazione in concreto del Regolamento gli Stati membri devono 'designare' autorità competenti.

Il secondo rileva sul piano della ricognizione delle responsabilità per l'uso di sistemi di intelligenza artificiale, che viene affidata, per il momento, agli Stati membri. Analogamente, quanto all'apparato sanzionatorio e all'adozione di codici di condotta.

Il terzo, più generale, deriva dal fatto che buona parte delle norme del Regolamento non sono *self-executing*. Come è noto, il regolamento UE è direttamente applicabile, ma nelle parti in cui non è *self-executing* non ha effetto diretto, e dunque (tra l'altro) non può essere invocato dinanzi a un giudice.

Si è dunque di fronte a uno dei casi in cui l'esecuzione della norma unionale non spetta all'esecutivo europeo (la Commissione) ma principalmente agli Stati, i quali sono tenuti tra l'altro a comunicare alla Commissione l'indicazione dell'autorità di notifica e dell'autorità di vigilanza del mercato dei sistemi di IA.

2 L'applicazione in Italia: il Ddl 1146

Correttamente, dunque, il governo ha presentato un ddl (1146, recante Disposizioni e delega al Governo in materia di intelligenza artificiale: il "DDL") che analizziamo in questo lavoro nella sua versione originaria, e che non si limita (principalmente nell'art. 18) a designare le autorità competenti per la notifica[1] e la vigilanza del mercato[2] per i sistemi di intelligenza artificiale (rispettivamente, Agid e ACN)[3] ma interviene su una serie di set-

[1] L'art. 3, n. 19 del Regolamento definisce l'autorità di notifica come "l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio". L'art. 28.1 del Regolamento chiarisce che "[c]*iascuno Stato membro designa o istituisce almeno un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio. Tali procedure sono sviluppate nell'ambito della collaborazione tra le autorità di notifica di tutti gli Stati membri*". Tali autorità, tra l'altro, devono garantire obiettività, imparzialità, prevenire conflitti di interesse (art. 28.3) e garantire separazione tra attività istruttoria e decisionale (28.4)

[2] L'art. 3 n. 26 del Regolamento definisce come "autorità di vigilanza del mercato" l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti. Il D. Lgs. 157/2022 ha individuato l'Agenzia delle Dogane e dei Monopoli e la Guardia di Finanza come autorità incaricate.

[3] L'articolo 18.1 del ddl stabilisce che:

"a) l'AgID è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, fatto salvo quanto previsto dalla lettera b). L'AgID provvede, altresì, a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea;

b) l'ACN, anche ai fini di assicurare la tutela della cybersicurezza, come definita dall'articolo 1, comma 1, del decreto-legge14 giugno 2021, n.82, convertito, con modificazioni, dalla

tori (tra gli altri la sanità, il lavoro, le professioni intellettuali, la pubblica amministrazione, la giustizia, la sicurezza nazionale) in cui definisce il perimetro dell'intervento della politica (industriale si definiva, una volta).

2.1 Le autorità di vigilanza

Si può comprendere anche, in quest'ottica, perché le autorità designate (ex art. 70 del Regolamento) non siano autorità indipendenti, ma agenzie governative[4]. La scelta peraltro è coerente con quella del legislatore europeo, che per l'attuazione e il coordinamento della disciplina non ha costituito un'agenzia europea ma piuttosto un ufficio[5], presso la Commissione europea (art. 64 del Regolamento), la quale è assistita da un gruppo di esperti scientifici indipendenti (art. 68) e da un Comitato europeo per l'intelligenza artificiale (articoli 65 ss.)[6], che si avvale a sua volta di un forum consultivo

legge 4 agosto 2021, n.109, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN è, altresì, responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza;
c) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale".

[4] La questione, evidentemente, è tra le più dibattute, al momento: il Regolamento prevede che l'attività delle autorità di notifica e vigilanza sia imparziale (principio che caratterizza l'operato della pubblica amministrazione: art. 97 Cost.) ma anche indipendente. L'indipendenza è da valutare in relazione alla nomina dei componenti, ma deve essere anche finanziaria, strumentale e infrastrutturale (art 70.3), nonché funzionale, riguardante cioè l'attività e l'adozione di decisioni da parte delle autorità.

[5] L'Ufficio per l'IA è la struttura attraverso la quale la Commissione persegue i compiti relativi allo sviluppo delle capacità dell'uomo nel settore dell'IA (art. 64. 1); esso partecipa come osservatore al Comitato europeo per l'IA (art.65), esamina le proposte di raccomandazioni o le richieste di pareri a esso inoltrate, anche con riferimento all'elaborazione di codici di condotta e di best practices (art.64, 1, lett. e, i), nonché sulla valutazione e sul riesame del regolamento (art. 66, d, ii) riceve segnalazioni e consulenze dal panel di esperti indipendenti.

[6] Il Comitato contribuisce al coordinamento tra le autorità nazionali responsabili, fornisce consulenze, raccoglie conoscenze e best practices, formula raccomandazioni su questioni attinenti all'attuazione del regolamento, sulla valutazione e sul riesame del medesimo, sulla necessità di modificare l'allegato III, ed in genere favorisce la alfabetizzazione in tema di

(art. 67). Il controllo (ad opera dell'Ufficio IA a livello europeo, e delle agenzie/autorità, a livello nazionale) quindi è tecnico, ma le scelte (la "strategia nazionale per l'IA", di cui al Capo III del DDL) restano politiche.

La legittimità della scelta peraltro, nonostante un parere non ostativo del GPDP[7] è tuttora oggetto di un acceso dibattito, anche in dottrina, che muove intorno all'indipendenza (dal mercato e dal Governo) richiesta, dal Regolamento, per le autorità designate, che dunque dovrà essere garantita su un piano sostanziale ma anche formale[8]. Ciò vale soprattutto per l'autorità di vigilanza sui sistemi di IA, essendo quella relativa alla notificazione attività soggetta alla sola discrezionalità tecnica.

Le opzioni fornite in tal senso sulla base della formulazione aperta dell'art. 70 del Regolamento sono state numerose; in base a quella prevalente, almeno al momento, nel dibattito dottrinale, in alternativa alla designata ACN, l'autorità competente per la vigilanza potrebbe essere l'autorità nazionale per la protezione dei dati personali (in ragione dell'indipendenza, della riserva di competenza e dell'approccio antropocentrico).

2.2 La vigilanza sul mercato

Dunque, se la scelta adottata nel DDL è condivisibile quanto alla notifica dei sistemi di intelligenza artificiale, con l'Agid, che assume il ruolo di agenzia di 'notificazione', non solo quanto all'intelligenza artificiale ma più in generale (dalle piattaforma di e-procurement alla data governance[9],

IA, coopera con le autorità competenti o con i paesi terzi, riceve le istanze degli Stati membri su segnalazioni qualificate (art. 66).

[7] Nel parere reso sul DDL il 2 agosto 2024, il GPDP ritiene, quanto alla collaborazione ex art. 18.2, che "[…] è anche opportuno prevedere la partecipazione del Garante al Comitato di coordinamento di cui all'articolo 18, c.2, secondo periodo, per realizzare pienamente quella leale cooperazione tra autorità competenti prevista dall'AI Act. Declinando in maniera più articolata le implicazioni di tale cooperazione, è inoltre opportuno integrare l'articolo prevedendo, in fine, che AgID e ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati, richiedendo altresì il parere dell'Autorità rispetto a fattispecie, al loro esame, che coinvolgano aspetti di protezione dei dati. Il Garante trasmetterà, per parte sua, elementi informativi in ordine a profili di competenza di AgID o ACN suscettibili di emergere nella trattazione di propri procedimenti".

[8] In senso critico sulla scelta, tra gli altri, A. Pajno, *La governance dell'IA tra regolamento europeo e disciplina nazionale*, ASTRID Rassegna 13/24.

[9] Quanto alla data governance, ci riferiamo al decreto legislativo 7 ottobre 2024, n. 144, che adegua la normativa nazionale al regolamento (Ue) 2022/868 del Parlamento europeo

per le quali peraltro sono auspicabili forme di collaborazione strutturale con ANAC, che gestisce la piattaforma unica della trasparenza nonché la banca nazionale dei contratti pubblici), e si candida dunque a questa funzione in modo strutturale sui mercati digitali (web2, ma anche web3), qualche precisazione merita forse la disciplina sulla vigilanza. Si tratta infatti di vigilanza sui sistemi di intelligenza artificiale, che operano in modo trasversale, su tutti i mercati, anche quelli su cui vigilano autorità indipendenti.

Può essere quindi opportuno sia definire in modo preciso nella norma nazionale il contenuto dell'attività di vigilanza attribuita all'ACN, sulla base di quanto disposto dal Regolamento, sia precisare i termini della collaborazione tra le autorità designate e le altre autorità indipendenti – almeno di quelle che tutelano i diritti fondamentali, come previsto nell'art. 77 del Regolamento – collaborazione al momento indicata forse in modo troppo laconico nell'articolo 18.2 del DDL[10].

---

e del Consiglio del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (Ue) 2018/1724. L'Agenzia per l'Italia Digitale viene indicata nel decreto come l'autorità responsabile per lo svolgimento dei compiti relativi alla procedura di notifica dei soggetti che intendono offrire servizi di scambio di dati e alla successiva comunicazione alla Commissione europea. All'AgID spetta anche il compito di assicurare il rispetto, da parte dell'intermediario, delle condizioni per la fornitura dei servizi compresa l'erogazione delle sanzioni. AgID è indicata inoltre quale autorità competente a tenere il registro delle organizzazioni di data altruism, monitorarne le attività e a assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo di specifiche categorie di dati; dovrà anche provvedere all'implementazione delle funzioni previste per lo "sportello unico", estendendo il punto d'accesso garantito dal catalogo nazionale dei dati aperti, al fine di facilitare l'accesso ai dati da parte delle imprese e della società civile, al fine di promuovere innovazione e crescita.
Si tratta di attività che AgID dovrà assolvere assicurando imparzialità, trasparenza, coerenza, affidabilità e tempestività, salvaguardando la concorrenza leale e la non discriminazione. Compiti che dovranno essere svolti in stretta e leale cooperazione con le altre autorità nazionali competenti e in particolare con l'Autorità garante per la protezione dei dati personali, l'Agenzia per la cybersicurezza nazionale e l'Autorità garante della concorrenza e del mercato.

[10] L'articolo 18.2 del DDL precisa che "Le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo. A quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima. Ai componenti del

Del resto, gli articoli 4, 23 e 24 del DDL hanno per oggetto l'informazione e i contenuti testuali, fotografici, audiovisivi e radiofonici, nonché il diritto d'autore (materie di competenza AGCom) e l'articolo 4 anche la protezione dei dati personali (competenza del GPDP), disciplinata peraltro ulteriormente, in modo compiuto, dal Regolamento. Quindi, il tema della collaborazione almeno con queste due autorità, che vigilano anche sul rispetto di diritti fondamentali, si pone già nell'immediato.

In modo parzialmente differente il tema si pone però anche per il rapporto tra le agenzie designate e le autorità che vigilano sui mercati (AGCM, ART, ARERA, CONSOB, BI) o sull'operato della pubblica amministrazione (ANAC).

La ripartizione delle competenze non può essere valutata in astratto, ma in concreto. Se l'agenzia designata per la vigilanza sui sistemi di IA è l'ACN, perché il profilo cardine della tutela è individuato nella sicurezza (scelta del tutto legittima e coerente con la tassonomia del Regolamento IA, che vede nella sicurezza l'obiettivo-cardine), allora la vigilanza sui sistemi di IA sarà garantita da ACN, quanto alla sicurezza, in via esclusiva. L'ACN potrebbe però anche – su richiesta – fornire assistenza e consulenza alle altre autorità, alle quali resterebbe la competenza quanto alla valutazione del precipitato dell'uso dell'IA sui mercati. Qualora l'uso di sistemi di IA abbia favorito (o addirittura consentito) comportamenti anticoncorrenziali, discriminatori, iniqui, o abbia orientato (in modo illecito o comunque non trasparente) decisioni delle imprese o dei consumatori, o ancora abbia violato il diritto alla protezione dei dati personali o il diritto all'informazione, saranno le autorità di settore competenti a valutare sia i comportamenti e gli effetti sul mercato, sia l'adeguatezza, rispetto ai mercati vigilati, dei requisiti di trasparenza e spiegabilità. Questo, sulla base sia della banca dati custodita da AGiD - che dovrebbe quindi garantire strutturalmente una collaborazione con ANAC - sia della verifica di ACN quanto alla sicurezza.

L'esigenza di una 'lex finium regundòrum' nasce dalla prassi, che in Italia ha visto a volte autorità indipendenti impegnate in contenziosi tra loro, sviluppati nel corso di più di un decennio, per ottenere dai giudici una definizione del perimetro delle rispettive competenze, quando questo non era chiarito a priori dal legislatore[11]. Riteniamo opportuno evitare sin d'ora

Comitato non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati".

[11] Ci si riferisce qui alla copiosa giurisprudenza sulle pratiche commerciali scorrette, che ha visto la giustizia amministrativa impegnata per anni nella perimetrazione della compe-

che ciò accada anche con riferimento ai sistemi di intelligenza artificiale, e potrebbe non essere adeguato a tal fine un atto delegato successivo[12].

2.3 Vigilanza 'trasversale' e matrice regolatoria

Per inquadrare il tema riteniamo occorra partire dalla 'matrice regolatoria'. Vigilanza e regolazione dei mercati sono organizzati 'a matrice'[13]. Vi sono le autorità competenti a vigilare e (molte di esse anche) a regolare mercati 'verticali' (banche, assicurazioni, mercati finanziari, energia/gas/rifiuti, comunicazioni elettroniche, trasporti) e autorità competenti a vigilare 'orizzontalmente' su tutti i mercati, in modo trasversale (concorrenza, protezione dei dati personali, e ora, anche intelligenza artificiale). Molte di queste autorità indipendenti hanno origine 'unionale': sono sorte su istanza del legislatore europeo; altre pur avendo origine diversa hanno visto poteri e funzioni modificate in modo rilevante dalle norme europee. Tutte hanno sviluppato competenze specifiche sui mercati su cui vigilano e (quelle 'verticali') su cui regolano.

Tutte le autorità di vigilanza e (alcune anche di) regolazione operano su mercati su cui sistemi di intelligenza artificiale stanno modificando velocemente parametri di riferimento e rapporti di forza tra gli operatori. Ognuna di queste è evidentemente la più idonea a intervenire sul mercato che già vigila e in alcuni casi, regola. S'impone pertanto un coordinamento con l'ACN, autorità trasversale, sui sistemi di intelligenza artificiale.

L'intervento di vigilanza peraltro, su questi mercati, è rilevante solo se produce effetti immediati: di qui lo sviluppo recente ma continuo degli strumenti cautelari attivabili dalle autorità indipendenti.

L'intervento regolatorio invece ha tempi diversi, e si sviluppa con modalità di co-regolazione, realizzata recentemente secondo i principi della 'regolazione partecipata'[14], adottati peraltro anche dal Regolamento IA (artt.

tenza tra AGCM e AGCom.

[12] L'articolo 22 del DDL prevede deleghe al governo per l'adozione di uno o più decreti legislativi per l'adeguamento della normativa nazionale al Regolamento per varie materie; tra queste peraltro non v'è la definizione dei termini della collaborazione tra autorità designate e le altre "autorità od organismi designati" ex art. 77 del Regolamento. La delega propone peraltro notevoli e ulteriori quesiti, per i quali si rinvia nuovamente a F. Pajno, cit.

[13] F. Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia – La sovranità perduta sui servizi*, Rubbettino, 2019.

[14] F. Bassan, *Digital Platforms and Blockchains: The Age of Participatory Regulation*, European Business Law Review 2023/7, pp. 1103-1132.

56 e 57, ma anche 95 ss.), secondo i quali le autorità collaborano con il mercato per sviluppare la tecnologia in modo coerente con i diritti fondamentali e con i contenuti minimi del welfare europeo continentale, delineati poi in atti di soft law (linee guida, standards tecnici, codici di condotta) e di hard law (atti normativi, di secondo livello). Sappiamo peraltro ormai che soft law e hard law non sono in antitesi tra loro, ma costituiscono i gradini di una scala, che le norme salgono, e scendono[15].

2.4 La vigilanza sui sistemi di IA, in concreto

Sulla base di queste premesse, decisivo diventa, nel DDL, individuare sia il perimetro dell'attività dell'ACN quanto alla vigilanza sui sistemi di intelligenza artificiale, sia l'eventuale coordinamento tra l'ACN e le autorità indipendenti di vigilanza (e regolazione) sui mercati: quelle che tutelano diritti fondamentali da un lato, in relazione alle quali dunque, l'uso di sistemi di IA è per definizione 'ad alto rischio' e quelle che tutelano i mercati, dall'altro, in relazione ai quali il rischio è 'medio'. Nella versione attuale della norma, questi elementi non sembrano sufficientemente chiari.

Infatti, l'autorità di vigilanza sul mercato (l'ACN, dunque), ai sensi del Regolamento, vigila sul mercato, previene le violazioni relative alle pratiche vietate (ex art. 5 del Regolamento), effettua prove in condizioni reali per i sistemi di IA sottoposti a controllo (art. 76), riceve la segnalazione di incidenti gravi (art. 73), in relazione ai quali deve informare sia la Commissione, sia le autorità o gli organismi pubblici nazionali di cui all'art. 77.1 ("*che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, in relazione all'uso dei sistemi di IA ad alto rischio*") e adotta misure adeguate, esercitando poteri significativi: tra l'altro, può accedere al codice sorgente del sistema di IA ad alto rischio (art. 74.13).

La cooperazione tra autorità di vigilanza del mercato e le autorità/organismi pubblici ex art. 77 (i.e. le autorità di vigilanza e regolazione che tutelano diritti fondamentali) è confermata dall'art. 79, che impone alla prima di informare queste ultime e cooperare ogni volta che ritenga che un sistema di IA presenti un rischio per uno dei diritti fondamentali su cui queste vigilano.

[15] F. Bassan, *Corso di diritto internazionale dell'economia e dei mercati*, Giappichelli, Torino, p. 345.

2.5 Rapporto tra vigilanza su IA e autorità ex art. 77 del Regolamento

Le autorità (o organismi pubblici) ex art. 77 possono chiedere comunque documentazione agli operatori, se è necessario per l'adempimento dei loro mandati e nei limiti della loro giurisdizione (ancora, art. 77).

Anche queste autorità devono essere individuate dagli Stati membri, e il relativo elenco deve essere notificato alla Commissione europea e agli altri Stati membri, e dev'essere poi aggiornato periodicamente.

Tra queste, il Regolamento sembra indicare in modo espresso il Garante per la protezione dei dati personali come autorità competente per i sistemi di IA ad alto rischio elencati nell'allegato III, punto I, nella misura in cui tali sistemi siano utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia, e per i sistemi di IA ad alto rischio elencati nell'allegato III, punti 6, 7 e 8.

Rientra tra le autorità ex art. 77, certamente, anche l'AGCom, competente (anche) in materia di informazione.

Sembra dunque opportuno redigere sin d'ora almeno l'elenco delle autorità indicate ex art. 77 del Regolamento, nel DDL o in altro strumento, unitamente all'indicazione delle due autorità designate per la notifica e la vigilanza sul mercato, e delegificare le forme di aggiornamento dell'elenco. È opportuno anche indicare sin d'ora le modalità di coordinamento, sia con le autorità ex art. 77 del Regolamento sia con le altre autorità.

3 La ricerca Consumerism 2024

Questa ricerca si pone l'obiettivo di proporre soluzioni, partendo dall'esperienza che le autorità indipendenti hanno sviluppato, sino ad oggi, in materia di intelligenza artificiale, verificare quali possono essere in concreto, gli strumenti per disciplinare i mercati (ivi inclusi gli standard tecnici, linee guida, codici di condotta), i punti di contatto, le modalità di cooperazione. Ciò, si ripete, anche per evitare che, nell'attuale silenzio della norma, l'individuazione di tali modalità sia affidata alla giurisprudenza amministrativa.

3.1 IA e impatto sui consumatori: gli strumenti di tutela delle autorità indipendenti

Per adeguare le regole sui mercati vigilati, le autorità indipendenti possono adottare gli strumenti di hard e soft law già sperimentati, anche

secondo i meccanismi del circolo regolatorio[16], e le forme della regolazione partecipata[17].

In termini generali, la trasparenza (comprensibilità e prevedibilità delle decisioni), responsabilità (controllo e supervisione degli operatori sulle attività dell'IA) e non discriminazione (prevenzione delle pratiche discriminatorie) possono essere garantite con soluzioni e tecniche di disciplina del mercato che prevedono standard tecnici, codici di condotta, sandbox regolamentari, per inserire una mappatura dei sistemi di IA che consenta al mercato di: identificare quelli vietati, valutare i rischi differenziando quelli alti (tra gli altri, la selezione del personale) da quelli con minor impatto (ad esempio l'uso di un chatbot per semplificare il customer care); adottare misure di mitigazione per assicurare che i sistemi siano privi di bias e discriminazioni; adottare piani di emergenza adeguati; garantire la trasparenza, anche mediante la tracciabilità delle decisioni algoritmiche (ad esempio, mediante l'utilizzo della blockchain), che consenta di contestarle; garantire rigorose misure per la protezione dei dati personali, in conformità al GDPR, quali la crittografia dei dati, l'anonimizzazione, politiche di accesso rigorose; garantire la formazione continua delle imprese, in relazione agli aspetti tecnici, etici, normativi; indicare procedure per il monitoraggio e la revisione periodica dei sistemi di IA adottati.

Evidentemente, ogni settore ha le sue specificità, che possiamo sintetizzare come segue.

3.2 L'impatto dell'AI nei diversi settori

In ciascuno dei settori (verticali) regolati, così come per le autorità con competenze orizzontali, trasversali (AGCM, GPDP) si pone il tema dell'utilizzo dei sistemi di intelligenza artificiale per vigilare (SupAI) e regolare (RegAI) i sistemi IA utilizzati dagli operatori vigilati.

a) protezione dei dati personali (GPDP)

L'articolo 16 TFUE (protezione dei dati personali) è una delle basi giuridiche del Regolamento; costituisce pertanto un parametro di legittimità della sua applicazione. Al GDPR, del resto, il Regolamento in molti casi si sovrappone, in altri si integra, in altri ancora si allontana, creando questioni interpretative (*infra*, Cappai), rispetto alle quali, deve dedursi, la riserva di competenza del GPDP (art. 74.8 del Regolamento) fa prevalere, tra gli interessi in gioco, quello degli utenti/consumatori alla protezione dei dati

[16] *Supra*, nota 14.

[17] *Supra*, nota 13.

personali. In sintesi, nel conflitto che già si intravede tra *product safety approach* e *rights based approach*, a prevalere dovrebbe essere il secondo. Da qui anche, la proposta del GPDP – nel parere del 2 agosto 2024 – di sostituire i commi 2 e 3 dell'articolo 4 del DDL con una norma generale che affermi un "vincolo generale di conformità dei trattamenti di dati personali funzionali a sistemi di i.a. alla disciplina rilevante in materia [di privacy]".

Non si pone in dubbio, peraltro, il fatto che il GPDP costituisca una delle autorità che debba essere indicata nel DDL come "autorità nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali" (ex art. 77 del Regolamento). Gli interventi recenti del GPDP su OpenAI (*infra*, Cappai) sono del resto un esempio dei vantaggi (molti) e dei limiti (pochi) di un intervento del Garante sui sistemi di IA, condotto prima della pubblicazione del Regolamento, e dunque nei limiti del perimetro delle competenze all'epoca attribuitegli.

b) informazione e comunicazione (AGCom)

Quanto ai profili dell'informazione e dell'audiovisivo, il DDL 1146 interviene direttamente (art. 23) con modifiche al decreto legislativo 8 novembre 2021, n. 208 (TUSMA, Testo unico dei servizi di media audiovisivi), per vietare metodologie e tecniche che consentono di manipolare in maniera non riconoscibile allo spettatore il contenuto di informazioni "attraverso l'utilizzo di sistemi di intelligenza artificiale" (modifica all'Articolo 6, comma 2, lett. e) del TUSMA), o imporre obblighi informativi (modifica all'art. 40-bis del TUSMA) cui vengono assoggettate anche le piattaforme per la condivisione di video (VSP) (art. 42 TUSMA).

Analogamente, il DDL prevede modifiche alla legge sul diritto d'autore per escludere la tutela autoriale dell'opera generate con l'intelligenza artificiale.

Anche l'AGCom dovrebbe essere una delle autorità indicate nel DDL come "autorità nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali" (ex art. 77 del Regolamento).

In alcune sue comunicazioni, il BEREC[18] ha individuato tra le applicazioni più significative di sistemi di intelligenza artificiale nel settore: la pianificazione e l'aggiornamento della rete e della capacità trasmissiva; la modellazione, previsione e propagazione dei canali; l'ottimizzazione della

[18] "Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation", giugno 2023.

qualità del servizio e classificazione del traffico; la condivisione dinamica dello spettro; l'ottimizzazione della qualità del servizio e classificazione del traffico; il rilevamento delle minacce e ottimizzazione della sicurezza di reti e servizi; il rilevamento e prevenzione delle frodi.

c) settori bancario, assicurativo, mercati finanziari

Le applicazioni dei sistemi IA sono simili nei settori bancario, assicurativo e finanziario, con alcune specificità. Ad esempio, sistemi di IA possono essere utilizzati per: rilevare frodi (identificare transazioni sospette, rilevare attività fraudolente in tempo reale, adottare modelli predittivi per individuare anomalie); prestare servizi di consulenza finanziaria personalizzata; valutare il rischio di credito, di nuovo mediante modelli predittivi; automatizzare i processi, per migliorare l'efficienza operativa; analizzare i dati dei clienti per offrire servizi su misura.

Decisivo è anche il ruolo delle autorità di settore, tra le più pronte a utilizzare la tecnologia per vigilare e regolare (SupAI e RegAI) nonché ad applicare i principi della regolazione partecipata[19].

d) trasporti (ART)

Nei trasporti, sistemi di intelligenza artificiale possono consentire di: ottimizzare i flussi di traffico e ridurre congestioni e tempi di attesa; sviluppare la manutenzione predittiva, migliorando l'efficienza e prevenendo interruzioni improvvise; gestire la sicurezza, monitorando i sistemi di sicurezza, identificando comportamenti anomali o potenziali rischi (come incidenti o guasti tecnici) e intervenendo in tempo reale; migliorare l'esperienza degli utenti, monitorandone il feedback, ottimizzando gli orari di servizio, fornendo assistenza personalizzata e prevedendo le esigenze dei passeggeri; automatizzare la verifica della conformità alle regole (es. monitoraggio del rispetto delle tariffe, dei contratti di servizio o dei diritti dei passeggeri) e l'adozione di sanzioni.

e) concorrenza (AGCM)

L'AGCM si occupa già di comportamenti delle imprese che, mediante uso di sistemi di intelligenza artificiale, incidono sugli assetti concorrenziali e sulla tutela dei consumatori (ad esempio: generazione automatica di false recensioni, pubblicità occulte, nuove forme sofisticate

[19] Si veda ad esempio: M. Doria, F. Bassan, M. Rabitti, A. Sciarrone Alibrandi e U. Malvagna, *Caratteristiche degli smart contracts*, Quaderni della Banca d'Italia – Occasional Papers, n. 863, pp. 1-86.

di attacchi di phishing, pubblicità manipolative) e a tal fine si è dotata di una "Unità Data Science". Rilevante è anche il possibile uso dell'AI da parte di AGCM per la vigilanza sui mercati.

f) energia (ARERA)

La vigilanza sulla sicurezza delle infrastrutture, in relazione ai sistemi di intelligenza artificiale, è funzione prioritaria dell'ARERA, che dovrà quindi attrezzarsi per una RegAI adeguata.

Altri usi di IA nel settore sono relativi alle piattaforme che utilizzano l'IA per ottimizzare il funzionamento degli impianti di climatizzazione, migliorando l'efficienza energetica; integrare contemporaneamente i dati ambientali, energetici, meteorologici e di prezzo dell'energia per regolare dinamicamente gli impianti in tempo reale e assicurare che essi operino in modo ottimale.

Rilevante è anche l'utilizzo dell'IA da parte dell'ARERA(SupAI), ad esempio per migliorare l'accesso e le funzionalità del call center dello Sportello.

g) Pubblica Amministrazione (ANAC)

Nell'ambito della transizione digitale della PA la riforma dei contratti pubblici (d. lgs. 36/2023) ha previsto un Banca Dati Nazionale dei Contratti Pubblici (BDNCP), che l'ANAC ha reso già operativa. L'articolo 30 del d. lgs. consente l'utilizzo di sistemi di intelligenza artificiale per assumere decisioni che però devono conformarsi ai tre principi di conoscibilità e comprensibilità, non esclusività della decisione algoritmica e non discriminazione algoritmica. A questi si aggiunge il principio della "riserva di umanità della scelta" (*human in the loop*), che tutela la discrezionalità della scelta dell'Amministrazione, codificando la prassi giurisprudenziale consolidata (a partire dalla sentenza 881/2020 del Consiglio di Stato).

L'integrazione tra la BDNCP e la Piattaforma Unica della Trasparenza consentirà all'ANAC di rendere fruibile una mole significativa di informazioni cui l'uso di sistemi di intelligenza artificiale può attribuire valore e utilità. Ad esempio, per redigere modelli di bandi di gara che tengano conto delle migliori prassi; per prevedere i costi complessivi di un'opera; per creare chatbox che facilitino il rapporto tra stazione appaltante e imprese; per assistere la Commissione di gara nella scelta della migliore offerta.

Il DDL 1146 sull'intelligenza artificiale si occupa espressamente (art. 13) dell'uso dell'intelligenza artificiale nella Pubblica Amministrazione, indicandola come meramente strumentale e di supporto all'attività provvedimentale.

4 Ipotesi per un coordinamento

Sulla base di quanto premesso, è ragionevole ipotizzare una modifica dell'articolo 18 del DDL, nel senso di:

(i) prevedere una procedura d'urgenza

(ii) conferire espressamente alle autorità nazionali per l'intelligenza artificiale (AgID e ACN), un ruolo di consulenza a favore:
a. della Pubblica amministrazione,
b. delle autorità nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali ai sensi dell'art. 77 del Regolamento, e
c. delle altre autorità indipendenti, nonché

(iii) prevedere una collaborazione strutturale tra:
a. le autorità nazionali per l'intelligenza artificiale, (rispettivamente, AGiD per la notifica e ACN per la vigilanza sul mercato) e
b. le autorità nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali ai sensi dell'art. 77 del Regolamento.
Tale collegamento strutturale potrebbe riprendere la forma di quello (Joint Committee) che applicano da anni le tre ESAs (ESMA, EIOPA e EBA) con riferimento alla tutela dei consumatori,

(iv) prevedere un ruolo di consulenza dell'ACN per le autorità (quelle notificate ex art. 77 ma anche le altre, che vigilano sui mercati) che ne facciano richiesta.

Marco Cappai

Protezione dei dati personali e intelligenza artificiale: quale *governance*?

Il presente contributo, dopo aver descritto il rapporto intercorrente tra Regolamento IA e GDPR, e dopo aver esaminato la governance *apprestata dal nuovo quadro regolatorio sull'intelligenza artificiale, si sforza di individuare, anche alla luce della più recente attività di* enforcement *del Garante privacy, l'assetto istituzionale ottimale sul piano del diritto interno. Nel commentare le scelte compiute nel d.d.l. IA, si ricerca, in particolare, una formula allocativa dei pubblici poteri in grado di preservare il ruolo di custode del diritto alla protezione dei dati personali affidato al GPDP, senza per questo menomare gli obiettivi, chiaramente anche di* policy*, che sembrano emergere dal cantiere normativo in corso.*

1 Il rapporto tra Regolamento IA e Gdpr

Il Regolamento (UE) 2024/1689 del 13 giugno 2024 "*che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*" ("**Regolamento IA**") si radica sulla competenza di ravvicinamento delle disposizioni nazionali che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno (art. 114 TFUE), nel pieno rispetto dei valori europei, in primo luogo quello della protezione dei dati personali (art. 16 TFUE). In una materia come l'IA, invero, la frammentazione del quadro giuridico di riferimento produr-

rebbe due principali conseguenze negative. In particolare, la stratificazione di una moltitudine di regimi nazionali differenziati sullo stesso fenomeno determinerebbe: i) un sistema di tutele a macchia di leopardo; ii) un disincentivo all'innovazione (conss. nn. 8 e 9).

Proprio per questa ragione il Regolamento ha optato per un approccio di uniformazione di natura orizzontale. Pone dei requisiti minimi che, ancorché scalari [Sistemi di IA con rischi minimi o nulli: non regolati < Sistemi di IA con rischi limitati: sottoposti a soli obblighi di trasparenza < Sistemi di IA con rischi elevati: soggetti a più pervasivi poteri di controllo preventivo e vigilanza *ex post* < Utilizzi dei sistemi di IA che pongono rischi inaccettabili: sempre vietati], sono uniformi su tutto il territorio dell'Unione e ineriscono, essenzialmente, all'affidabilità (*trustworthiness*) della tecnologia. Tale anima del regolamento riflette un *product safety approach* e, non a caso, si intreccia, in larga parte, con la disciplina europea in materia di sicurezza dei prodotti[20].

Al contempo, la protezione dei "valori europei" rappresenta una dichiarata finalità del Regolamento, che intende coniugare il carattere dell'affidabilità con quello dell'"antropocentrismo" della tecnologia (cons. 1 e art. 1), al fine di assicurare che l'IA sia rispettosa dei diritti fondamentali (*rights based appraoch*).

Tra questi, quello alla riservatezza dei dati personali (artt. 16 TFUE e 8 CDFUE) occupa, senza dubbio, un ruolo preminente, come del resto già riconosciuto, in sede internazionale, dall'OECD[21] e, prima ancora, dall'Independent High-Level Expert Group on Artificial Intelligence nominato dalla Commissione europea[22].

Da ultimo, anche le Autorità di protezione dei dati personali del G7 hanno evidenziato che "*many AI technologies, including generative AI, are based on the processing of personal data, which can subject natural persons to unfair stereotyping, bias and discrimination even when not directly processing their respective personal data. This, in turn, may influence larger societal processes with deep fakes and disinformation. Consequently, data protection and the need to protect the right to privacy are more critical than ever*"[23].

[20] M. Almada - N. Petit, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *CMLRev*, n. 62(1)/2025, 85 ss.

[21] *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2024, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, § 1.2.a.

[22] *Ethics Guidelines for Trustworthy AI*, 8 aprile 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>.

[23] *Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI*, 11 ottobre

Coerentemente con la descritta impostazione *rights based*, il Regolamento "*non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione del diritto dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati*" (cons. 157), prevedendo espressamente che "*il diritto dell'Unione in materia di protezione dei dati personali … si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento*". Resta dunque "*impregiudicat*[o] *il regolamento (UE) 2016/679*", fatte salve le previsioni specifiche poste, in punto di trattamento dei dati personali, dal Regolamento. In particolare, l'art. 2, § 7 fa esplicito riferimento agli artt. 10, § 5 e 59, su cui si tornerà *infra*.

Tra la disciplina dell'IA e la tutela della privacy sussistono tre principali tipologie di rapporto:

a) **Sovrapposizione/Duplicazione:** in non pochi casi il Regolamento IA e il GDPR convergono su aspetti specifici, regolando, sotto diversi e complementari punti di vista, il medesimo fenomeno. Si pensi al diritto dell'interessato, sancito all'art. 22 GDPR, "*di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Come intuibile, decisioni automatizzate di questo genere hanno tipicamente luogo tramite sistemi di IA. Proprio per tale ragione, il cons. 10 del Regolamento IA precisa che, in aggiunta a quanto previsto nel regolamento stesso, "*gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione*". Ancora, l'affidabilità dei sistemi di IA è garantita anche attraverso "*misure tecniche e organizzative*" (art. 15, § 4) e "*misure volte a prevenire … gli attacchi alla riservatezza*" (art. 15, § 5), le quali si affiancano, senza sostituirle, alle cc.dd. "*misure di sicurezza*" di cui all'art. 32 e cons. 83 del GDPR. Per fare un ulteriore esempio, poi, così come, in caso di c.d. *data breach*, entrano in azione i presidi di cui all'art. 33 GDPR, il Regolamento IA delinea un obbligo di "*condivisione di informazioni su incidenti gravi*" (art. 73), avendo cura di precisare, nella parte definitoria, che costituisce "*incidente grave*", *inter alia*, "*la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali*" (art. 3, n. 49, lett. *c*).

2024, <https://www.gpdp.it/garante/document?ID=10063176>, § 6.

In tutti questi casi, dunque, i due plessi disciplinari si applicano in via cumulativa e parallela;

b) **Integrazione:** nel prendere atto delle descritte sovrapposizioni, in taluni casi il legislatore europeo ha cercato, per esigenze di razionalizzazione e semplificazione del sistema, di tracciare un rapporto di integrazione tra le due discipline. Tale operazione coinvolge tanto la parte del Regolamento caratterizzata da un *product safety approach* (cfr. ad es. cons. 81 e art. 8, § 2), tanto, per ciò che qui rileva, la componente espressione di un *rights based approach*. Per fare un esempio significativo, le valutazioni d'impatto sui diritti fondamentali (FRIA) per i sistemi di IA ad alto rischio valgono anche, con le dovute addizioni, agli effetti della valutazione d'impatto sulla protezione dei dati (DPIA) di cui all'art. 35 GDPR (art. 27, § 4 Regolamento IA)[24];

c) **Frizione/Estensione della base legale per l'esenzione:** in alcuni casi, il Regolamento IA introduce degli allentamenti alla normativa europea di protezione dei dati personali, sul presupposto che la scrupolosa osservanza della seconda potrebbe essere di ostacolo al perseguimento di finalità di interesse pubblico egualmente meritevoli di tutela. E così, ampliando lo spettro di deroghe contemplate dall'art. 9(2) GDPR, l'art. 10, § 5 del Regolamento IA pone una base legale espressa per il trattamento di dati sensibili, nell'ipotesi in cui il loro trattamento sia necessario "*al fine di garantire il rilevamento e la correzione delle distorsioni* [n.d.r. "*suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future*"] *in relazione ai sistemi di IA ad alto rischio*", e sempre che siano rispettate sei condizioni cumulative dettagliate alle lettere *a)-f)* del medesimo paragrafo. Con una logica non dissimile, l'art. 59 del Regolamento IA disciplina l'"*ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico*".

[24] A ciò deve aggiungersi che il Regolamento persegue una logica di integrazione non solo esterna (nei rapporti con il GDPR), ma anche interna (cioè tra diverse disposizioni del medesimo testo normativo). Ad esempio, si stabilisce che le informazioni che, ai sensi dell'art. 13 Regolamento IA, devono essere fornite dal *deployer* per assolvere ai doveri di trasparenza assumono valore anche agli effetti della FRIA, senza necessità, cioè, di duplicare gli adempimenti (art. 26, § 9 Regolamento IA).

2 La *Governance* europea dell'IA e i criteri direttivi per la *Governance* nazionale

Il Capo VII del Regolamento IA è dedicato alla "*Governance*".

Si prevede, in primo luogo, l'istituzione dell'Ufficio AI (art. 64), processo già anticipato dalla Commissione prima dell'entrata in vigore del Regolamento[25]. Come evidenziato nell'Introduzione, la scelta di istituire un Ufficio interno alla Commissione, in luogo di un'Agenzia o Autorità indipendente europea, è in sé rivelatrice del fatto che, anche a livello sovranazionale, l'applicazione del Regolamento IA presenta riflessi di *policy*, non essendo, cioè, del tutto scevra da tratti di politicità, nel senso lato del termine. L'Ufficio ha principalmente funzioni di supporto e consulenza, ma assume anche compiti di vigilanza diretta in riferimento ai modelli di IA per finalità generali (*general purpose artificial intelligence* - GPAI)[26]. Al di fuori di questa ipotesi, il Regolamento prevede l'integrale decentramento, invece, dell'attività di *enforcement* sugli Stati membri[27].

Si prevede, poi, l'istituzione di un Consiglio europeo per l'intelligenza artificiale (art. 65), che fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del regolamento. Esso è composto di un rappresentante per Stato membro e vi partecipano, senza diritto di voto, l'Ufficio IA e l'EDPS.

Chiudono il cerchio il Forum consultivo (art. 67), che rappresenta una selezione equilibrata di *stakeholder*, e i Gruppi di esperti scientifici indipendenti (art. 68), entrambi volti a favorire l'ingresso di conoscenze e competenze, ma anche di interessi privati e sociali, nella fase di "messa a terra" del Regolamento.

Per quanto concerne la *governance* nazionale (art. 70), si prevede che ciascuno Stato membro istituisce o designa come autorità competenti almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del Regolamento.

Al pari di quanto previsto per i servizi finanziari (art. 74, § 6), sus-

[25] Decisione C(2024) 390 final del 24 gennaio 2024.

[26] Art. 88 del Regolamento IA.

[27] L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, n. 4/2022, 1110-12.

siste una riserva esplicita di competenza in favore del GPDP. Ai sensi dell'art. 74, § 8, "*per i sistemi di IA ad alto rischio …, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III del presente regolamento, punti 6, 7 e 8, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680*".

Al contempo, il Regolamento pone enfasi sull'importanza che l'Autorità di vigilanza, se differente da quella di protezione di diritti fondamentali, stabilisca un effettivo coordinamento con quest'ultima.

Ai sensi dell'art. 77, § 1 "*le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali … in relazione all'uso dei sistemi di IA ad alto rischio di cui all'allegato III hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione*". Il § 3 aggiunge che "*qualora la documentazione … non sia sufficiente per accertare un'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità pubblica o l'organismo pubblico di cui al paragrafo 1 può presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici. L'autorità di vigilanza del mercato organizza le prove coinvolgendo da vicino l'autorità pubblica o l'organismo pubblico richiedente entro un termine ragionevole dalla richiesta*".

Ai sensi dell'art. 79, § 2, "*qualora l'autorità di vigilanza … abbia un motivo sufficiente per ritenere che un sistema di IA presenti un rischio …*[28]*, essa effettua una valutazione del sistema di IA interessato per quanto riguarda la sua conformità a tutti i requisiti e gli obblighi di cui al* [R]*egolamento… Qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti …, e coopera pienamente con essi. I pertinenti operatori cooperano, per quanto necessario, con l'autorità di vigilanza del mercato*

[28] *I.e.* qualora si tratti di un "*prodotto che potenzialmente potrebbe pregiudicare la salute e la sicurezza delle persone in generale, la salute e la sicurezza sul posto di lavoro, la protezione dei consumatori, l'ambiente e la sicurezza pubblica, nonché altri interessi pubblici tutelati dalla normativa di armonizzazione dell'Unione applicabile, oltre quanto ritenuto ragionevole ed accettabile in relazione all'uso previsto del prodotto o nelle condizioni d'uso normali o ragionevolmente prevedibili, incluse la durata di utilizzo e, se del caso, i requisiti relativi alla messa in servizio, all'installazione e alla manutenzione*".

e con le altre autorità o gli altri organismi pubblici nazionali [di tutela di diritti fondamentali]". Se le suddette autorità "*rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza indebito ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di rendere il sistema di IA conforme, ritirarlo dal mercato o richiamarlo*". Ai sensi del § 5, "*qualora l'operatore di un sistema di IA non adotti misure correttive adeguate nel periodo* [assegnato]*, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato nazionale, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo*", dandone notifica, ai sensi del § 6, alla Commissione. La Commissione o l'Autorità di vigilanza di un altro Stato possono opporsi alla misura provvisoria entro 3 mesi.

Se il sistema di IA classificato "ad alto rischio" apparisse "conforme", ma il procedimento congiunto appena descritto dovesse comunque evidenziare un "rischio", nei termini sopra divisati, l'Autorità di vigilanza potrebbe imporre misure e comunicarle alla Commissione. In tale ultima circostanza, però, non opera il meccanismo del silenzio-assenso (art. 82).

3 Gli spazi di discrezionalità lasciati aperti dall'art. 70 del Regolamento IA

La formulazione aperta dell'art. 70 del Regolamento IA ha aperto un dibattito, tuttora in corso, su quale debba essere la *governance* nazionale dell'intelligenza artificiale più desiderabile.

Secondo quanto illustrato dall'EDPB nello Statement 3/2024 "*on data protection authorities' role in the Artificial Intelligence Act framework*" del 16 luglio 2024, risponderebbe ai criteri di razionalità e semplificazione la scelta degli Stati membri di individuare le Autorità di protezione dei dati personali quali Autorità di vigilanza ai sensi dell'art. 70, § 1 Regolamento IA, ferma restando la necessità di dotare tali soggetti di risorse umane e finanziarie aggiuntive (§ 12). Ciò in quanto le Autorità di protezione dei dati personali: i) già possiedono l'*expertise* necessaria, avendo partecipato attivamente al cantiere normativo dell'*AI Act* e occupandosi, tra l'altro, di aspetti come il trattamento dei dati personali tramite decisioni completamente automatizzate e le misure di sicurezza (§§ 6 e 8); ii) assicurerebbero un "*single contact point*" ai soggetti interessati e alle imprese vigilate. A tali rilievi si aggiungono quelli mossi dal Garante privacy nazionale nella precedente Segnalazione al Parlamento e al Governo. In tale sede, il GPDP già evidenziava come la sua nomina, in vece di agenzie riconducibili all'Esecutivo, assicurerebbe i

criteri di indipendenza richiesti dal Regolamento, oltre ad apparire più razionale, atteso che il Garante è l'unico soggetto nei cui confronti il Regolamento IA pone una "riserva di competenza" (come visto, ai sensi dell'art. 74, § 8). Inoltre, l'individuazione del Garante come Autorità di vigilanza ridurrebbe al minimo il rischio di "conflitti di competenza e duplicazione ingiustificata degli oneri amministrativi per soggetti pubblici e privati"[29].

Da ultimo, le ragioni (sia tecniche che di indipendenza) che militano a favore di un coinvolgimento attivo delle Autorità di protezione dei dati personali nella *governance* dell'IA sono state ribadite anche nel corso del G7 (*Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI* cit., rispettivamente §§ 8-11 e § 12).

La posizione assunta dall'EDPB e dal Garante privacy appare animata dalle migliori intenzioni e denota, indubbiamente, un certo pragmatismo.

Ciò non equivale a dire, però, che una scelta legislativa di segno diverso sarebbe automaticamente contraria al Regolamento IA o determinerebbe, di per sé, un pregiudizio alla protezione dei dati personali.

Si è visto, infatti, che il Regolamento IA lascia impregiudicato il GDPR. Salvo diversamente disposto nel Regolamento IA, le regole di diritto sostanziale di cui al Regolamento (UE) 679/2016 (cui si aggiungono il Regolamento (UE) 2018/1725, sul trattamento di dati personali da parte di istituzioni o organismi europei, e la direttiva (UE) 2016/680, sulla protezione dei dati personali delle persone coinvolte in procedimenti penali) sono pienamente applicabili ai trattamenti che abbiano luogo nel contesto di sistemi di IA, rispetto ai quali i Garanti (europei e nazionali) mantengono tutti i propri poteri di intervento. Ciò in quanto l'Unione intende creare le basi, sul piano assiologico, per uno sviluppo tecnologico antropocentrico.

Allo stesso tempo, assicurare la piena e rigorosa applicazione del GDPR ai sistemi di IA ad alto rischio potrebbe porre alcune complessità sul piano operativo. Ad esempio, la maggior *trustworthiness* della tecnologia potrebbe esigere trattamenti di categorie sensibili di dati personali o potrebbe richiedere modalità implementative suscettibili di entrare in tensione con princìpi cardine come, ad esempio, la *data minimization*[30] o la *purpose limitation*[31]. Significativamente, almeno due norme del Regolamento IA pro-

[29] cfr. Segnalazione al Parlamento e al Governo sull'Autorità per l'i. a., doc. web 9996508 del 25 marzo 2024.

[30] Art. 5, § 1, lett. *c)* del GDPR.

[31] Art. 5, § 1, lett. *b)* del GDPR.

pongono, come visto, degli allentamenti della disciplina generale dettata dal GDPR[32]. Pur assumendo un carattere circoscritto e mostrandosi rispettose, nel loro complesso, dello spirito del GDPR, questi "adattamenti" suggeriscono, su un piano più generale, che le due anime del Regolamento IA (*product safety approach* e *rights based approach*) seguono, in linea di massima, una linea di convergenza, ma in talune circostanze potrebbero divergere, tanto da richiedere una previa composizione normativa. L'asse potrebbe ulteriormente spostarsi verso le ragioni di affidabilità tecnologica del prodotto se nell'equazione del bilanciamento facesse ingresso anche la variabile dell'innovazione e, più in particolare, del grado di competitività che si vuole riconoscere al modello europeo o nazionale di IA. A seconda della sensibilità dell'interprete, cioè, il punto di equilibrio potrebbe pendere verso l'innovazione o sbilanciarsi, invece, verso la protezione di diritti fondamentali. Detto in termini più compiuti: ferma restando l'incomprimibilità del diritto alla privacy, a fronte di una pluralità di opzioni ermeneutiche tutte astrattamente plausibili si potrebbe propendere, a seconda degli approcci, per soluzioni interpretative più o meno rigide.

Per altro profilo, non deve trascurarsi il diverso scenario in cui si registrino frizioni applicative tutte interne alla componente *rights based* del Regolamento IA. Come si vedrà[33], in astratto un determinato utilizzo di un modello di IA potrebbe andare a beneficio di un diritto fondamentale comprimendone un altro. Per fare un esempio, un accordo tra il legittimo titolare dei diritti di sfruttamento economico di un diritto di proprietà intellettuale e uno sviluppatore di sistemi di IA generativa che utilizzano *large language models* (LLM) potrebbero essere di mutuo interesse, se funzionale all'affinamento della tecnologia sottostante e alla contestuale protezione e valorizzazione del diritto d'autore, che pure rientra nel catalogo dei diritti fondamentali[34]. Tuttavia – lo si vedrà nel seguito – un simile accordo potrebbe anche sollevare criticità in punto di trattamento di dati personali. Criticità delle quali le parti dovrebbero tener conto, allora, nella relativa DPIA e FRIA.

Trattandosi di un discorso complesso e plurisfaccettato, l'illustrazione pratica di un *case-study* potrebbe risultare di ausilio alla miglior intelligenza della questione (*infra* § 4).

[32] *I.e.*, gli artt. 10, § 5 e 59, cui fa richiamo l'art. 2, § 7 del Regolamento IA. Le citate previsioni rappresentano fattispecie, positivizzate, di trattamento per legittimo interesse *ex* art. 6, § 1, lett. *f)* del GDPR.

[33] *Infra* § 4.

[34] Art. 17, § 2 CDFUE.

Seguirà, quindi, la succinta descrizione del d.d.l. IA (§ 5) e, per concludere, una breve riflessione sugli ulteriori correttivi che, a giudizio di chi scrive, sarebbe auspicabile apportare al testo legislativo oggetto di dibattito parlamentare (§ 6).

4 *The Space Between*: il caso Openai come dimostrazione pratica della pluralità di approcci possibili all'IA

Un ottimo terreno di confronto per saggiare la cennata tensione tra competitività e garanzia è quello dell'intelligenza artificiale generativa.

In alcuni commenti si è osservato che l'applicazione troppo stringente del principio di limitazione delle finalità di cui all'art. 5, § 1, lett. *b)* GDPR potrebbe collidere con la circostanza che, in sistemi di questo genere, gli usi successivi possono essere molteplici (raccolta di dati/addestramento/validazione/*testing*)[35]. Nei medesimi contributi si è altresì auspicato che, in conformità con gli orientamenti del CNIL, il principio di minimizzazione dei dati personali (art. 5, § 1, lett. *c* GDPR) venga applicato nella fase *post-training*, e non in quella di *pre-training*. In questo contesto, va diffondendosi l'idea che la base giuridica più appropriata per il trattamento di dati personali ad opera di sistemi IA sia quella del legittimo interesse *ex* art. 6, § 1, lett. *f)* GDPR[36], sempre che ne siano integrati presupposti e condizioni[37]. Seguendo questa linea interpretativa, cioè, vi sarebbe un legittimo interesse al trattamento del dato personale per assicurare la "sicurezza" e

[35] Cfr. E. Drouard - O. Kurochkina - R. Schlich - D. Ozturk, *The Interplay between the AI Act and the GDPR: Part II – Compliance Challenges for AI Systems That Use Personal Data*, in *AIRe*, n. 3/2024, 297 e ss.

[36] Cfr. ICO, *Consultation series on generative AI and data protection*, <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-series-on-generative-ai-and-data-protection/>; CNIL, Sheet No. 8, *Relying on the legal basis of legitimate interests to develop an AI system*, 2 luglio 2024, <https://www.cnil.fr/fr/node/165894>. Come noto, ai sensi dell'art. 21(1) GDPR, "*l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, letter*[a] *f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*".

[37] Sui quali, da ultimo, v. le EDPB Draft Guidelines 1/2024 "*on processing of personal data based on Article 6(1)(f) GDPR*", Versione 1.0 , adottate l'8 ottobre 2024.

"affidabilità" del sistema di IA[38], specie quando entrino in gioco interessi pubblici qualificati.

Queste posizioni si sforzano, insomma, di trovare un punto di equilibrio tra protezione del diritto umano e sviluppo tecnologico.

Tuttavia, un'Autorità di controllo ben potrebbe adottare una linea più rigorosa, nel rispetto del principio di proporzionalità.

La prassi decisionale del Garante privacy italiano in materia di IA generativa sembrerebbe favorire tale ultima impostazione.

Già a marzo 2023, con più di un anno di anticipo sull'entrata in vigore del Regolamento IA, il GPDP ha disposto in via di urgenza la limitazione provvisoria del trattamento, ai sensi dell'art. 58, § 2, lett. *f)* del GDPR, nei confronti di OpenAI L.L.C., società statunitense sviluppatrice del prodotto "ChatGPT", oggi definibile, ai sensi del Regolamento IA[39], come "*sistema di IA per finalità generali*"[40]. Ciò – si noti – proprio sul presupposto dell'"*assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT*", nonché dell'"*assenza di qualsivoglia verifica dell'età degli utenti in relazione al servizio ChatGPT*"[41]. Il successivo 11 aprile il Garante ha sospeso l'efficacia del citato provvedimento interinale e ordinato, ai sensi dell'art. 58, § 2, lett. *d)* del GDPR, *inter alia*, una serie di miglioramenti informativi, nonché ingiunto "*la modifica della base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento algoritmico, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse in relazione alle valutazioni di competenza della società in una logica di* accountability"[42].

Tale azione ha indotto, il 13 aprile 2023, l'EDPB a istituire una *task force* dedicata al servizio ChatGPT[43].

Con comunicato stampa del 29 gennaio 2024 il GPDP ha reso noto di aver notificato a OpenAI l'atto di contestazione per aver violato, sotto molteplici profili, la normativa in materia di protezione dei dati personali[44].

---

[38] Arg. ex conss. nn. 49 e 71 GDPR.

[39] Segnatamente, ai sensi dell'art. 3, n. 66.

[40] Cfr., per la disciplina operativa, il Capo V, artt. 51 e ss.

[41] Provv. n. 112 del 30 marzo 2023, doc. web n. 9870832, ratificato dal Collegio nell'adunanza dell'8 aprile 2023.

[42] Provv. n. 114 dell'11 aprile 2023, doc. web n. 987470.

[43] Cfr. <https://www.edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en>.

[44] *ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla norma-*

L'istruttoria – si chiarisce nel comunicato – terrà conto degli orientamenti espressi dalla *task force*, che tuttavia non vincolano l'*enforcer* nazionale.

A maggio 2024 la *task force* istituita dall'EDPB ha prodotto un *interim report*[45]. Il suddetto Report, per quanto qui di interesse, non sembra opporsi aprioristicamente a un trattamento – quantomeno nelle fasi prodromiche di raccolta/*web-scraping*; *pre-processing*/*filtering*; e *training* – per legittimo interesse *ex* art. 6, § 1, lett. *f)* GDPR, nella misura in cui vengano adottati opportuni accorgimenti tecnici, come ad esempio "*technical measures, defining precise collection criteria and ensuring that certain data categories are not collected or that certain sources (such as public social media profiles) are excluded from data collection*", o "*measures … to delete or anonymise personal data that has been collected via web scraping before the training stage*"[46]. Siccome un'analisi individuale dei dati raccolti sarebbe di fatto impossibile, il *data controller* dovrebbe però dotarsi quantomeno di meccanismi di filtro diretti a espungere dal *dataset* dati sensibili *ex* art. 9, § 1 GDPR, sempre che non ricorrano le condizioni di cui al § 2 del medesimo articolo[47]. Per quanto concerne gli *input* forniti attivamente dal *data subject* attraverso la maschera di *prompt*, il trattamento *ex* art. 6, § 1, lett. *f)* GDPR potrebbe ritenersi ammissibile, ma solo a fronte di un'informativa molto chiara[48]. Nel diverso caso di raccolta tramite *web scraping* di dati personali provenienti da soggetti passivi che non facciano un utilizzo attivo del servizio ChatGPT, invece, l'eccezione all'informativa di cui all'art. 14, § 5, lett. *b)* del GDPR potrebbe trovare applicazione[49].

Se il Garante, come inizialmente preannunciato nei Comunicati stampa, dovesse tener conto delle linee direttrici elaborate dalla *task force*, potrebbe esservi spazio per uno sviluppo antropocentrico e, al contempo, tecnologicamente sostenibile dei servizi oggetto di indagine[50].

In primo luogo, il GPDP ha aperto un nuovo filone di indagine in

tiva privacy, doc. web n. 9978020.

[45] *Report of the work undertaken by the ChatGPT Taskforce*, 23 maggio 2024, <https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf>.

[46] Report cit., § 17.

[47] *Ivi*, § 19.

[48] *Ivi*, §§ 21-22, ove il riferimento all'informativa di cui all'art. 14 del GDPR.

[49] *Ivi*, § 27.

[50] Nelle more, potrebbero altresì sopraggiungere le nuove Linee guida dell'EDPB in materia di legittimo interesse, delle quali pure il Garante dovrà, in caso, tener conto (EDPB, Draft Guidelines n. 1/2024 cit.).

relazione al modello "Sora" sviluppato da OpenAI, in grado, secondo quanto annunciato dallo sviluppatore, di creare scene dinamiche, realistiche e fantasiose, partendo da poche istruzioni testuali[51].

In secondo luogo, il Garante privacy ha inviato un avvertimento, ai sensi dell'art. 58, § 2, lett. *a)* del GDPR, nei confronti di OpenAI e GEDI Gruppo Editoriale S.p.A. in riferimento a un accordo siglato negli Stati uniti il 24 settembre 2024. In forza di tale accordo, una mole ingente di contenuti degli editori coinvolti[52] sarebbe utilizzata da OpenAI per consentire agli utenti del servizio ChatGPT di fare ricerche in tempo reale di notizie di attualità, con contestuale fornitura di un riassunto – elaborato da sistemi di gen-AI – e del *link* diretto alla pertinente notizia. Inoltre, tutti i contenuti editoriali verrebbero utilizzati da OpenAI anche per migliorare i propri servizi e addestrare i propri algoritmi. Secondo il Garante, l'accordo sarebbe stato concluso sulla base di una DPIA carente e potrebbe violare gli artt. 9, 10, 13 e 14 del GDPR[53]. La posizione del Garante sembra essere stata in qualche modo anticipata dall'intervento di un suo componente pubblicato lo scorso maggio. Vi si legge che mentre alcuni editori, come il New York Times, hanno intentato causa contro OpenAI dopo mesi di trattative infruttuose, "altri editori … raggiungono accordi di licenza milionari con le fabbriche degli algoritmi e risolvono o, meglio, prevengono ogni questione a monte, moltiplicando gli utili e le forme di sfruttamento sui propri archivi che si rivelano utili e protagonisti di un mercato diverso rispetto a quello dell'informazione, quello, appunto, dei contenuti destinati a rendere «intelligenti» gli algoritmi di una manciata di Corporation già divenute oligopoliste del mercato dei servizi basati sull'intelligenza artificiale generativa"[54]. Al riguardo, il componente dubita del fatto che la cessione dei diritti

[51] *Intelligenza artificiale, il Garante privacy avvia istruttoria su "Sora" di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo*, 8 marzo 2024, doc. web n. 9991867.

[52] L'accordo di estende, in particolare, ai contenuti pubblicati sui seguenti siti: www.repubblica.it, www.lastampa.it, www.laprovinciapavese.gelocal.it, www.lasentinella.gelocal.it, www.limesonline.com, www.huffingtonpost.it, www.formulapassion.it, www.mymovies.it, www.alfemminile.com.

[53] Provv. n. 741 del 27 novembre 2024, doc. web n. 10077129.

[54] Cfr. Scorza: *"L'IA si ciba di news: dati personali a rischio". In tutto il mondo si diffondono i contratti di licenza tra editori di giornali e big tech per lo sfruttamento commerciale dei contenuti al fine di addestrare gli algoritmi: bisogna riflettere sulle ripercussioni per i dati personali e, di conseguenza, dignità e libertà degli interessati* - Intervento di Guido Scorza, 14 maggio 2024, doc. web n. 10013837, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/ 10013837>.

autorali dai giornalisti agli editori comporti anche la facoltà, per questi ultimi, di sfruttare economicamente i contenuti a fini di *training* algoritmica. Anche perché – si legge nell'intervista – "l'addestramento degli algoritmi di intelligenza artificiale generativa non ha nulla a che fare con il diritto di cronaca considerato che… i contenuti generati da tali servizi sono semplicemente verosimili su base statistica e probabilistica".

5 Il Ddl AI e il parere preventivo espresso dal Gpdp

Come visto, il Regolamento IA è rimasto neutrale rispetto alla questione delle designazioni nazionali: sarebbe soddisfatto dall'individuazione del Garante privacy nazionale quale Autorità di vigilanza, ma non si oppone a priori a una *governance* nazionale dell'IA che non segua un simile schema.

In questo contesto, il 20 maggio 2024 il Governo ha sottoposto all'*iter* di approvazione parlamentare il disegno di legge n. 1146, rubricato "*Disposizioni e delega al Governo in materia di intelligenza artificiale*".

Come si legge nell'AIR, il d.d.l. persegue due obiettivi generali: "1*) rafforzare la competitività italiana come obiettivo strategico nella politica economica italiana nell'ambito del contesto europeo; 2) garantire ai cittadini italiani l'uso affidabile e responsabile dell'IA, attraverso una visione antropocentrica che non solo garantisca la supervisione umana in ogni fase di sviluppo e di utilizzo dei sistemi IA, ma che garantisca, attraverso la trasparenza e l'accesso dei cittadini alle informazioni, la tutela dei diritti fondamentali*".

In punto di *governance*, l'art. 20 del d.d.l., nella versione approvata in Senato il 20 marzo 2025 (A.C. 2316), costruisce un sistema articolato su più livelli ma, sostanzialmente, descrivibile come a trazione duale:

i) in primo luogo, l'Agenzia per l'Italia digitale (AgID), ferme restando le funzioni già attribuite, è responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale, e provvede a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA, secondo quanto previsto dalla normativa nazionale e dell'Unione europea (art. 20, comma 1, lett. *a*);

ii) in secondo luogo, l'Agenzia per la cybersicurezza nazionale (ACN), ferme restando le funzioni già attribuite, è responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza, nonché per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di IA, secondo quanto

previsto dalla normativa nazionale e dell'Unione europea (art. 20, comma 1, lett. *b*);

iii) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di IA conformi alla normativa nazionale e dell'Unione europea, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale (art. 20, comma 1, lett. *c*);

iv) è istituito presso la Presidenza del Consiglio dei ministri un Comitato di coordinamento, composto dai direttori generali dell'AgID e dell'ACN e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Il Comitato ha il compito di assicurare il coordinamento e la collaborazione tra le Autorità nazionali per l'intelligenza artificiale e le altre pubbliche amministrazioni e autorità indipendenti (art. 20, comma 3);

v) restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali (art. 20, comma 4).

Resta inoltre ferma l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorità di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, § 6 Reg. IA (art. 20, commi 1 e 2). Di conseguenza, la strategia nazionale per l'intelligenza artificiale è predisposta anche con la loro intesa (art. 19, comma 1) e le stesse "partecipano", *ratione materie*, al Comitato di coordinamento (art. 20, comma 3).

Nel "*Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale*"[55], il Garante ha espresso un giudizio complessivamente favorevole sul d.d.l., formulando però una serie di rilievi.

Dopo aver proposto di sostituire i commi 2 e 3 dell'art. 4 – contenenti richiami alla normativa sulla protezione dei dati personali – con un articolo a sé, diretto ad affermare un "vincolo generale di conformità dei trattamenti di dati personali funzionali a sistemi di i.a. alla disciplina rilevante in materia [di privacy]", e dopo aver suggerito una serie di modifiche e integrazioni su aspetti di dettaglio, al fine di assicurare il pieno rispetto della normativa in materia di protezione dei dati personali, il Garante ha formulato alcune critiche costruttive in punto di *governance* istituzionale.

In primo luogo, il Garante ha chiesto di essere inserito tra i soggetti abilitati a esprimersi sulla Strategia nazionale per l'intelligenza artificiale messa a punto dalla struttura della Presidenza del Consiglio dei ministri

[55] Provv. n. 477 del 2 agosto 2024, doc. web n. 10043532.

competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali per l'intelligenza artificiale e sentiti il Ministro delle imprese e del *Made in Italy*, per i profili di politica industriale e di incentivazione, e il Ministro della difesa, per gli aspetti relativi ai sistemi di IA impiegabili in chiave duale (art. 19, comma 1 d.d.l.).

In secondo luogo, "per realizzare pienamente quella leale cooperazione tra autorità competenti prevista dall'AI Act", il Garante segnala l'utilità di un suo coinvolgimento permanente nel Comitato di coordinamento disciplinato dall'art. 20, comma 3 d.d.l.

In terzo luogo, e per le medesime ragioni, il GPDP ritiene "opportuno integrare l'articolo prevedendo, in fine, che AgID e ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati, richiedendo altresì il parere dell'Autorità rispetto a fattispecie, al loro esame, che coinvolgano aspetti di protezione dei dati. Il Garante trasmetterà, per parte sua, elementi informativi in ordine a profili di competenza di AgID o ACN suscettibili di emergere nella trattazione di propri procedimenti".

In quarto e ultimo luogo, per ragioni di certezza del diritto il Garante chiede di esplicitare ciò che è implicito nel Regolamento IA (artt. 74, § 8 e 77, §§ 1 e 2), designando cioè espressamente il medesimo soggetto come Autorità chiamata a occuparsi, per i profili di competenza, dei sistemi di IA implicanti il trattamento di dati sensibili.

6 Ulteriori proposte di modifica

Come ben evidenziato dal Garante, il d.d.l. potrebbe (e dovrebbe) meglio articolare i doveri di coordinamento tra p.A. coinvolte, direttamente o indirettamente, nella *governance* dell'IA. Lo stesso art. 74, § 10 Regolamento IA, del resto, stabilisce che "*gli Stati membri agevolano il coordinamento tra le autorità di vigilanza del mercato designate a norma del presente regolamento e altre autorità o organismi nazionali pertinenti che controllano l'applicazione … di … disposizioni del diritto dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III*".

Come ricordato dall'EDPB (§ 11), il faro di questa previsione dovrebbe essere il principio di leale collaborazione di cui all'art. 4, § 3 TUE, nella declinazione pregnante risultante dalla sentenza della Corte di giustizia sul caso *Meta Platforms e al.*[56] e, deve aggiungersi, dalla pronuncia del Con-

[56] 4 luglio 2023, C-252/21, §§ 53-63.

siglio di Stato sul caso *Telepass c. AGCM*[57].

L'importanza della leale collaborazione è emersa, da ultimo, anche nel corso del G7 privacy[58].

Si tratta di osservazioni pienamente condivisibili, e che anzi meriterebbero di essere ulteriormente sviluppate.

Come si è visto, il Regolamento prevede che il GPDP, quando la documentazione fornita dall'impresa non sia sufficiente alle proprie indagini, possa rivolgersi motivatamente all'ACN per richiedere motivatamente di "*organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici*" (art. 77, §§ 1 e 3 del Regolamento IA).

Un meccanismo di questo genere appare di fondamentale importanza e dovrebbe forse essere oggetto di estensione se si considera che le competenze del Garante restano, come naturale che sia, impregiudicate. E questo, si noti, vale per tutte le tipologie di IA, non solo quelle ad alto rischio, sicché non si vedono ragioni per escludere "richiest[e] motivat[e]" aventi ad oggetto sistemi di IA non sottoposti alla vigilanza dell'ACN. Anche perché, nel disegno dell'Esecutivo, l'ACN dovrebbe guadagnare un'*expertise* di primo piano sulla *black box* algoritmica.

Ebbene, l'art. 20 d.d.l. non dettaglia in alcun modo le modalità operative del suddetto coordinamento/avvalimento. Né è lecito attendersi indicazioni utili dall'esercizio delle deleghe legislative conferite al Governo in materia di IA (art. 24 d.d.l.), che invero non offrono princìpi e criteri direttivi sul punto.

Ferma restando la diretta applicabilità dell'art. 77, §§ 1 e 3 del Regolamento IA, potrebbe trattarsi di un'occasione persa.

Il legislatore, ad esempio, potrebbe sforzarsi di tipizzare le conseguenze dell'inerzia serbata o del diniego opposto dall'ACN a fronte di richieste di supporto avanzate dal Garante (o altre Autorità). In secondo luogo, il legislatore ben potrebbe mettere in campo misure atte a mitigare il rischio dell'inerzia o del rifiuto di assistenza. Ciò non esclude – si noti – l'opportunità di dotare il Garante delle risorse umane e finanziarie idonee a fronteggiare le sfide poste dall'IA.

Una seconda osservazione di carattere generale attiene alla questione dei livelli e delle sedi del coordinamento istituzionale.

Si è visto che il Regolamento AI ha un contenuto eterogeneo e, come tale, abbisogna tanto di indirizzo politico quanto di vigilanza indipendente. I due momenti, però, dovrebbero restare quanto più possibile distinti. A garan-

[57] Sez. VI, 15 gennaio 2024, n. 497.

[58] *Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI* cit., § 16.

zia di una piena e indipendente protezione dei dati personali, separati devono rimanere, allora, anche i circuiti istituzionali che li hanno in carico.

Se ne possono trarre due conseguenze sul piano operativo: mentre non appare necessario, né forse desiderabile, coinvolgere il Garante nella messa a punto della Strategia nazionale sull'IA (art. 19 d.d.l.), trattandosi di attività, per l'appunto, di indirizzo politico; per ragioni eguali e contrarie non sembra sufficiente aggiungere il Garante alla platea di soggetti abilitati a sedere nel Comitato di coordinamento (art. 20, comma 3 d.d.l.). Qui l'operazione dovrebbe essere, forse, più radicale e coraggiosa, nel senso che i Dicasteri dovrebbero essere espunti dal consesso, e le mura del confronto non dovrebbero essere quelle di Palazzo Chigi. La previsione sembra esser frutto, per il vero, di una errata e decontestualizzata trasposizione dell'art. 65 del Regolamento, che istituisce il Consiglio europeo per l'intelligenza artificiale, cui prendono parte una "rappresentante" per Stato membro. Ma sul piano del diritto interno il coordinamento delle *policy* è già assicurato dal procedimento composito di approvazione della Strategia nazionale (art. 19 d.d.l.). E non v'è ragione di riproporre il *format* quando si tratti di gestire il coordinamento tra le Autorità designate in materia di IA e le altre Autorità indipendenti. Non appare conducente, cioè, incardinare in sede governativa il coordinamento, giacché coordinamento significa anche dialettica. E il sottoporre a stretta osservazione governativa l'agire interistituzionale di due Agenzie che, come detto, potrebbero possedere, agli effetti del Regolamento, sufficienti requisiti di indipendenza, ma certo non sono Autorità indipendenti[59], potrebbe determinare la caduta dell'impalcatura, non solidissima, della *governance* nazionale tratteggiata nel d.d.l. In conclusione, il coordinamento sull'*enforcement* dovrebbe aver luogo in campo neutro e coinvolgere solo le Agenzie designate in materia di IA e le Autorità indipendenti maggiormente toccate dal fenomeno, tra le quali rientra, a pieno titolo, il Garante. Ciò, peraltro, sul modello di quanto già avviene, in Italia, per assicurare l'effettiva attuazione del *Digital Services Act*[60] e del

[59] Cfr., al riguardo, il parere circostanziato (C(2024) 7814) rilasciato dalla Commissione europea lo scorso 5 novembre, ai sensi della direttiva (UE) 2015/1535. Si osserva che la scelta di designare agenzie governative in luogo di autorità indipendenti non è esclusiva dell'Italia: cfr. gli esempi di Danimarca, Spagna e Germania.

[60] L'art. 49 del Digital Services Act (DSA, Regolamento (UE) n. 2022/2065) impone agli Stati membri di designare un "Coordinatore dei servizi digitali". La scelta, come noto, è ricaduta sull'Autorità per le Garanzie nelle Comunicazioni (art. 15, comma 1 D.L. n. 123/2023, conv., con modificazioni, dalla L. n. 159/2023). Si prevede, a tal fine, che "*l'Au-*

Data Governance Act [61].

torità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione" (art. 15, comma 2).

[61] Nel dare attuazione al Data Governance Act (DGA, Regolamento (UE) n. 2022/868), l'Italia ha designato l'AgID quale autorità competente allo svolgimento dei compiti relativi alla procedura di notifica per i servizi di intermediazione dei dati, nonché quale autorità competente alla registrazione di organizzazioni per l'altruismo dei dati (art. 2, comma 1 d. lgs. n. 144 del 2024, attuativo, in particolare, degli artt. 13, 23 e 26 DGA). In tale contesto, si prevede che "*l'AgID opera in stretta e leale cooperazione con l'Agenzia per la cybersicurezza nazionale, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali e, a tal fine, può stipulare con gli stessi specifici accordi di collaborazione non onerosi. Gli accordi definiscono le forme e i modi di esercizio del coordinamento, anche endoprocedimentale, delle competenze, nell'ambito delle rispettive attribuzioni di AgID, del Garante per la protezione dei dati personali, dell'Agenzia per la cybersicurezza nazionale e delle altre amministrazioni competenti, in relazione alla materia trattata. Nel rispetto del principio di leale collaborazione, gli accordi prevedono forme specifiche di consultazione del Garante per la protezione dei dati personali, ogniqualvolta il procedimento amministrativo realizzato da AgID abbia implicazioni in termini di protezione dei dati*" (art. 2, comma 2). L'AgID, inoltre, deve sentire, per gli aspetti di competenza, l'ACN, l'AGCM e il GPDP prima di stabilire con proprio provvedimento le disposizioni tecniche e organizzative per facilitare l'altruismo dei dati nonché le informazioni necessarie che devono essere fornite agli interessati in merito al riutilizzo dei loro dati nell'interesse generale (art. 2, comma 3).

Francesca Pellicanò[62] e Rosaria Petti

L'intelligenza artificiale e i settori regolati dall'Autorità per le garanzie nelle comunicazioni

Sommario. 1. Premessa – 2. Le telecomunicazioni *(Rosaria Petti)* – 3. L'audiovisivo *(Francesca Pellicanò)* – 4. Conclusioni

1 Premessa

L'utilizzo dei sistemi di IA e delle relative applicazioni è destinato ad avere un impatto profondo sui mercati regolati e sui diritti che l'Autorità per le garanzie nelle comunicazioni è chiamata a tutelare, con riferimento alla garanzia del pluralismo, alla tutela della dignità umana e dei diritti fondamentali degli individui, alla tutela dei minori, alla sicurezza delle reti, alla tutela del diritto d'autore, alla tutela degli utenti nella fruizione dei servizi di comunicazione elettronica e di media digitali.

Infatti, nell'ottica di una Autorità convergente per la regolamentazione dei servizi di comunicazioni digitali, l'applicazione di nuovi strumenti tecnologici fondati su varie forme di AI è un fenomeno destinato a investire un'ampia gamma di prodotti e servizi già regolamentati o di prossima regolazione. Si pensi, ad esempio, all'Internet of Things e alle reti e servizi di comunicazioni elettroniche di ultima generazione; alla trasparenza algoritmica delle piattaforme online e alle altre regole introdotte con i Regolamenti P2B, DSA e DMA, per ricondurre alcune funzioni automatizzate dei servizi digitali, quali i sistemi di raccomandazione di contenuti, nell'alveo dei principi fondamentali che governano il mercato unico europeo.

Nel settore audiovisivo, le sfide regolamentari connesse alla diffusione dell'AI, compresi il software, gli algoritmi e i dati utilizzati o generati da essa, da un lato hanno innescato trasformazioni nei processi di produ-

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

zione e consumo di contenuti audiovisivi e dall'altro pongono l'esigenza di garantire nuove forme di tutela del copyright, del pluralismo informativo e dei media e, più in generale, di assicurare un quadro regolamentare al passo con l'evoluzione tecnologica.

2 Le Telecomunicazioni

L'excursus normativo rivela un quadro complesso, nel quale le norme di diretto impatto sull'IA e più in dettaglio sugli algoritmi sono contenute in molteplici plessi normativi relativi a svariati ambiti oggettivi nei quali Agcom, in virtù del suo expertise tecnico multidisciplinare su reti e servizi e sull'analisi di mercato, è candidata ad avere competenze future. Ci si riferisce, per esempio al Digital Services Act (DSA) e al ruolo di Digital Service Coordinator (DSC) da esso istituito, ma anche al Data Act che candida proprio i regolatori delle comunicazioni elettroniche ad attuare la portabilità dei servizi cloud e dei dati digitali.

L'Artificial Intelligence Act (AI Act), in linea con la più recente produzione legislativa europea sui servizi digitali, è un regolamento "orizzontale", destinato ad applicarsi trasversalmente a tutti i settori economici, avendo riguardo alle implicazioni dirette e ai rischi connessi alla diffusione di software e altri strumenti tecnologici fondati sull'impiego di IA.

Il Regolamento è dunque destinato a operare in parallelo, anzi, in sinergia, con i quadri regolamentari settoriali in cui tali prodotti trovano impiego (es: Copyright, protezione dei dati personali).

Sebbene l'IA sia un tema orizzontale, in quanto abilita più funzionalità in settori diversi o la stessa funzionalità utile in più settori, va sottolineato come tale trasversalità funzionale, d'ordine applicativo, sia associata a una di tipo abilitante. Ciò in quanto nessun sistema di IA può funzionare senza dati di addestramento e senza risorse dedicate di tipo hardware e software, che oggi possono essere reperite mediante l'acquisto di servizi di cloud computing.

Servizi questi che iniziano ad essere regolati in vari plessi normativi per varie funzionalità (DMA, DSA, Data Act, IA Act per il machine learning sul quale impatta il servizio cloud MLaaS, machine learning as a service, di cruciale importanza per gli sviluppi dell'AI).

Pertanto, la regolazione di rilievo per i sistemi di intelligenza artificiale non è solo quella specificamente dedicata all'intelligenza artificiale, ma anche quella che introduce le regole per garantire la trasparenza algoritmica, l'accesso e l'utilizzo dei dati digitali, il contrasto alle deepfake ge-

nerate da algoritmi. Per quanto concerne gli ambiti di tutela dell'Autorità, soprattutto il pluralismo informativo e il diritto d'autore, tendono ad essere sempre più pervasi dal ricorso ad algoritmi

Tuttavia, le aree di utilizzo dell'intelligenza artificiale da parte degli operatori sono varie anche nel settore telecomunicazioni

Le reti di telecomunicazioni, caratterizzate da prestazioni sempre più spinte, enorme capillarità di copertura, raccolta di dati da miliardi di oggetti intelligenti e dominio del software per il supporto alle varie funzioni e servizi, sono terreno fertile per l'applicazione delle tecnologie di intelligenza artificiale.

In questo settore, l'intelligenza artificiale gioca un ruolo chiave nell'ottimizzazione delle operazioni di rete, nel miglioramento dell'esperienza del cliente e nella gestione delle infrastrutture. Si tratta infatti di ambiti ove i processi sono altamente digitalizzati e sono disponibili dati digitali per l'addestramento e il funzionamento dei sistemi di IA, in grado di facilitare l'adozione delle tecnologie di IA. Inoltre, la scala delle reti di telecomunicazioni e la complessità della gestione delle reti e della Customer Management Relationship incentivano l'adozione di sistemi automatizzati. È evidente, dunque, come la mappatura dell'impatto dell'IA nel settore delle telecomunicazioni richieda il coinvolgimento degli stakeholders, le serie di dati con cui vengono addestrati i sistemi di IA, l'hardware necessario per far funzionare i sistemi di IA, nonché la comprensione del modo in cui i prodotti e i servizi di telecomunicazione che integrano l'IA vengono utilizzati dai consumatori.

Seguendo i case studies – individuati dal BEREC, nel giugno del 2023, nel "Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation" – è possibile distinguere i seguenti settori: (1) pianificazione e aggiornamento della rete e della capacità trasmissiva; (2) modellazione, previsione e propagazione dei canali; (3) ottimizzazione della qualità del servizio e classificazione del traffico; (4) condivisione dinamica dello spettro; ottimizzazione della qualità del servizio e classificazione del traffico; (5) rilevamento delle minacce e ottimizzazione della sicurezza di reti e servizi; (6) rilevamento e prevenzione delle frodi.

La pianificazione e l'aggiornamento delle reti e delle capacità sono attività nel settore delle telecomunicazioni che richiedono ingenti risorse, sia finanziarie che materiali. Ciò è ulteriormente complicato dal fatto che le reti sono progettate per gestire l'utilizzo futuro previsto, poiché sono costruite per durare per decenni. Allo stesso tempo, la velocità di sviluppo, soprattutto nel settore della telefonia mobile, richiede frequenti modifiche delle reti (roll-out, aggiornamento o migrazione), il che significa che la pia-

nificazione e l'aggiornamento della rete sono attività continue.

La maggior parte della letteratura si concentra sull'uso di applicazioni di intelligenza artificiale nelle reti mobili, tuttavia, esistono anche applicazioni di intelligenza artificiale per le reti fisse. Proprio perché la pianificazione e l'aggiornamento della rete sono un'attività continua e dispendiosa in termini di risorse, le applicazioni di intelligenza artificiale che riducono i costi di implementazione (finanziari o materiali) sono molto interessanti per i fornitori di telecomunicazioni.

Per i fornitori di servizi di telecomunicazione è importante prevedere l'utilizzo di una rete e pianificare l'infrastruttura di conseguenza. La pianificazione della capacità di rete mira a fornire tali previsioni e a ottimizzare la realizzazione o la gestione dell'infrastruttura per far fronte all'utilizzo previsto. Ciò può anche significare che le reti possono essere utilizzate per un periodo di tempo più lungo: ad esempio, nel caso delle reti in fibra ottica, il multiplexing a divisione di spazio utilizzando modelli di intelligenza artificiale può aumentare la capacità di una singola fibra e prolungare la durata dell'infrastruttura esistente, ritardando la necessità di installare nuovi cavi in fibra ottica.

Inoltre, il BEREC individua gli strumenti di cui potranno avvalersi gli stessi regolatori di comunicazioni elettroniche (ANR) per rendere più efficaci ed efficienti i processi decisionali e le attività di monitoraggio sui mercati di riferimento.

Su tali aspetti, il Rapporto segnala altresì i rischi associati alle applicazioni dell'AI nei processi decisionali delle istituzioni pubbliche che dipendono da dati imparziali e affidabili e che, quindi, possono essere negativamente influenzati da una scarsa trasparenza degli algoritmi che utilizzano i dati nei sistemi automatizzati di cui le ANR potrebbero avvalersi. La privacy e la sicurezza rimangono peraltro aspetti importanti che giustificano un attento monitoraggio delle soluzioni di AI realizzate nel contesto regolamentare.

3 L'audiovisivo

Molteplici sono gli *overlapping* regolamentari tra le implicazioni pratiche dell'AI Act e il settore dell'audiovisivo, sebbene, sulla base del Disegno di legge n. 1146 approvato dal Consiglio dei ministri il 23 aprile 2024, non pare profilarsi un ruolo diretto di AGCOM nell'applicazione dell'AI Act.

Seppure sia prematuro, in tale fase, valutare compiutamente l'impatto effettivo sul ruolo di AGCOM rispetto all'AI Act, in assenza di una

norma consolidata, nondimeno si può in questa sede già rilevare che tale Regolamento si intersecherà prevedibilmente con i tanti temi legati all'IA suscettibili di innovare i campi di intervento, già chiari e ben consolidati, dell'Autorità: la tutela dei minori, dell'utenza, diritto d'autore, la promozione del pluralismo e la lotta alla disinformazione. Dalla lettura del DDL si evince, infatti, il richiamo ad alcuni fondamentali principi etici che si intersecano trasversalmente anche con temi di competenza AGCOM: infatti, l'art. 4 del DDL ribadisce, che "L'utilizzo di sistemi di intelligenza artificiale nell'informazione avviene senza recare pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e all'obiettività, completezza, imparzialità e lealtà dell'informazione. […]4. L'accesso alle tecnologie di intelligenza artificiale dei minori di anni quattordici richiede il consenso di chi esercita la responsabilità genitoriale. Il minore degli anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili."

Non sorprende, pertanto, che il medesimo DDL, pur non attribuendo specifiche competenze applicative ad AGCOM, nondimeno già prefigura espressamente un ruolo di questa con riferimento alla tutela dell'utenza nel settore dei media: infatti, all'art. 23 già prevede alcune modifiche al decreto legislativo 8 novembre 2021, n. 208, recante il "*Testo unico dei servizi di media audiovisivi*", nell'applicazione del quale l'autorità competente è AGCOM. Il DDL prevede infatti di aggiungere al già esistente il divieto di utilizzare metodologie e tecniche capaci di manipolare in maniera non riconoscibile allo spettatore il contenuto di informazioni anche le pratiche effettuare "*attraverso l'utilizzo di sistemi di intelligenza artificiale*" (modifica all'Articolo 6, comma 2, lett. e) del Tusma), di inserire un articolo 40-*bis*, in base al quale "*(Contenuti testuali, fotografici, audiovisivi e radiofonici che utilizzano sistemi di intelligenza artificiale) – 1.* Qualunque contenuto informativo diffuso da fornitori di servizi audiovisivi e radiofonici tramite qualsiasi piattaforma in qualsiasi modalità, incluso il video *on demand* e lo *streaming*, che, previa acquisizione del consenso dei titolari dei diritti, sia stato, attraverso l'utilizzo di sistemi di intelligenza artificiale, completamente generato ovvero, anche parzialmente, modificato o alterato in modo tale da presentare come reali dati, fatti e informazioni che non lo sono, deve essere reso, a cura dell'autore o del titolare dei diritti di sfruttamento economico, se diverso dall'autore, chiaramente visibile e riconoscibile da parte degli utenti mediante inserimento di un elemento o segno identificativo, anche in filigrana o marcatura incorporata purché chiaramente visibile e riconoscibile, con l'acro-

nimo "IA" ovvero, nel caso di contenuti audio, attraverso annunci audio ovvero con tecnologie adatte a consentire il riconoscimento. Tale identificazione deve essere presente sia all'inizio della trasmissione e all'inizio del contenuto, sia alla fine della trasmissione e alla fine del contenuto, nonché ad ogni ripresa del programma a seguito di interruzione pubblicitaria. L'inserimento del segno identificativo è escluso quando il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico o fittizio, fatte salve le tutele per i diritti e le libertà dei terzi. Fermo restando quanto previsto dall'articolo 41, per le finalità di cui al presente articolo nonché all'articolo 42, commi 1, lettera *c-bis)*, e 7, lettera *c-bis)*, l'Autorità promuove forme di co-regolamentazione e di autoregolamentazione tramite codici di condotta sia con i fornitori di servizi di media audiovisivi e radiofonici sia con i fornitori di piattaforme per la condivisione di video»".

AGCOM, dunque, seppur non direttamente coinvolta nell'applicazione dell'AI Act, si troverà (laddove, *ça va sans dire*, in corso di *iter* non vi siano modifiche in tal senso) ad assicurare, mediante auto e co-regolamentazione, la trasparenza di contenuti audiovisivi o solo audio, generati da intelligenza artificiale, nei confronti dei consumatori-utenti. Inoltre, vengono incluse nell'ambito di applicazione anche le piattaforme per la condivisione di video (VSP), mediante la modifica proposta all'articolo 42 del Testo unico, in base alla quale i fornitori di VSP soggetti alla giurisdizione italiana devono adottare, tra l'altro, misure adeguate volte a tutelare il grande pubblico da contenuti informativi che siano stati, attraverso l'utilizzo di sistemi di intelligenza artificiale, completamente generati ovvero, anche parzialmente, modificati o alterati in modo da presentare come reali dati, fatti e informazioni che non lo sono; inoltre, questi sono tenuti ad avere una funzionalità che consenta agli utenti che caricano contenuti video generati dagli utenti di dichiarare se tali contenuti video contengono contenuti generati, modificati o alterati, anche parzialmente, in qualsiasi forma e modo, attraverso l'utilizzo di sistemi di intelligenza artificiale di cui sono a conoscenza o di cui si possa ragionevolmente presumere che siano a conoscenza.

Sempre il medesimo DDL prevede, all'art. 24, le necessarie modifiche alla legge sul diritto d'autore confermando la scelta di escludere la tutela autoriale dall'opera generata con l'intelligenza artificiale, allineandosi con quanto già emerso a livello europeo e statunitense.

A tale riguardo vi è, dunque, da mettere in conto, a livello nazionale, un ruolo importante dell'Autorità nell'attuazione, e rispetto, dei principi che presidiano l'utilizzo dell'intelligenza artificiale nei settori di competenza.

Per fare fronte alle sfide imminenti, l'Autorità si è tempestivamente dotata di un supporto qualificato e specializzato in merito alle implicazioni

dei sistemi di intelligenza artificiale sugli ambiti di competenza dell'Autorità e sul ruolo che la stessa potrà assumere, mediante l'istituzione di un Comitato di esperti di alto livello sull'IA, con funzioni consultive (si veda la delibera n. 11/24/CONS).

Inoltre, nella riorganizzazione entrata in vigore lo scorso 1° ottobre, l'Autorità ha altresì istituito uno specifico Ufficio intelligenza artificiale, col compito di svolgere le attività di studio e analisi necessarie al coordinamento delle attività in materia di Big data e intelligenza artificiale anche collaborando con gli specifici Comitati all'uopo istituiti dall'Autorità e in raccordo con le articolazioni rispettivamente interessate della stessa Autorità.

A ciò si aggiunge la necessità di un'armoniosa applicazione del futuro atto di recepimento dell'AI Act, che necessariamente, peraltro, dovrà integrarsi con le previsioni relative ai contenuti online recate dal DSA, la normativa europea di base che regola la "gestione" dei contenuti on line e che introduce in capo alle piattaforme obblighi di trasparenza di rimozione dei contenuti illegali ai sensi del diritto dell'Unione o nazionale, di procedure di ricorso e di gestione dei rischi sistemici, processi di revisione indipendenti e condivisione dei dati con ricercatori selezionati. Pur non menzionando esplicitamente l'"intelligenza artificiale", il DSA contiene, pertanto, diversi riferimenti all'uso di algoritmi e sistemi automatizzati, con specifici obblighi per tutte le piattaforme online a informare sulla moderazione algoritmica dei contenuti e sui sistemi di raccomandazione nei loro termini di servizio. È necessario assicurare, pertanto, che la convergenza dei diversi sistemi normativi conduca a un'applicazione armoniosa, coerente e congruente, e che assicuri un rafforzamento della tutela, anziché un intervento difforme ed eccessivamente frastagliato che avrebbe l'effetto di depotenziare la portata applicativa delle leggi e dei regolamenti europei.

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

Sara Perugini[63]

L'AGCM di fronte all'intelligenza artificiale

Il quadro normativo europeo e nazionale in materia di IA fondato su una visione antropocentrica ha lo scopo di individuare criteri regolatori capaci di bilanciare le opportunità e i rischi offerti dalle nuove tecnologie.
In parallelo, l'uso degli algoritmi, i recenti sviluppi dell'intelligenza artificiale e l'ultima frontiera dell'intelligenza generativa agevolano l'adozione da parte delle imprese di condotte che oltre a produrre un impatto concorrenziale incidono, spesso in modo improprio, sulle scelte dei consumatori.
Il presente contributo intende discutere il ruolo – attuale e futuro – che l'AGCM, attraverso una solida ed equilibrata politica di protezione dei consumatori e di tutela della concorrenza, può giocare per garantire anche in questo settore competitività tra le imprese e benessere dei consumatori.

1 Premessa

L'utilizzo sempre più pervasivo dei modelli e dei sistemi di intelligenza artificiale e lo sviluppo dell'AI generativa hanno indotto l'UE ad adottare, dopo molteplici iniziative di *soft law*[64], il Reg. UE 2024/1689 del

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

[64] Cfr. Commissione Europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, Bruxelles, 19 febbraio 2020; Parlamento Europeo, *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 2020/2012(INL), Bruxelles, 20 ottobre 2020; Consiglio dell'Unione Europea, *Conclusioni della presidenza - La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale*, 11481/20, Bruxelles, 21 ottobre 2020.

13 giugno 2024 entrato in vigore il 1° agosto 2024 (AI Act) [65].

La normativa rappresenta il primo atto di regolamentazione del settore dell'IA a livello globale e si inserisce nel più ampio quadro dei recenti interventi dell'UE adottati in ambito digitale, primi fra tutti, il *Digital Services Act* (DSA) e il *Digital Market Act* (DMA).

L'obiettivo è quello di istituire un quadro giuridico armonizzato[66] promuovendo la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile mediante una classificazione dei sistemi di IA[67] in base al livello di rischio associato al loro uso (inaccettabili, alti, limitati e minimi) per cui maggiore è il rischio e maggiori le responsabilità e i divieti per chi sviluppa o adopera sistemi di intelligenza artificiale.

L'ambito di applicazione soggettivo coinvolge l'intera catena di valore dell'IA, dai fornitori ai distributori, indipendentemente dalla collocazione della loro sede sul territorio dell'UE, purché l'*output* prodotto dal sistema di IA sia utilizzato nell'UE[68].

[65] Il presente regolamento si dovrebbe applicare a decorrere dal 2 agosto 2026. Tuttavia, tenuto conto del rischio inaccettabile associato all'uso dell'IA in determinati modi, i divieti nonché le disposizioni generali del presente regolamento dovrebbero applicarsi già a decorrere dal 2 febbraio 2025. Sebbene la piena efficacia di tali divieti discenda dall'istituzione della governance e dall'esecuzione del presente regolamento, è importante anticipare l'applicazione di detti divieti per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile (cfr. considerando 179).

[66] Il considerando 8 evidenzia che "*Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo, è opportuno stabilire regole che disciplinino l'immissione sul mercato, la messa in servizio e l'uso di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi*".

[67] Ai sensi dell'art. 3 n 1) del Regolamento il sistema di IA è "*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*".

[68] Quanto all'ambito di applicazione oggettivo, il Regolamento non si applica "*ai settori che non rientrano nell'ambito di applicazione del diritto dell'Unione"* nonché *"ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici"* e, in ogni caso, "*non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale*" e "*non osta al mantenimento o all'introduzione da parte degli Stati membri di disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori.*

Sotto il profilo dell'*enforcement*, il Regolamento istituisce un Consiglio europeo per l'intelligenza artificiale per il coordinamento delle politiche nazionali e una uniforme applicazione della normativa e attribuisce alla Commissione la competenza esclusiva per la vigilanza e l'esecuzione del capo V[69] concernente i modelli di IA con finalità generali[70], ivi compreso il potere di infliggere loro sanzioni pecuniarie amministrative nei casi indicati dall'art. 101 del Regolamento[71].

Gli Stati membri dovranno a loro volta istituire autorità nazionali per facilitare una conforme applicazione delle norme del Regolamento e la sorveglianza del mercato e l'applicazione di sanzioni amministrative[72].

Sul piano interno, lo si è accennato nell'introduzione al presente Rapporto, il legislatore nazionale con il disegno di legge n. 1146/2024[73] prevede di introdurre "*misure specifiche adatte al contesto italiano*" che ne rafforzino la competitività assicurando la tutela dei diritti fondamentali mediante la supervisione umana in ogni fase di sviluppo e di utilizzo dei sistemi IA e individuando, a livello di *governance*, l'Agenzia per l'Italia digitale (AGID)[74] e l'Agenzia per la cybersicurezza nazionale (ACN)[75] quali esclu-

[69] Ai sensi dell'art. 88, paragrafo 1, del Regolamento "*La Commissione affida l'attuazione di tali compiti all'ufficio per l'IA, fatte salve le competenze di organizzazione della Commissione e la ripartizione delle competenze tra gli Stati membri e l'Unione sulla base dei trattati*".

[70] La definizione di "modello di IA per finalità generali" è contenuta nell'art. 3 punto 63 del Regolamento.

[71] Ai sensi dell'art. 101 del Regolamento "*La Commissione può infliggere ai fornitori di modelli di IA per finalità generali sanzioni pecuniarie non superiori al 3 % del fatturato mondiale annuo totale dell'esercizio precedente o a 15 000 000 EUR, se superiore, ove essa rilevi che il fornitore, intenzionalmente o per negligenza: a) ha violato le pertinenti disposizioni del presente regolamento; b) non ha ottemperato a una richiesta di documento o di informazioni a norma dell'articolo 91 o ha fornito informazioni inesatte, incomplete o fuorvianti; c) non ha ottemperato a una misura richiesta a norma dell'articolo 93; non ha messo a disposizione della Commissione l'accesso al modello di IA per finalità generali o al modello di IA per finalità generali con rischio sistemico al fine di effettuare una valutazione a norma dell'articolo 92*".

[72] L'entità di queste è definita nel Regolamento e varia in base alla gravità e alla natura dell'infrazione nonché alla dimensione e al fatturato dell'operatore economico responsabile al fine di garantirne la capacità dissuasiva.

[73] "*Disposizioni e delega al Governo in materia di intelligenza artificiale*".

[74] L'AgID è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale e provvede a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale (art. 18 comma 1, lett. a) Reg.).

sive autorità competenti[76].

In parallelo, lo sviluppo dell'AI generativa a partire dal lancio nel novembre 2022 di ChatGPT 3.5. da parte di Open AI – in pochi mesi scaricato e utilizzato da milioni di utenti – ha provocato una corsa allo sviluppo di *software* analoghi da parte di altre grandi imprese digitali concorrenti, sollevando una serie di questioni di rilievo concorrenziale e preoccupazioni di natura consumeristica che l'Autorità *Antitrust* è chiamata ad affrontare.

In tale contesto, scopo della presente analisi, è quello di verificare, dopo un cenno a quanto sino ad oggi fatto, l'impatto delle nuove previsioni europee e nazionali sulle discipline *antitrust* e consumeristiche di competenza dell'AGCM e, al contempo, ragionare sul ruolo attuale e futuro che l'Autorità – stante la possibile geometria europea e nazionale dell'*enforcement* in materia – può giocare per garantire anche in questo ambito competitività tra le imprese e benessere dei consumatori.

2 Intelligenza Artificiale e tutela del consumatore: interventi dell'Agcm

L'intelligenza artificiale mediante il *machine learning,* i *big data* e i vari strumenti che alimenta, sta rivoluzionando il contesto tecnologico delle aziende con un impatto sulla nostra economia e sulla società. I sistemi di intelligenza artificiale stanno infatti diventando parte integrante di molti settori, in particolare dei mercati digitali, consentendo alle aziende di automatizzare le procedure, analizzare grandi quantità di dati e supportare un processo decisionale informato.

Chatbot basati sull'intelligenza artificiale, analisi predittiva e consigli

[75] L'ACN, invece, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale; la stessa autorità nazionale è, altresì, responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza (art. 18 comma 1, lett. b) Reg.).

[76] Ai sensi dell'art. 70, par. 1, del Regolamento "*Ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro*".

personalizzati sono solo alcuni esempi di come queste tecnologie stanno migliorando l'esperienza dei clienti e ottimizzando le operazioni.

Dal lato del consumatore, l'IA offre strumenti potenti per migliorarne la sicurezza e la soddisfazione, ma pone anche nuove sfide che richiedono una scrupolosa attenzione.

L'uso distorto dell'intelligenza artificiale può infatti favorire, specialmente in ambito digitale, l'adozione di condotte scorrette da parte delle imprese alcune delle quali da tempo al centro dell'azione dell'AGCM.

Si pensi al fenomeno delle false recensioni che – oltre ad essere oggetto di specifiche ipotesi di pratiche ingannevoli introdotte nel nostro ordinamento in attuazione della Direttiva c.d. Omnibus[77] – è stato sanzionato dall'Autorità anche prima della riforma.

Recentemente, è stata accertata la vendita da parte di una piattaforma *online* di "interazioni"/"apprezzamenti" tra utenti non riconducibili a utenti reali e/o a reali esperienze di consumo[78] e lo scorso anno è stata sanzionata la vendita di recensioni non autentiche, in quanto generate artificiosamente al fine di promuovere la visibilità, i prodotti o i servizi di chi le acquistava, con l'effetto di alterare le scelte di consumo degli utenti[79].

Lo sfruttamento di tecniche di intelligenza artificiale può, inoltre, generare un indebito condizionamento negli utenti e integrare una pratica commerciale aggressiva.

Un valido esempio in tal senso è rappresentato dalla recente istruttoria chiusa nei confronti di TikTok[80]. Con la decisione – concernente la presenza di video di ragazzi che adottano comportamenti autolesionistici – l'Autorità ha accertato, tra l'altro, la sussistenza di una pratica commerciale aggressiva consistente nell'uso di un sistema di raccomandazione basato su tecniche di profilazione algoritmica che, adoperando i dati degli utenti,

[77] La Direttiva 2019/2161/CE (c.d. Omnibus) e il Decreto Legislativo del 7 marzo 2023, n. 26, di recepimento, hanno dato un notevole rilievo alla necessaria autenticità delle interazioni sui media sociali, tipizzando una nuova fattispecie di pratica in ogni caso ingannevole, ovvero quella di "*inviare, o incaricare un'altra persona giuridica o fisica di inviare, recensioni di consumatori false o falsi apprezzamenti o di fornire false informazioni in merito a recensioni di consumatori o ad apprezzamenti sui media sociali, al fine di promuovere prodotti*", di cui all'art. 23, lett. bb-quater), del Codice del consumo.

[78] Cfr. Provv. n. 31261 dell'11 giugno 2024 PS12665 in Boll. 26/2024.

[79] Cfr. Provv 30574 del 28 marzo 2023, PS12371, in Boll. 29/2023. L'istruttoria è stata condotta ai sensi degli artt. 20 e 21 del Codice del consumo, prima dell'attuazione a livello nazionale della Direttiva c.d. *Omnibus*.

[80] Cfr. Provv. 31124, del 5 marzo 2024, PS12543, in Boll. 11/2024.

personalizza la visualizzazione della pubblicità e ripropone contenuti simili a quelli già visualizzati e con cui si è interagito attraverso la funzione *like*.

Il ricorso alla disciplina in materia di pratiche commerciali scorrette può mitigare anche le ripercussioni che le scelte commerciali dei consumatori hanno nei servizi supportati dall'intelligenza artificiale sul trattamento dei dati personali. È quanto contestato in un caso ancora in corso avviato nei confronti di una piattaforma avente ad oggetto l'utilizzo, attraverso la profilazione algoritmica, dei dati degli utenti finalizzata a personalizzare la visualizzazione della pubblicità, inducendoli indebitamente ad un uso crescente della piattaforma[81].

Altre criticità che possono emergere dalla diffusione di sistemi di IA generativa sono legate alla proliferazione di pubblicità occulte, di pubblicità talmente personalizzate sulle caratteristiche e fragilità personali (o *bias* cognitivi) da poter diventare manipolative, nonché di nuove forme più sofisticate di attacchi di *phishing*.

3 AI Act e Codice del Consumo

In tale contesto viene innanzitutto da chiedersi se l'entrata in vigore del Regolamento europeo e la futura adozione del disegno di legge nella sua attuale formulazione possano generare, sotto il profilo sostanziale, interferenze con le discipline consumeristiche di competenza dell'Autorità[82].

Invero, se da un lato, il diverso interesse tutelato dal Regolamento porterebbe ad escludere la sussistenza di un rischio di interferenza con le discipline di vocazione consumeristica, dall'altro, una più attenta analisi porta a rilevare come il provvedimento europeo contenga nozioni che si intersecano con le fattispecie contenute nel Codice del Consumo.

Già ad una prima lettura, la nozione stessa di "pratiche di IA vietate"[83] contenuta nel Regolamento europeo nell'ambito dei sistemi AI che

[81] Cfr. comunicato stampa Google PS12714.

[82] L'entrata in vigore del Regolamento pone questioni di sovrapposizione anche con altre discipline già in vigore in campi ad essa vicini se non sovrapponibili. Si pensi al *Digital Service Act* e a come andrebbero chiariti tra l'altro il regime giuridico e i requisiti per le VLOP nel processo di adeguamento alla nuova normativa o al *Data act* il cui obiettivo primario è migliorare l'accesso e l'uso dei dati derivanti dagli strumenti e richiederà una riflessione sui processi decisionali basati su informazioni acquisite da detti strumenti grazie all'IA.

[83] Ai sensi dell'art. 5 lett. a) e b) del Regolamento vi rientrano, tra le altre, "*l'immissione sul*

pongono rischi inaccettabili vietati nel mercato interno dell'UE, appare costruita sulla falsariga della nozione di pratica commerciale scorretta (*rectius* sleale di cui alla Direttiva 2005/29/CE) e con essa in parte coincide.

Pur distinguendosi da quest'ultima in termini di ampiezza e di requisiti – a ben vedere anche più stringenti[84] – la fattispecie appare atta a ricomprendere, in assenza di norme che ne escludono esplicitamente l'applicazione, anche condotte ingannevoli che, mediante l'uso di un sistema di IA, appaiono idonee a "*distorcere il comportamento di un consumatore*" e ad incidere su decisioni di "*natura commerciale*" e, dunque, condotte vietate dal Codice del Consumo.

Vengono altresì in rilievo gli obblighi di trasparenza cui sono soggetti i sistemi di IA che presentano "*rischi limitati*" come l'obbligo di informare gli utenti che i contenuti sono generati ricorrendo all'IA, in modo che possano prendere decisioni informate in merito all'ulteriore utilizzo (art. 50 Reg.).

Un tipico esempio è rappresentato da sistemi di IA come i *chatbot*: i destinatari devono essere informati del fatto che stanno interagendo con una macchina in modo che possano prendere una decisione informata se continuare o fare un passo indietro e i *provider* devono anche garantire che

mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo" ovvero "*l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo*".

[84] Rispetto alla nozione di pratica commerciale contenuta nel Codice del Consumo la nozione di pratica di IA di cui all'art. 5 lett. a) Cod. cons. appare per un verso, più ampia in quanto atta a ricomprendere condotte idonee ad incidere su qualsiasi decisione anche di natura non commerciale; per altro verso connotata da requisiti più stringenti. Perché si configuri una pratica in violazione dell'art. 5 del Regolamento, infatti, a differenza di quanto richiesto dagli artt. 18 e ss. del Codice del Consumo, deve ricorrere l'elemento soggettivo della volontà ("*tecniche volutamente manipolative e ingannevoli*") nonché l'idoneità della condotta a generare un *danno significativo* nei destinatari. Sul punto il considerando 29 chiarisce che "*non è necessario che il fornitore o il deployer abbiano l'intento di provocare un danno significativo, purché tale danno derivi da pratiche manipolative o di sfruttamento consentite dall'IA*".

il contenuto generato dall'IA sia identificabile. Ciò si applica anche ai contenuti audio e video che costituiscono *deep fake*.

La violazione dei suddetti obblighi qualora idonea ad incidere su una decisione di natura commerciale, potrebbe integrare una omissione ingannevole in violazione dell'art. 22, comma 5, cod. cons.

Rilevano, ancora a titolo esemplificativo, le disposizioni che incoraggiano l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti previsti per questi ultimi (art. 95 Reg.)[85].

È noto, infatti, come gli impegni che il professionista assume aderendo ad un codice di condotta assumano rilevanza nell'ambito della disciplina in materia di pratiche commerciali scorrette integrando, qualora disattesi, una azione ingannevole in violazione dell'art. 21 comma 2, lett. b) Cod. cons. ovvero ipotesi di pratiche commerciali di per sé ingannevoli in violazione dell'art. 23, comma 1 lett. a) e c) Cod. cons. Più in generale, il professionista potrebbe incorrere in una violazione dell'art. 21, comma 2, lett. b) Cod. cons. anche in relazione a codici di condotta che non rientrano nelle suddette fattispecie.

Rispetto a queste e ad altre interferenze sostanziali che potrebbero presentarsi nel caso concreto, l'interprete è chiamato ad applicare il modello sancito dalla sentenza della Corte di Giustizia del 13 settembre 2018 secondo cui il *contrasto* cui si riferisce l'articolo 3, paragrafo 4, della Direttiva 2005/29/Ue, da un lato, riguarda solo norme dell'Unione e non norme nazionali che non costituiscono diretta trasposizione di disposizioni europee; dall'altro, che lo stesso sussiste solo quando disposizioni estranee alla Direttiva 2005/29/Ue, disciplinanti *aspetti specifici* delle pratiche commerciali sleali, impongono ai professionisti, senza alcun margine di manovra, *obblighi incompatibili* con quelli stabiliti dalla Direttiva 2005/29/Ue, dando vita ad una divergenza che non ammette la coesistenza di entrambi i plessi normativi[86].

---

[85] Ai sensi dell'art. 95 paragrafo 3, del Regolamento "*I codici di condotta possono essere elaborati da singoli fornitori o deployer di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione di qualsiasi portatore di interessi e delle sue organizzazioni rappresentative, comprese le organizzazioni della società civile e il mondo accademico. I codici di condotta possono riguardare uno o più sistemi di IA tenendo* conto *della similarità della finalità prevista dei sistemi pertinenti*".

[86] La giurisprudenza amministrativa successiva, nel tentativo di esplicitare la suddetta incompatibilità, ha evidenziato che *«Per contrasto deve intendersi non la mera difformità, bensì un rapporto di incompatibilità che non permetta la coesistenza di entrambe le realtà normative»* (Consiglio di Stato, VI, 31 dicembre 2021, n. 8757, PS1747-*Arkopharma-4321 SLIM*) e ha rilevato

Applicato al rapporto in esame, stante l'indubbio rango europeo del Reg. UE 2024/1689, la disciplina in materia di pratiche commerciali scorrette dovrà considerarsi recessiva rispetto al Regolamento unicamente nei casi di *incompatibilità assoluta* tra norme e limitatamente allo *specifico aspetto* considerato.

Nel merito, l'analisi che precede conduce, *prima facie*, ad un giudizio di complementarità tra le due discipline data l'assenza, almeno in astratto, di prescrizioni tra loro incompatibili che diano vita ad una *divergenza insanabile*.

Un conforto a favore di tale interpretazione viene, del resto, dallo stesso legislatore europeo che, a più riprese, sottolinea la *complementarità* tra le prescrizioni del Regolamento e il vigente diritto dell'Unione in materia di tutela dei consumatori[87]. Inoltre, con riferimento alle pratiche di IA il Regolamento esplicitamente prevede che il divieto "*è complementare alle disposizioni contenute nella direttiva 2005/29/CE*"[88].

A corollario, sul piano del rapporto tra discipline, potrà farsi applicazione della disciplina in materia di pratiche commerciali sia nel caso di comportamenti non conformi al Regolamento che nel caso di comportamenti che si presentino, per quello specifico aspetto, conformi a prescrizioni del Regolamento, purché tali prescrizioni siano "compatibili" rispetto

---

che *«Il contrasto sussiste solo quando disposizioni di stretta derivazione UE, disciplinanti aspetti specifici delle pratiche commerciali sleali, impongono ai professionisti, senza alcun margine di manovra, obblighi "incompatibili" con quelli stabiliti dalla direttiva 2005/29, dando vita a una divergenza insanabile che non ammette la coesistenza di entrambi i plessi normativi»* (Consiglio di Stato, VI, 27 dicembre 2021, n. 8620, PS50 - *Telecom-Disservizi passaggio ad altro operatore*) ovvero che *«Il citato "criterio di incompatibilità" implica che tra le due discipline sussista una complessiva divergenza di contenuti che non ne consenta l'astratta coesistenza»* (Consiglio di Stato, VI, 5 giugno 2020, n. 3575, PS10666 *ATAC – Soppresse corse ferroviarie*).

[87] Il considerando 9 del Regolamento recita: "*Le norme armonizzate stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in linea con il nuovo quadro legislativo, non dovrebbero pregiudicare il vigente diritto dell'Unione, in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e protezione dei lavoratori e sicurezza dei prodotti, al quale il presente regolamento è complementare. Di conseguenza, restano impregiudicati e pienamente applicabili tutti i diritti e i mezzi di ricorso previsti da tali disposizioni di diritto dell'Unione a favore dei consumatori e delle altre persone su cui i sistemi di IA possono avere un impatto negativo, anche in relazione al risarcimento di eventuali danni a norma della direttiva 85/374/CEE del Consiglio*". Inoltre, secondo il considerando 45 "*il presente regolamento non dovrebbe incidere sulle pratiche vietate dal diritto dell'Unione, ivi incluso dal diritto in materia di protezione dei dati, non discriminazione, protezione dei consumatori e concorrenza*".

[88] Cfr. il considerando 29.

alla disciplina in materia di pratiche commerciali[89].

Una diversa valutazione deve essere riservata, almeno in linea di principio, alle norme contenute nel disegno di legge n. 1146/2024 rispetto alle quali non trova applicazione il modello seguito dalla Corte di giustizia in quanto prive di rango europeo.

In proposito c'è da dire tuttavia che il testo, nella sua attuale formulazione, non sembra contenere prescrizioni che interferiscono con la disciplina in materia di pratiche commerciali[90].

Ulteriori questioni si pongono sotto il profilo dell'*enforcement*.

Il Regolamento affida ampi e rilevanti poteri di vigilanza agli Stati Membri che sono tenuti a designare almeno una autorità di notifica e almeno una autorità di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del Regolamento[91].

Come evidenziato in premessa, il Governo ha presentato il disegno di legge 1146/2024, attualmente approvato dal Senato[92] che designa come autorità nazionali per l'intelligenza artificiale l'Agenzia per l'Italia Digitale (funzione di notificazione) e l'Agenzia per la Cybersicurezza Nazionale (funzione di controllo) e demanda loro il compito di assicurare "*il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipen-*

[89] Ciò che ne discende è la possibilità per l'Autorità di continuare ad accertare e sanzionare condotte che facciano uso di sistemi di IA vietati dal Regolamento (art. 5 lett. a) e b) che incidono su decisioni di natura commerciale. Diversamente, ricadranno nell'esclusivo ambito di applicazione della novella e della competente Autorità nazionale (AGID) tutte quelle pratiche di IA vietate che incidono su decisioni non commerciali purché, naturalmente, presentino gli ulteriori requisiti previsti dalla fattispecie (volontarietà, danno potenziale ecc.). Allo stesso modo, i *chatbot* che non chiariscano l'uso di intelligenza artificiale, saranno contrari all'art. 50 del Regolamento e, qualora utilizzati in ambito commerciale, suscettibili di integrare una omissione ingannevole in violazione dell'art. 22, comma 5 Cod. cons. accertata e sanzionata dalla sola Autorità in applicazione dell'art. 27 comma 1 bis cod. cons.

[90] Il decreto, infatti, introduce norme in materie come la salute, la sicurezza e il diritto di autore oggetto di specifiche clausole di salvaguardia contenute nel Codice del Consumo (art. 19 comma 2 cod. cons.) o, come nel caso dei *deepfake,* nuove fattispecie di reato.

[91] Secondo il considerando 154 "*Le autorità nazionali competenti dovrebbero esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità dovrebbero astenersi da qualsiasi atto incompatibile con le loro funzioni e dovrebbero essere soggetti alle norme in materia di riservatezza ai sensi del presente regolamento*".

[92] Cfr. il link <https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm >.

denti" (art. 18).

Viene pertanto da chiedersi quale sia il rapporto tra le azioni amministrative rispettivamente esercitate dall'AGCM in materia di pratiche commerciali scorrette e dalle suddette autorità competenti in materia di IA.

Sul punto, non sembra possa dubitarsi dell'applicazione, anche in tale ambito, del criterio di ripartizione preventiva delle competenze sancito dall'art. 27 co. 1-bis Cod. cons. con conseguente competenza dell'Autorità ad accertare la scorrettezza di pratiche commerciali scorrette integranti contestualmente anche violazioni del Regolamento. L'Autorità sarà inoltre tenuta, nel caso di pratiche commerciali che facciano uso di sistemi di IA, a richiedere il parere settoriale previsto dalla medesima disposizione.

Ciò che ne discende è la possibilità per l'Autorità di continuare ad accertare e sanzionare condotte che facciano uso di sistemi di IA vietati dal Regolamento (art. 5 lett. a) e b) che incidono su decisioni di natura commerciale.

Diversamente, ricadranno nell'esclusivo ambito di applicazione della novella e della competente Autorità nazionale (AGID) tutte quelle pratiche di IA vietate che incidono su decisioni non commerciali purché, naturalmente, presentino i requisiti ulteriori richiesti dalla fattispecie (volontarietà, danno potenziale ecc.).

Allo stesso modo, i *chatbot* che non chiariscano l'uso di intelligenza artificiale, saranno contrari all'art. 50 del Regolamento e, qualora utilizzati in ambito commerciale, suscettibili di integrare una omissione ingannevole in violazione dell'art. 22, comma 5 Cod. cons. accertata e sanzionata dalla sola Autorità in applicazione dell'art. 27 comma 1 bis cod. cons.

Pertanto, da un lato, l'assenza di ipotesi di incompatibilità sostanziale tra le singole prescrizioni dell'IA Act e le disposizioni in materia di pratiche commerciali scorrette e, dall'altro, l'operatività del criterio di ripartizione preventiva di cui all'art. 27 co. 1bs Cod. cons. appaiono scongiurare che, in questa materia, possa configurarsi il rischio di una concreta violazione del principio *ne bis in idem*[93]. Rispetto ai poteri di *enforcement* attributi alla Commissione che, come detto, ha la competenza esclusiva per la vigilanza e l'esecuzione del capo V concernente i modelli di IA con finalità generali, ivi

[93] Del resto, alla luce più recente giurisprudenza del Consiglio di Stato e del TAR Lazio, in materia di pratiche commerciali scorrette stante la vigenza dell'art. 27 comma 1-*bis* Cod. cons., l'operatività del principio del *ne bis in idem* e delle condizioni elaborate dalla giurisprudenza della Corte di Giustizia al ricorrere delle quali sarebbero ammesse limitazioni al principio stesso deve essere esclusa proprio in forza della presenza del suddetto criterio di ripartizione preventiva.

compreso il potere di infliggere ai fornitori di tali modelli sanzioni pecuniarie amministrative nelle ipotesi di cui all'art. 101 del Regolamento, non sembra possano presentarsi casi di interferenza con le competenze dell'Autorità in materia. La figura del fornitore, infatti, stando alla definizione offerta dal Regolamento[94], non sembra essere destinata a intrattenere rapporti con gli utenti finali e, dunque, per quanto di interesse a porre in essere pratiche commerciali scorrette vietate dal Codice del Consumo.

Sul punto conviene tuttavia ricordare che, nel caso in cui dovesse verificarsi una ipotesi di condotta pluri-offensiva soggetta all'*enforcement* della Commissione ex art. 101 del Regolamento e all'*enforcement* dell'AGCM, l'art. 27 comma 1 bis cod. cons. non troverebbe applicazione in quanto circoscritto all'ambito nazionale. In questo caso, troverebbe applicazione l'art. 50 della Carta dei diritti fondamentali dell'Unione europea e, nello specifico, il rispetto delle condizioni richieste dalla giurisprudenza euro-unitaria per ammettere limitazioni all'applicazione del principio del *ne bis in idem* ivi sancito[95], tra cui, il rispetto del principio di leale collaborazione tra gli organismi

[94] Cfr. art. 3, punto 3) del Reg. "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito*".

[95] Come noto, per essere ritenuto giustificato un cumulo di procedimenti o sanzioni per gli stessi fatti deve soddisfare tre condizioni: i) che tale cumulo non costituisca un onere eccessivo per l'interessato; ii) che esistano norme chiare e precise che consentano di prevedere quali atti e omissioni possano essere oggetto di cumulo; iii) che i procedimenti in questione siano stati condotti in modo sufficientemente coordinato e ravvicinato nel tempo. In proposito viene in rilievo la sentenza della Corte di Giustizia del 14 settembre 2023 resa a seguito del rinvio pregiudiziale disposto dal Consiglio di Stato nell'ambito del contenzioso tra l'AGCM e le società Volkswagen Group Italia S.p.A. (VW Italia) e Volkswagen Aktiengesellschaft (VW AG) sul caso PS10211 - *Volkswagen-emissioni inquinanti autoveicoli diesel*. La Corte di Giustizia – nel chiarire le condizioni che possono giustificate limitazioni all'applicazione del principio del *ne bis in idem* – declina in modo nuovo il principio di leale collaborazione tra autorità. La Corte afferma espressamente che "*Il coordinamento di procedimenti o sanzioni riguardanti gli stessi fatti può certamente rivelarsi più difficile qualora, come nel caso di specie, le autorità di cui trattasi appartengano a Stati membri diversi. Sebbene occorra prendere in considerazione i vincoli pratici propri di tale contesto transfrontaliero, questi ultimi non possono giustificare che si relativizzi detto requisito o che non se ne tenga conto*". La Corte mostra di considerare indispensabile il requisito del coordinamento tra i procedimenti istruttori per ammettere la suddetta deroga, anche in occasione del cumulo di procedimenti di due Stati membri che siano stati avviati da autorità competenti in diversi settori di attività e in assenza di un meccanismo giuridico di coordinamento dei loro interventi.

deputati al controllo e, dunque, in questo caso tra Commissione e Autorità.

4 Intelligenza Artificiale e criticità concorrenziali: cenni

L'avanguardia delle tecnologie di IA e la loro integrazione nel *business* delle aziende, costituisce la chiave per mantenere un vantaggio competitivo nel mercato.

Lo stesso disegno di legge n. 1146/2024 al fine di accrescere la competitività del sistema economico nazionale nel settore dell'IA pone come principio generale, tra gli obiettivi dello Stato e delle altre Autorità pubbliche, la promozione della concorrenza unita a innovatività ed equità (art. 5).

Il mercato dell'intelligenza artificiale, tuttavia, presenta molteplici criticità concorrenziali sulle quali, non a caso, si è concentrato il Summit dei membri del G7 Concorrenza Italia (*G7 Competition Authorities and Policymakers' Summit*) svolto presso la sede dell'AGCM nelle scorse giornate del 3 e 4 ottobre[96].

Ciò che preoccupa è, in primo luogo, la capacità delle grandi aziende digitali con un potere sostanziale nei contigui mercati digitali di consolidare o estendere tale potere nei mercati adiacenti dell'AI.

Tale rischio è amplificato dagli effetti di rete, dal riutilizzo degli *output* come *input* per affinare i modelli di fondazione AI (*data feedback loop*) e dall'integrazione in ecosistemi non contendibili e scarsamente competitivi[97]. Elementi questi ultimi che possono determinare barriere all'ingresso, ostacoli alla concorrenza e una riduzione del benessere dei consumatori. Un ulteriore timore riguarda la possibilità che gli *incumbent* del mercato digitale possano – in ragione della complessa serie di *partnership* sussistente con altre aziende di AI – ostacolare la concorrenza. L'acquisizione di talenti

[96] Cfr. *Discussion Paper for the G7 Competition Summit* e il *G7 2024 - Digital Competition Communiqué* allegati al comunicato stampa del 4 ottobre 2024 <https://www.agcm.it/media/comunicati-stampa/2024/10/G7-Concorrenza-le-Autorita-contro-i-rischi-dell-IA>.

[97] Lungo la filiera dell'AI si assiste, in particolare, all'integrazione verticale delle grandi aziende digitali anche attraverso accordi, alleanze strategiche e/o l'acquisizione di partecipazioni di minoranza nelle fasi a monte (talvolta stipulati con modalità che sfuggono allo scrutinio sulle concentrazioni delle autorità *antitrust*), con esiti che favoriscono il consolidamento di ecosistemi integrati (in tutte le fasi), limitatamente sostituibili tra loro sotto il profilo concorrenziale.

(forza lavoro qualificata) e la definizione di alleanze strategiche[98], potrebbe consentire agli operatori digitali esistenti di sfuggire ai controlli *antitrust*, consolidando al contempo la rispettiva posizione dominante e indebolendo la concorrenza nel settore dell'AI.

Si pensi al caso Microsoft e Open I concernente l'assunzione da parte di Microsoft di diversi dipendenti e soprattutto dirigenti della start-up Inflection. Mustafa Suleyman, uno dei protagonisti del settore dell'IA a livello mondiale, aveva annunciato a marzo di voler lasciare il suo incarico di amministratore delegato di Inflection, da lui co-fondata, per unirsi al colosso americano, insieme ad altri dipendenti chiave dell'azienda, come un altro co-fondatore, Karén Simonyan. Lo scorso settembre l'Autorità *antitrust* britannica ha annunciato la chiusura dell'indagine ritenendo che non vi sono rischi per la concorrenza in quanto, così come nel precedente via libera alla *partnership* siglata tra Microsoft e la francese Mistral, non sono stati riscontrati i presupposti di una fusione societaria.

Un'ulteriore criticità attiene alla possibilità che l'uso dell'AI e degli algoritmi faciliti la collusione tra le imprese, consentendo loro di coordinare i prezzi, condividere informazioni sensibili e minare la concorrenza. Inoltre, è possibile che le tecnologie di AI vengano impiegate per attuare forme di discriminazione di prezzo, a danno dei consumatori e delle dinamiche di mercato.

Né sembra che possa essere trascurato l'emergere di pratiche anticoncorrenziali da parte di imprese già attive nell'AI. Condotte quali il *self-preferencing*, la vendita abbinata o aggregata (*tying or bundling*), limitano di fatto la scelta dei consumatori e aumentano le barriere all'ingresso per le imprese di minori dimensioni e le *start-up*.

Un ultimo profilo, non per questo meno rilevante, attiene all'eccessiva concentrazione dei principali fattori per lo sviluppo di soluzioni AI. Ciò può favorire l'insorgere di posizioni dominanti in capo a un numero ristretto di imprese, in grado di sfruttare i colli di bottiglia esistenti o emergenti, ridurre la concorrenza e limitare l'accesso al mercato a nuovi operatori. Anche l'accesso alle risorse energetiche rappresenta una preoccupazione crescente in quanto i modelli di fondazione AI continuano ad aumentare in dimensione e complessità.

Simili preoccupazioni concorrenziali richiedono una applicazione tempestiva e vigorosa del diritto *antitrust* (*ex post*) e dei suoi principi guida[99]

[98] Quale modalità alternativa all'acquisizione diretta di asset, suscettibili di integrare le c.d. *killer acquisition* e, quindi, soggette a scrutinio *antitrust* in talune giurisdizioni.

[99] Quali i principi di concorrenza non falsata, accesso al mercato e opportunità, scelta per

e, date le caratteristiche del mercato, un costante monitoraggio da parte dell'Autorità degli sviluppi della filiera dell'IA, per anticipare e affrontare i potenziali rischi per la concorrenza e per formulare soluzioni di *policy*.

Accanto all'applicazione tradizionale del diritto della concorrenza un ruolo tutt'altro che neutrale nel mercato dell'IA è affidato anche alla regolamentazione *ex ante* contenuta nel *Digital Market Act* che nei limitrofi mercati digitali stabilisce regole per prevenire comportamenti anticoncorrenziali da parte delle grandi piattaforme[100].

Difatti, per un verso, alcune delle preoccupazioni concorrenziali che caratterizzano la filiera dell'IA sono oggetto di specifici divieti posti a carico dei *gatekeepers* stabiliti per mercati digitali dal DMA. Si pensi a condotte quali il *self-preferencing*, la vendita abbinata o aggregata (*tying or bundling*) che, nei mercati digitali, il DMA mira a contrastare mediante la prevenzione dell'autopreferenzialità e la facilitazione dell'interoperabilità con altre piattaforme. Si pensi anche all'accesso ai dati e all'obbligo imposto ai *gatekeepers* dal DMA di consentire ai propri utenti aziendali di accedere ai dati generati durante l'utilizzo delle piattaforme. Un obbligo che, è prevedibile, spiegherà effetti anche per la prevenzione del consolidamento di posizioni di vantaggio competitivo nella disponibilità di dati proprietari derivante dall'intensificarsi di accordi di partnership e/o di licenza che legano gli sviluppatori alle grandi imprese digitali[101].

Per altro verso, i *gatekeepers* destinatari del DMA offrono servizi che – come emerge anche dalle indagini di «non conformità» al DMA avviate dalla Commissione verso Apple, Google e Meta – sono basati in molti casi sull'uso di sistemi di intelligenza artificiale.

È dunque evidente che, anche i *gatekeepers* in qualità di utilizzatori dei sistemi di IA, dovranno conformarsi alle regole dettate dall'IA Act e saranno considerati responsabili in caso di mancata conformità, a meno che non decidano di bloccare negli Stati europei l'introduzione dei suddetti servizi[102].

Pertanto, da un lato, l'*IA Act* si intersecherà inevitabilmente con il

---

i consumatori/utenti, interoperabilità, innovazione, trasparenza e responsabilità (accountability).

[100] Sul rapporto tra regolazione *ex ante* ed *ex post* nel settore cfr. Rapporto OCSE Rapporto dell'OCSE sull'impatto delle regolamentazioni dei mercati digitali nei Paesi G7.

[101] In materia di dati, occorre tenere presente anche il Regolamento 2023/2854 (c.d. Data Act) che entrerà in vigore il 12 settembre 2025.

[102] È quanto, ad esempio, dichiarato da Apple in relazione a servizi che fanno uso di sistemi di IA applicati altrove per migliorare l'assistente Siri.

DMA e dall'altro, l'Autorità in qualità di autorità nazionale competente per la sua attuazione, avrà un ruolo significativo nel rilevare condotte poste in essere dai *gatekeepers* nella filiera dell'IA analoghe a quelle vietate nel mercato digitale dal DMA, nonché nel monitoraggio delle eventuali violazioni di regole sui mercati digitali delle imprese attive nel segmento dell'IA.

5 Conclusioni

Il quadro europeo e nazionale brevemente descritto cerca di disciplinare l'intelligenza artificiale in tutti gli aspetti del suo dispiegarsi, ma deve fare i conti con uno sviluppo tecnologico imprevedibile nei tempi e nelle direzioni in cui si muoverà.

L'analisi che precede mostra, tuttavia, come l'entrata in vigore del Regolamento europeo e la *governance* che va delineandosi in ambito nazionale non costituisca un ostacolo all'azione di *enforcement* dell'AGCM che, dotandosi delle competenze e degli strumenti tecnologici necessari ad affrontare la natura complessa e dinamica dell'IA e dei mercati digitali e agendo sul doppio binario della tutela del consumatore e di promozione della concorrenza, potrà continuare a svolgere un ruolo centrale nelle sfide poste dall'era digitale[103].

[103] L'AGCM – così come sta progressivamente avvenendo in altre Istituzioni e Autorità di Vigilanza – si è recentemente dotata di una Unità di Data Science. Cfr. comunicato stampa del 22 luglio 2024 al link <https://www.agcm.it/media/comunicati-stampa/2024/7/Creata-l-Unita-Data-Science-dell-AGCM>.

Autorità di Regolazione dei Trasporti

Federico Nespega

L'intelligenza artificiale nel settore dei trasporti pubblici

Il Regolamento europeo sull'intelligenza artificiale (AI Act) distingue chiaramente gli obblighi posti a carico degli sviluppatori e degli utilizzatori, affiancando alla priorità della sicurezza un approccio normativo orientato alla centralità dell'essere umano. In questa prospettiva, l'enfasi su trasparenza, spiegabilità e protezione dell'utente si traduce in un sistema di garanzie che richiama, anche implicitamente, la figura del consumatore medio.

Tra i settori regolati, quello dei trasporti si configura come ambito privilegiato di applicazione dell'intelligenza artificiale, in virtù del potenziale trasformativo delle tecnologie intelligenti nel migliorare l'efficienza operativa, ridurre le esternalità ambientali e ottimizzare le interazioni tra utenti, operatori, amministrazioni pubbliche e autorità di regolazione.

Una corretta attuazione del Regolamento europeo, anche mediante gli strumenti normativi nazionali (a partire dal disegno di legge attualmente in discussione), risulta determinante per delineare in modo chiaro le competenze delle diverse autorità coinvolte, tra cui AGID, ACN e l'Autorità di Regolazione dei Trasporti (ART).

1 Il potenziale dell'IA nei trasporti pubblici: innovazione e trasformazione sistemica

L'intelligenza artificiale (IA) rappresenta una delle tecnologie abilitanti più rilevanti nella trasformazione dei sistemi di trasporto, in particolare nel contesto della mobilità pubblica. Grazie alla capacità di elaborare grandi volumi di dati e di apprendere dai flussi informativi in tempo reale, l'IA permette una gestione predittiva, adattiva e personalizzata della mobilità urbana. Ciò risponde a esigenze crescenti di efficienza, sostenibilità e inclusività, ponendo tuttavia nuove sfide istituzionali e regolatorie.

Dal punto di vista giuridico-economico, l'introduzione dell'IA sollecita una ridefinizione delle funzioni delle autorità pubbliche, chiamate a esercitare un ruolo attivo non solo nella regolazione *ex post*, ma anche nella programmazione, selezione e valutazione degli strumenti tecnologici adottati. La transizione digitale non può infatti essere considerata un processo neutro, ma un cambiamento sistemico che incide sui rapporti tra pubblico e privato, sull'allocazione delle risorse e sulla protezione degli interessi generali.

In tale contesto, la regolazione dell'IA nei trasporti assume una duplice funzione: abilitante, in quanto crea le condizioni per uno sviluppo tecnologico conforme all'interesse collettivo; conformativa, poiché orienta tale sviluppo verso finalità compatibili con i principi di equità, accessibilità e sicurezza. La crescente diffusione di soluzioni algoritmiche impone, inoltre, una riflessione critica sulla distribuzione del potere decisionale, sulla trasparenza dei processi e sulla responsabilità connessa alle scelte automatizzate. Le autorità pubbliche devono pertanto promuovere un ecosistema di mobilità intelligente che non sia solo tecnicamente efficiente, ma anche democraticamente legittimato e orientato alla giustizia sociale.

2 L'impatto dell'IA nella mobilità urbana: governance, infrastrutture e diritti

L'adozione dell'intelligenza artificiale nel settore dei trasporti urbani sta trasformando in profondità la natura dei servizi pubblici di mobilità, influenzando i modelli organizzativi, i criteri allocativi e le modalità di interazione tra amministrazioni pubbliche e attori privati. L'impiego di tecnologie intelligenti abilita una gestione integrata e dinamica della rete urbana, attraverso piattaforme digitali, sistemi predittivi e strumenti di automazione capaci di ottimizzare l'intermodalità e la personalizzazione dell'offerta.

Tuttavia, tale trasformazione non è neutra rispetto alla distribuzione del potere decisionale. Le autorità pubbliche non sono più meri regolatori *ex post*, ma diventano co-decisori nella definizione e gestione delle infrastrutture tecnologiche, spesso in partenariato con operatori privati e grandi piattaforme digitali. Ciò solleva interrogativi in merito alla trasparenza delle scelte, alla responsabilità delle decisioni algoritmiche e alla tutela dei diritti fondamentali.

I sistemi di gestione automatizzata del traffico, basati su modelli di *machine learning*, offrono vantaggi evidenti in termini di efficienza. Tuttavia, possono produrre effetti collaterali significativi, come la marginalizzazione delle aree periferiche, discriminazioni indirette o la prioritizzazione delle utenze più redditizie. Tali rischi richiedono un attento bilanciamento tra logiche di ottimizzazione e obiettivi di equità territoriale e coesione sociale.

Dal punto di vista normativo, emerge la necessità di integrare i principi tradizionali del diritto amministrativo con le nuove esigenze poste dalla regolazione algoritmica. Il Regolamento europeo sull'intelligenza artificiale *(AI Act)* sottolinea l'importanza di garantire la sorveglianza umana, la documentazione dei processi decisionali e la responsabilità per gli esiti automatizzati, soprattutto nei settori ad alto impatto sociale come i trasporti pubblici.

Inoltre, la disponibilità di dati granulari e in tempo reale sta modificando anche le logiche economiche alla base dei servizi: sistemi di tariffazione dinamica, segmentazione dell'offerta, valutazione istantanea della *performance* pongono nuove sfide in termini di protezione dei dati, non discriminazione e accesso universale. Le autorità amministrative devono pertanto agire come garanti di un equilibrio tra innovazione e diritti, definendo regole chiare, strumenti di valutazione dell'impatto algoritmico e meccanismi di correzione capaci di prevenire forme di esclusione digitale.

3 L'IA per la pianificazione della mobilità urbana sostenibile: verso città intelligenti ed inclusive

La pianificazione urbana svolge un ruolo cruciale nella capacità delle città di governare i processi di innovazione tecnologica applicati alla mobilità. In particolare, l'intelligenza artificiale consente di superare i tradizionali limiti informativi che ostacolavano lo sviluppo di politiche integrate e sostenibili. L'uso di dati in tempo reale e di modelli predittivi supporta la simulazione del comportamento dei viaggiatori, l'individuazione di scenari ottimali e la definizione di indicatori misurabili per valutare

l'efficacia delle misure adottate.

Nel contesto del Piano Urbano della Mobilità Sostenibile, *l'IA* si configura come uno strumento strategico per definire obiettivi coerenti con l'Agenda 2030 delle Nazioni Unite (Obiettivo 11 – Città e comunità sostenibili), facilitando il monitoraggio dei risultati e l'adattamento continuo delle strategie in risposta a dinamiche urbane complesse. Le piattaforme digitali basate su IA permettono infatti di centralizzare l'acquisizione dei dati, integrare fonti eterogenee e fornire supporto decisionale in tempo reale alle autorità locali.

A livello infrastrutturale, l'architettura dei sistemi *IA-based* comprende tre livelli principali: sul campo, l'impiego di sensori, dispositivi *IoT,* telecamere e *Floating Car Data* consente di raccogliere informazioni dettagliate su flussi di traffico, comportamenti degli utenti e condizioni della rete; a livello centrale, le tecnologie *Big Data*, i modelli di simulazione dinamica e gli algoritmi predittivi permettono di rappresentare l'interazione tra domanda e offerta in modo realistico e tempestivo; infine, a livello distribuito, le piattaforme *MaaS* connesse con i sistemi centrali facilitano l'integrazione dei servizi e la personalizzazione dell'offerta per l'utente finale.

Questa struttura multilivello permette la creazione di Centrali di Controllo della Mobilità che, tramite l'impiego dell'*IA*, consentono una gestione proattiva e adattativa delle reti urbane, abilitando interventi tempestivi in caso di eventi critici e ottimizzando l'allocazione delle risorse. In tale quadro, le amministrazioni locali sono chiamate a svolgere un ruolo attivo non solo nell'adozione delle tecnologie, ma anche nella definizione di *standard*, regole di interoperabilità e meccanismi di verifica dell'impatto sociale ed ecologico.

La pianificazione supportata dall'IA deve essere, in ultima istanza, una pianificazione inclusiva, capace di garantire che l'innovazione tecnologica non aggravi le disuguaglianze spaziali, ma contribuisca a ridurle, rafforzando la capacità delle città di promuovere mobilità accessibile, sicura e sostenibile per tutti.

4 Aree di applicazione dell'IA nella mobilità: innovazioni, funzioni e implicazioni

L'intelligenza artificiale sta influenzando profondamente l'evoluzione della mobilità pubblica, attraverso un ampio spettro di applicazioni che spaziano dalla guida autonoma alla gestione intelligente del traffico, dalla manutenzione predittiva alla sostenibilità ambientale. Tali innovazioni

non solo ridefiniscono i modelli operativi del settore, ma sollevano questioni cruciali in termini di *governance*, regolazione e impatto sociale.

Tra le aree più significative si annoverano:

- **Veicoli autonomi**: Auto, camion e droni dotati di IA sono in grado di operare senza intervento umano, grazie all'integrazione di sensori, telecamere e algoritmi avanzati di navigazione, aumentando la sicurezza e riducendo i costi operativi nel lungo periodo.
- **Ottimizzazione del traffico**: I sistemi di *traffic management* basati su *IA* analizzano i flussi in tempo reale, regolano dinamicamente i semafori e prevedono congestioni, riducendo tempi di percorrenza, emissioni e consumo di carburante.
- **Navigazione intelligente**: L'*IA* abilita funzioni di assistenza alla guida, riconoscimento dei segnali stradali e adattamento alle condizioni ambientali, migliorando l'esperienza del conducente e il livello di sicurezza.
- **Logistica autonoma**: L'impiego di veicoli autonomi e droni per la consegna merci rende più efficiente l'ultimo miglio urbano, favorendo soluzioni sostenibili per la distribuzione in città.
- **Trasporto pubblico intelligente**: L'*IA* consente di ottimizzare orari e percorsi in base alla domanda, migliorare la gestione delle flotte, semplificare la bigliettazione tramite sistemi di riconoscimento automatizzato e rendere l'accesso ai servizi più fluido e inclusivo.
- **Sistemi *ITS e C-ITS***: Le infrastrutture connesse, integrate con *IA*, facilitano la comunicazione tra veicoli e reti stradali (*V2X*), migliorando il coordinamento tra gli attori della mobilità.
- **Sicurezza stradale**: Algoritmi predittivi e sistemi *ADAS* rilevano situazioni di rischio, supportano la prevenzione degli incidenti e contribuiscono a una progettazione più sicura degli spazi pubblici.
- **Sostenibilità ambientale**: L'ottimizzazione dei consumi energetici e l'integrazione con la mobilità elettrica rendono i sistemi intelligenti strumenti essenziali per la transizione ecologica dei trasporti urbani.

Tutte queste applicazioni, pur connesse alla dimensione tecnologica, producono effetti rilevanti sul piano economico e giuridico. Esse impongono una riflessione sulla regolazione delle piattaforme digitali, sulla trasparenza algoritmica, sulla responsabilità in caso di errore e sulla necessità di garantire un accesso equo e inclusivo alle innovazioni. In tale prospettiva, il ruolo delle autorità pubbliche si conferma centrale per orientare lo sviluppo tecnologico in funzione dell'interesse collettivo.

5 Rischi e vulnerabilità dell'Intelligenza Artificiale nei trasporti: sicurezza, trasparenza e responsabilità

L'adozione dell'intelligenza artificiale nel settore dei trasporti, pur offrendo significativi vantaggi in termini di efficienza, sostenibilità e personalizzazione dei servizi, comporta anche rischi strutturali che devono essere attentamente valutati e regolati. La natura pervasiva e autonoma dei sistemi IA solleva questioni cruciali sul piano della sicurezza informatica, della tutela dei dati personali, della giustizia algoritmica e della responsabilità pubblica.

a. **Sicurezza informatica e resilienza delle reti**: I sistemi di trasporto intelligenti, essendo fortemente interconnessi e digitalizzati, sono vulnerabili da attacchi informatici. La protezione delle infrastrutture critiche richiede soluzioni di *cybersecurity* avanzata, integrate con sistemi *IA* per la rilevazione in tempo reale di intrusioni, manomissioni o anomalie. La resilienza del sistema diventa una componente essenziale della sicurezza pubblica.

b. **Privacy, sorveglianza e uso dei dati personali**: L'IA si fonda sulla raccolta di grandi quantità di dati relativi agli spostamenti, alle preferenze e al comportamento degli utenti. È pertanto imprescindibile conformarsi al Regolamento generale sulla protezione dei dati (*GDPR*), applicando principi di minimizzazione, anonimizzazione e trasparenza. Gli utenti devono poter esercitare un controllo effettivo sui propri dati e comprendere come questi siano utilizzati nei processi decisionali automatizzati.

c. **Opacità decisionale e responsabilità algoritmica**: L'impiego di modelli di *machine learning* non interpretabili *("black box")* solleva interrogativi sul rispetto dei principi di legalità, trasparenza e motivazione amministrativa. In assenza di strumenti di *audit* algoritmico e supervisione pubblica, il rischio è quello di un'erosione della responsabilità delle autorità pubbliche. L'*AI Act* prevede obblighi stringenti per i sistemi ad alto rischio, inclusi quelli nel settore dei trasporti.

d. **Discriminazione e bias sistemici**: I *dataset* su cui si basano gli algoritmi possono riflettere o amplificare disuguaglianze esistenti, penalizzando utenti vulnerabili o territori meno connessi. Sistemi predittivi mal calibrati possono escludere implicitamente determinate categorie dalla pianificazione dei servizi. Occorrono quindi valutazioni di impatto algoritmico *ex ante*, integrate da misure di mitigazione *ex post*.

e. **Dipendenza tecnologica e fallimenti di *governance***: L'eccessiva dipendenza da fornitori privati di tecnologie *IA* può limitare la capacità delle autorità pubbliche di esercitare un controllo effettivo sulle scelte strategiche. Si configura così un rischio di *lock-in* contrattuale e tecnologico, che può compromettere la neutralità e la concorrenza nel mercato. Le amministrazioni devono rafforzare le proprie competenze interne, promuovere standard aperti e assicurare la propria autonomia nella valutazione delle soluzioni adottate.

Una governance dell'*IA* nei trasporti ispirata ai principi dello Stato di diritto richiede un approccio multilivello, capace di coniugare innovazione e tutela, efficienza e giustizia, automazione e controllo pubblico. Solo così sarà possibile garantire che l'intelligenza artificiale diventi uno strumento al servizio del bene comune e non una fonte di nuove diseguaglianze o vulnerabilità sistemiche.

6 Conclusioni: una mobilità intelligente pubblica, equa e costituzionalmente orientata

L'intelligenza artificiale rappresenta una leva strategica per la trasformazione del settore dei trasporti pubblici, con potenzialità significative in termini di efficienza operativa, sostenibilità ambientale e qualità dei servizi. Tuttavia, l'adozione di tecnologie intelligenti nella mobilità urbana non è un processo neutro: essa ridefinisce i confini tra pubblico e privato, introduce nuove modalità di esercizio del potere amministrativo e pone sfide inedite in termini di responsabilità, trasparenza e protezione dei diritti fondamentali.

Le autorità pubbliche si trovano oggi di fronte a un bivio: da un lato, possono limitarsi a svolgere un ruolo passivo, recependo soluzioni tecnologiche preconfezionate da attori privati; dall'altro, possono assumere una funzione proattiva e istituzionalmente centrale nella *governance* algoritmica, orientando lo sviluppo dell'innovazione verso obiettivi di equità, coesione territoriale e giustizia sociale.

Per intraprendere quest'ultima strada, è necessario rafforzare le competenze tecniche e giuridiche delle amministrazioni, sviluppare modelli di regolazione algoritmica ispirati all'interesse generale e dotarsi di strumenti di valutazione *ex ante* ed *ex post* dell'impatto delle tecnologie sull'effettivo godimento dei diritti di cittadinanza.

La piena attuazione del Regolamento europeo sull'intelligenza ar-

tificiale *(AI Act),* attraverso strumenti nazionali e prassi amministrative coerenti, rappresenta un passaggio essenziale per garantire una regolazione efficace e costituzionalmente orientata. In questo senso, un ruolo chiave può essere attribuito alle autorità di regolazione settoriali e agli organismi di vigilanza, come l'Autorità di Regolazione dei Trasporti (*ART*) e l'Agenzia per la *Cybersicurezza* Nazionale (*ACN*), anche con riferimento alla gestione sicura e centralizzata delle banche dati e alla definizione di *standard* condivisi.

L'intelligenza artificiale applicata ai trasporti deve essere regolata secondo una logica costituzionalmente orientata e adeguata della tecnica, in cui l'innovazione non sostituisce la decisione politica e amministrativa, ma ne diventa strumento operativo, trasparente e responsabile. Solo in questo modo sarà possibile coniugare la modernizzazione dei servizi pubblici con la tutela dei principi democratici, assicurando che la mobilità intelligente sia, prima di tutto, mobilità pubblica, equa e orientata al bene comune.

Cristiana Lauri

ARERA alla prova dell'IA. Tra sicurezza e sperimentazione

SOMMARIO. 1. Una premessa, anzi, una promessa: il miglioramento della qualità della vita – 2. IA e mercati energetici – 3. Le esigenze di sicurezza – 4. Le sperimentazioni tra ARERA e mercato – 5. Le tutele consumeristiche – 6. Prospettive regolatorie

1 Una premessa, anzi, una promessa: il miglioramento della qualità della vita

Il crescente impiego dell'intelligenza artificiale (d'ora in avanti IA) e delle relative applicazioni è destinato ad avere un impatto profondo sui mercati regolati e sui diritti che ARERA è volta a tutelare[104], con riferimento – al tempo stesso – alla garanzia dell'universalità, alla tutela della dignità umana e dei diritti fondamentali degli individui, alla tutela delle categorie fragili, alla sicurezza delle reti, alla stabilità degli approvvigionamenti e, non da ultimo, alle garanzie dei consumatori nella scelta delle migliori offerte disponibili sul mercato per soddisfare i propri bisogni[105].

Sono anche questi, del resto, i fronti su cui il legislatore è chiamato ora ad intervenire, in via trasversale, a seguito dell'approvazione al Senato del ddl sull'Intelligenza artificiale[106], nell'ambito del quale l'individuazione

[104] Con riferimento al settore energetico si veda il Report Agenzia Internazionale dell'Energia (AIE), *Energy and AI*, 2024, in www.iea.org, dove viene svolta una analisi completa dei dati avendo riguardo ai mercati dell'elettricità su scala globale e ai processi di consultazione con i decisori politici, gli attori del settore tecnologico e l'industria energetica.

[105] Evidenzia questi aspetti F. BASSAN, *Perché il via libera al ddl sull'AI è una buona notizia secondo Bassan*, in Formiche, 21 marzo 2025.

[106] Si tratta del ddl n. 1146/24, recante "*Disposizioni e delega al Governo in materia di intelligenza artificiale*", approvato dal Consiglio dei ministri il 23 aprile 2024 e dal Senato il 20 marzo

delle autorità competenti per la tutela dei diritti fondamentali rappresenterà un ulteriore passo decisivo per la definizione di un quadro di regole adeguato alle sfide poste dall'IA.

Quale Autorità avente competenze relative ai servizi dell'energia, del gas, del teleriscaldamento e teleraffrescamento, dell'acqua e dei rifiuti, ARERA dovrà sempre più adeguare la sua azione all'applicazione di strumenti fondati su diverse forme di IA, che investiranno un'ampia gamma di prodotti e servizi in parte già regolati o di prossima regolazione[107].

Come evidenziato dal Disegno di legge n. 1146 in materia di IA, la grande promessa di tale tecnologia è quella di promuovere il benessere della società[108] – o, in termini più ampi – la salute del pianeta, da intendersi nella sua accezione di "One Health" o "Planetary Health"[109], dunque in una prospettiva ampia, dove la promozione delle tecnologie digitali di IA abbraccia tutto ciò che attiene alla prevenzione, alla definizione di stili di vita più sani, alla cura delle persone più fragili – in ambito medico, educativo, per la tutela del territorio, con riferimento ai beni culturali e ambientali, alle comunità e a tutti i fattori connessi con la sostenibilità ambientale della transizione digitale basata sull'IA – tenendo quindi anche in considerazione, ad esempio, aspetti legati alla gestione dell'energia, specie da fonti rinnovabili, e alla mobilità sostenibile, unendoli trasversalmente a settori quali la tutela della *privacy*, della proprietà intellettuale e della sicurezza delle persone, anche in relazione agli aspetti che interessano strategicamente il settore della difesa

2025, il cui iter è stato caratterizzato dall'esigenza di coordinamento del testo con il Regolamento UE 2024/1689 del Parlamento Europeo e del Consiglio (c.d. "*AI Act*"), approvato il 13 giugno 2024, rispetto al quale la Commissione Europea – nel corso dell'istruttoria legislativa – aveva rilevato disallineamenti e contrasti, segnalati nel parere C (2024) 7814 (inviato all'Italia il 5 novembre 2024).

[107] Come emerge dalla Relazione annuale 2024 di ARERA.

[108] Nella prospettiva dell'affermazione di un principio antropocentrico, già posto a fondamento generale del regolamento europeo (cfr. art. 1 Reg. UE 2024/1689 e i relativi considerando nn. 1, 6, 8, 27, 176), in virtù del quale la tecnologia deve essere volta al servizio dell'essere umano e non viceversa.

[109] One Health è approccio integrato e unificante che mira a equilibrare e ottimizzare in modo sostenibile la salute delle persone, degli animali e degli ecosistemi, superare le barriere normative. A livello internazionale la strategia è supportata dal Quadripartito (WHO, WOAH, FAO, UNEP); cfr. il *One health joint plan of action (2022–2026).* A livello europeo, un impegno in tale direzione emerge anche dalle agenzie EFSA, AEA, ECDC, EMA, ECHA.

e la *cyber security* nazionale. Il Regolamento europeo[110] si presenta infatti come un testo generale, che rispecchia l'accentramento europeo sulla vigilanza – in capo alla Commissione UE – e che presuppone come effetto quello di una flessibilità nell'applicazione, lasciando un ampio spazio di discrezionalità agli Stati membri.

Il punto è stato ribadito dal Presidente di Arera, nell'evidenziare la dipendenza dalle risorse naturali dei settori di mercato in cui opera ARERA e la correlata tensione degli stessi verso il raggiungimento di livelli di dignitosa qualità della vita per tutti[111].

2 IA e mercati energetici

Nei settori regolati da ARERA, le sfide regolamentari connesse alla diffusione dell'IA, compresi il *software*, gli algoritmi e i dati utilizzati o generati da essa, si avviano verso profonde trasformazioni nei processi di produzione e consumo, ponendo l'esigenza di assicurare un quadro regolamentare al passo con l'evoluzione tecnologica e di garantire connesse e adeguate forme di tutela consumeristica. Il quadro regolatorio sull'IA costituisce in questo senso un passo ulteriore del percorso iniziato negli anni '90.

Nel settore energetico l'IA rappresenta un fondamentale fattore abilitante, in grado di accrescerne il valore. L'energia, specularmente, è elemento essenziale per supportare le tecnologie digitali.

Nonostante il quadro di regole in materia sia ancora in divenire e nonostante la persistenza dei divari tra regolatore (pubblico) e soggetti regolati (privati), la funzionalità dei sistemi elettrici s'interfaccerà sempre di più con l'IA in rapporto ai modelli di consumo, offrendo opportunità in termini di qualità dei servizi ma anche di margini di profitto per gli operatori.

Ciò appare confermato dalle tendenze che attualmente caratterizzano il settore energetico: il costante aumento registrato nell'elettrificazione, ove si prevede una ulteriore accelerazione della quota complessiva del consumo energetico finale; una crescente digitalizzazione e integrazione dei sistemi energetici attraverso la proliferazione di dispositivi e apparecchi collegati, veicoli elettrici, contatori intelligenti e sensori intelligenti in applicazioni industriali e commerciali; e, soprattutto, una certa complessità del sistema energetico nei modelli di approvvigionamento, domanda e flusso di energia.

[110] Regolamento UE 2024/1689 del Parlamento Europeo e del Consiglio (c.d. "*AI Act*").

[111] Cfr. *Relazione annuale*, cit.

Dal lato dell'offerta, infatti, la generazione di energia elettrica da fonti variabili, come l'eolico e il solare, sta aumentando rapidamente, mentre la generazione sta diventando più distribuita, grazie alla crescita di fonti di generazione più piccole e più disperse. Dal lato dei consumi, il numero di apparecchiature, veicoli e impianti industriali connessi risulta in aumento. Tali tendenze devono tuttavia combinarsi con la pressione sui costi, che negli ultimi anni ha richiesto significativi sforzi ai consumatori di energia su scala globale, con prezzi che hanno inciso pesantemente sul costo della vita.

Se nuovi operatori si stanno affacciando sul mercato, rendendo il settore energetico più competitivo e spingendo le aziende del settore a ricercare nuovi modi per aumentare l'efficienza, ridurre i costi e migliorare la sicurezza[112], ciò non potrà che determinare una maggiore attenzione alle questioni regolatorie sia sul fronte della domanda che su quello dell'offerta.

3 Le esigenze di sicurezza

Quello della sicurezza costituisce un tema assai ricorrente nei documenti di policy, nelle relazioni, e negli atti più recenti di ARERA.

L'AI Act stabilisce requisiti e obblighi specifici per i sistemi di intelligenza artificiale considerati ad alto rischio. Tra essi figurano, ad esempio, le applicazioni usate in ambiti come la sicurezza dei prodotti, il riconoscimento biometrico, le infrastrutture critiche e l'accesso ai servizi essenziali. Queste misure mirano a garantire che l'uso dell'IA sia sicuro, etico e rispettoso dei diritti fondamentali.

Il tema della sicurezza si riflette almeno su due assi fondamentali: l'uno è quello delle infrastrutture, l'altro riguarda le tutele consumeristiche.

Osservando il sistema nel suo complesso emerge un aumento dell'adozione delle nuove tecnologie (supercomputer e capacità di calcolo) da parte delle compagnie petrolifere e del gas per incrementare l'esplorazione e la produzione. L'IA determina inoltre un impatto importante nei sistemi elettrici in relazione ai profili di fornitura, trasmissione e domanda: produce un potenziale risparmio sui costi grazie alla riduzione nell'uso dei combustibili e consente una maggiore integrazione dell'elettricità rinnovabile nella rete. Anche nei settori di utilizzo finale le applicazioni dell'IA sono molteplici e hanno un potenziale significativo: nell'industria, l'IA viene utilizzata per ottimizzare i processi di produzione; nel comparto dei trasporti si presta a migliorare il funzionamento e la gestione dei veicoli, con una riduzione

[112] Cfr. Report Agenzia Internazionale dell'Energia (AIE), *Energy and AI*, 2024, p. 112.

dei consumi; nell'edilizia si registra un elevato potenziale in ragione dei vantaggi in termini di efficientamento, se pur ancora limitato da bassi tassi di digitalizzazione e costi dei materiali. L'IA mostra la sua utilità anche in attività ulteriori, come ad esempio le previsioni meteorologiche, migliorandone la precisione e riducendone la domanda di calcolo, in prospettiva di ottimizzare il funzionamento, la pianificazione e la resilienza dei sistemi energetici, per contribuire al raggiungimento degli obiettivi di contenimento del riscaldamento globale.

Molteplici sono tuttavia gli ostacoli che ad oggi ancora costituiscono un limite alla possibilità di implementare le applicazioni di IA: accanto ai necessari sviluppi regolatori, sarà necessario potenziare l'accesso ai dati, l'interoperabilità, le infrastrutture digitali, le competenze specialistiche e, più in generale la propensione culturale al cambiamento e la costruzione di un sistema di principi condivisi.

Questione aperta e in divenire è, non da ultimo, quella legata ai fabbisogni energetici dei data center, infrastrutture in crescita in relazione all'esplosione delle applicazioni di IA.

Il caso è ormai noto: DeepSeek, startup cinese nel settore dell'IA, si è imposta nel mercato grazie all'introduzione di *DeepSeek-R1*, un modello di linguaggio *open source*, gratuito e illimitato, in grado di eseguire compiti complessi di ragionamento a un costo significativamente inferiore rispetto ai concorrenti statunitensi, come OpenAI e Google, di fatto creando un terremoto nel mercato dei titoli tecnologici ed energetici e potenzialmente in grado di determinarne ulteriori su altri fronti, come ad esempio il nucleare. Il sistema *DeepSeek* sarebbe in grado di ridurre considerevolmente i consumi energetici a priori: il modello utilizza infatti solo una frazione della potenza di calcolo generalmente ritenuta necessaria per addestrare programmi simili, con conseguenze significative in termini di costi di sviluppo dell'intelligenza artificiale nonchè di impiego dell'energia necessaria ai *data center*.

È evidente come tali scenari contribuiscano a rafforzare ulteriormente alcune posizioni di forza nel mercato e nei rapporti tra poteri privati e poteri pubblici, riconfigurandoli. A tal riguardo sarà tuttavia utile comprendere quali saranno le scelte delle imprese, che potrebbero optare per un utilizzo dell'efficienza computazionale per la creazione di modelli sempre più efficienti o, al contrario, operare scelte imprenditoriali e di mercato che di fatto menterrano inalterati i consumi energetici[113].

[113] Così A. Lensen (cfr. O. Ajay, *DeepSeek's R1 Disrupts AI Energy Consumption*, in *The electricity hub*, 31 gennaio 2025).

4 Le sperimentazioni tra ARERA e mercato

In tema di sicurezza, avendo riguardo all'architettura che pare delinearsi dalle scelte relative alla governance dell'IA su scala europea e nazionale, è verosimile prevedere che una competenza forte sarà accentrata in capo ad ACN stante la preposizione di questa Autorità ai compiti di regolazione e vigilanza rispetto a tutti i temi rilevanti ai fini della sicurezza nazionale, in maniera trasversale e analoga per i diversi settori[114].

È dunque da chiedersi, semmai, cosa resti nelle corde di ARERA.

Alcune risposte possono provenire dalla lettura dei casi applicativi.

Un primo esempio è rappresentato dalla delibera 404/2022/R/gas "Progetti pilota di ottimizzazione della gestione e utilizzi delle infrastrutture del settore del gas naturale", in relazione alle prospettive di transizione energetica e decarbonizzazione. Ai sensi di tale documento le società Unareti, LD Reti e RetiPiù hanno ottenuto da ARERA un contributo complessivo di 4,3 milioni di euro per quattro progetti sperimentali. Si prevede, in particolare, l'implementazione di un nuovo sistema di gestione basato sull'intelligenza artificiale destinato a ridurre le emissioni di metano dalla rete e a realizzare nuovi generatori per recuperare l'energia normalmente dissipata nel passaggio dalla rete di trasporto a quella di distribuzione; alla sperimentazione di un sistema per massimizzare la produzione di un impianto di biometano immettendone l'eccesso in rete; e alla riduzione dell'impatto delle emissioni di metano provenienti dalla rete di distribuzione attraverso strumenti di monitoraggio innovativi che ne consentono la loro individuazione preventiva.

Un secondo esempio è dato dall'accoglimento, da parte di ARERA, di alcune richieste di Italgas per l'accesso al meccanismo di incentivazione su alcuni progetti pilota di ottimizzazione delle infrastrutture per il gas, con un contributo complessivo di oltre 3,21 milioni di euro. Tra essi figura il progetto "3D Asset Mapping" volto all'innovazione e alla digitalizzazione delle infrastrutture di distribuzione del gas in Italia, attraverso l'adozione di tecnologie avanzate come il "Mobile Mapping LiDAR" e il "Georadar GPR", che mirano a migliorare l'efficienza, la sicurezza e la qualità del servizio, offrendo benefici alle amministrazioni locali e ai cittadini. Il sistema consentirà di individuare inefficienze, prevedere guasti e pianificare manutenzioni preventive attraverso la tecnologia del *Digital Twin* che permette una rilevazione digitale delle infrastrutture presenti sopra e sotto il manto

[114] G. Tropea, *La cibersicurezza come nuova funzione dell'amministrazione*, in Apertacontrada, 28 gennaio 2025.

stradale con raccolta dati in tempo reale.

Emerge, dunque, pur in via sperimentale, uno sforzo regolatorio e finanziario teso ad offrire supporto alla non facile composizione delle esigenze di tutela ambientale e digitalizzazione dei mercati, nella direzione della *Green AI*[115] e rispetto al quale sarà interessante monitorare gli esiti e i risultati nel breve, medio e lungo periodo.

5 Le tutele consumeristiche

Diverso è invece il discorso con riferimento ai profili consumeristici, ove all'ARERA spettano le competenze ad essa attribuite dalla normativa di settore.

Se, infatti, attraverso i sistemi di calcolo avanzato e all'automazione si è giunti ad una gestione diffusa dell'energia, parallelamente si è ulteriormente potenziata la posizione dei poteri privati nei mercati energetici, caratterizzati da forte asimmetria informativa sbilanciata sugli operatori economici rispetto alle strutture di regolazione e all'utenza finale. È qui che la rapidità dell'impiego dell'IA potrebbe esacerbare i disallineamenti già esistenti ed è dunque nell'ambito della costruzione di un sistema strategico di tutele che una serie di interventi possono contribuire a definire punti di equilibrio.

a. Scelte nel mercato libero

L'uso di modelli di intelligenza artificiale impatta fortemente i mercati energetici e le negoziazioni che vi si svolgono, consentendo di elaborare stime in modo veloce e accurato rispetto a diverse variabili. Per stimare gli andamenti in termini di prezzi e volumi di domanda e di offerta, i modelli vengono addestrati in base ai dati storici e agli altri parametri rilevanti e sono anche in grado di tracciare il comportamento da parte della concorrenza.

Il sistema si va evolvendo parallelamente alla crescente disponibilità dei dati. In tale contesto diviene fondamentale, quale fattore coadiuvante, il sistema di accompagnamento dei consumatori verso le scelte nel mercato. A questo scopo risponde il Portale Consumi di ARERA, che consente di verificare i consumi e idealmente metterli a disposizione al fine di costruire dei profili

[115] V. Bolón-Canedo *et al.*, *A review of green artificial intelligence: Towards a more sustainable future*, in Neurocomputing, (599) 2024.

utili all'elaborazione di offerte mirate[116].

b. Monitoraggio dei servizi

L'IA consente di condurre una costante analisi sulle condizioni delle reti elettriche anche attraverso lo svolgimento di simulazioni per comprendere la necessità di interventi volti a mantenere la stabilità del sistema. Tale aspetto è fondamentale anche per orientare le scelte sul mercato dei servizi ancillari, cioè dei servizi di rete necessari per mantenere il sistema in equilibrio, che prevedibilmente acquisiranno sempre maggior rilevanza.

La riconversione dei contatori in *smart metering* ha costituito, ad esempio, un presupposto infrastrutturale essenziale per lo sviluppo di ulteriori tecnologie.

Più di recente, la normativa sugli edifici[117] ha mirato a potenziare interventi di isolamento termico, utilizzi di tecnologie di riscaldamento e raffreddamento più efficienti e l'installazione di illuminazione led volti a ridurre significativamente i consumi. Si affacciano poi sul mercato piattaforme che utilizzano l'IA, in esecuzione di quanto previsto dal piano Transizione 5.0, supportate da incentivi dedicati a interventi per l'efficienza energetica trainati da soluzioni digitali[118]. Un esempio è dato dalle piattaforme che ottimizzano il funzionamento degli impianti di climatizzazione, migliorando l'efficienza energetica, integrando contemporaneamente i dati ambientali, energetici, meteorologici e di prezzo dell'energia per regolare dinamicamente gli impianti in tempo reale[119].

[116] Disponibile alla pagina <https://www.consumienergia.it/portaleConsumi/>.

[117] Cfr. Direttiva 2024/1275 dell'8 maggio 2024 sulla prestazione energetica nell'edilizia.

[118] Il Piano Transizione 5.0, nell'ambito della più ampia strategia finalizzata a sostenere il processo di trasformazione digitale ed energetica delle imprese, ha messo a disposizione, nel biennio 2024-2025, 12,7 miliardi di euro. In linea con le azioni di breve e medio periodo previste dal piano *REPowerEU*, il Piano si pone l'obiettivo di favorire la trasformazione dei processi produttivi delle imprese, rispondendo alle sfide poste dalle transizioni gemelle, digitale ed energetica, <https://www.mimit.gov.it/it/incentivi/piano-transizione-5-0>.

[119] Si veda ad esempio la piattaforma "Simon" avviata, negli ospedali del gruppo Humanitas, che ha condotto ad una riduzione dei consumi energetici del 20%, migliorando il comfort interno del 50%.

c. Sportello consumatori

Lo Sportello consumatori continua a rappresentare una risorsa preziosa a supporto dei consumatori, tanto quelli "tradizionali", quanto i "prosumer", che producono e consumano energia rinnovabile all'interno delle configurazioni di autoconsumo diffuso. Il servizio di assistenza si estende inoltre agli utenti degli altri settori regolati da ARERA: il servizio idrico integrato, il teleriscaldamento e il teleraffrescamento e il settore dei rifiuti.

Nella relazione annuale 2024 di ARERA si evidenzia l'ulteriore incremento delle chiamate pervenute al call center dello Sportello consumatori, che si attestano, per tutti i settori, a oltre 1,5 milioni, con un aumento del 23% rispetto al 2022.

Sebbene sin dalla sua introduzione lo strumento si sia rivelato efficace e di qualità, la sempre crescente domanda di informazione e assistenza da parte dei consumatori, oltre a stimolare un continuo check-up della regolazione, richiede anche di valutare ulteriori modalità di efficientamento dei servizi, già oggi accessibili a tutte le fasce di popolazione anche attraverso i più recenti sviluppi tecnologici.

L'utilizzo dell'IA nelle modalità di accesso faciliterà e velocizzerà ulteriormente l'ottenimento delle informazioni e il contatto con un addetto specializzato dello Sportello, di recente migliorato anche attraverso una nuova veste grafica e un'interfaccia semplificata. Accedendo all'area personale gli utenti possono usufruire di diversi servizi digitali, tra cui il "Contact Center", volto a fornire informazioni sul mercato e sui diritti dei consumatori; la "Conciliazione", per risolvere controversie con i fornitori in via stragiudiziale; "Segnalazioni", per comunicare disservizi o criticità; "SMART," teso a risolvere problematiche relative al bonus sociale, alla doppia fatturazione e ai contratti contestati; "Reclami", dedicato alle segnalazioni nel settore idrico e dei rifiuti; "Help Desk", dedicato alle Associazioni dei consumatori.

Tale nuovo assetto ha reso lo Sportello del Consumatore ARERA ancor più intellegibile e trasparente, rendendolo strumento di attuazione dei percorsi di digitalizzazione e semplificazione nel settore dei consumi di energia.

d. Nucleo dell'Arma dei Carabinieri presso ARERA

Un ulteriore aspetto oggetto di regolazione è dato dalla delibera 164/2024/A, con cui ARERA ha istituito un Nucleo dell'Arma dei

Carabinieri, dipendente dal Comando Carabinieri Tutela Ambientale e Sicurezza Energetica, nella sede ARERA di Milano.
L'Arma metterà a disposizione personale altamente qualificato appartenente al Comando Carabinieri per la Tutela Ambientale e la Sicurezza Energetica, con l'obiettivo di ampliare le attività di vigilanza dell'Autorità alla luce, in particolare, delle funzioni di regolazione e controllo attribuite nei settori ambientali (ciclo dei rifiuti urbani, servizi idrici, teleriscaldamento e teleraffrescamento). Il supporto riguarderà anche attività di enforcement e di specifiche attività progettuali, mettendo a disposizione strumenti tecnologici avanzati e competenze altamente specializzate per l'effettuazione di accertamenti tramite verifiche ispettive in loco e controlli sui dati dichiarati all'Autorità medesima, contribuendo a rafforzare i necessari profili di trasparenza, certezza e affidabilità.

6 Prospettive regolatorie

Il Regolamento sull'IA mette in luce risultati vantaggiosi da conseguire sul piano sociale ed ambientale, tra cui figurano, ad esempio, gestione delle infrastrutture, energia, servizi pubblici, efficienza dal punto di vista energetico e delle risorse, mitigazione dei cambiamenti climatici e adattamento ad essi[120].

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

Nel frattempo, l'Organizzazione internazionale per la normazione (International Organization for Standardization, ISO), rete globale che sviluppa standard per produttori, regolatori e altri enti, ha affermato che entro pochi mesi saranno pubblicati criteri per un'intelligenza artificiale "sostenibile" (ISO/IEC DTR 20226 – *Information technology – Artificial intelligence – Environmental sustainability aspects of AI systems*). Questi includeranno standard per misurare l'efficienza energetica, l'uso delle materie prime, il trasporto e il consumo di acqua, nonché pratiche per ridurre gli impatti dell'IA

[120] Così il Considerando n. 3.

durante tutto il suo ciclo di vita, dal processo di estrazione dei materiali e di produzione dei componenti del computer, all'elettricità consumata per i suoi calcoli. Lo scopo è quello di consentire agli utilizzatori dell'IA di prendere decisioni informate sul loro uso dell'intelligenza artificiale.

Nonostante gli esempi visti sopra, nel Disegno di legge n. 1146 approvato al Senato non pare profilarsi un ruolo per ARERA.

Ciò non esclude, tuttavia, che ARERA, seppur non direttamente coinvolta nell'applicazione dell'AI Act, si troverà ad intervenire, mediante auto e co-regolamentazione, rispetto ai servizi resi nell'ambito dei suoi settori generati o potenziati da intelligenza artificiale, a vantaggio dei consumatori-utenti.

Il suo ruolo nel monitorare i mercati di riferimento sarà fondamentale in quanto i sistemi di IA funzionano (e migliorano) grazie all'inserimento di dati di addestramento e con adeguate risorse dedicate di tipo hardware e software, che oggi possono essere reperite mediante l'acquisto di servizi di *cloud computing*. Dovrà inoltre coniugare la sua azione con le regole relative alla trasparenza algoritmica, all'accesso e all'utilizzo dei dati digitali, data l'immensa mole di dati generata dai consumatori nei settori da essa regolati.

La mappatura degli impatti dell'IA nei settori regolati da ARERA richiede un contesto multiattoriale, che vive una profonda fase di evoluzione sia dal lato dell'offerta che da quello della domanda, e che ha il compito di operare nell'ambito di principi generali a garanzia dell'intero sistema in via di costruzione normativa.

In primo luogo, nonostante le prime applicazioni nel settore, i dati ad oggi disponibili rivelano la necessità di ulteriori sforzi da parte del settore energetico per cogliere al meglio le potenzialità dell'IA. Ciò richiederà una forte collaborazione tra poteri pubblici e poteri privati in questioni chiave su cui, tra tutte, emerge lo sviluppo di competenze digitali[121]. Ciò che si registra, infatti, è una arretratezza del mercato del lavoro nel settore energetico, che sembra ancora faticare a riconoscere il valore prioritario dell'IA e delle competenze digitali, ancora scarse, soprattutto se sommate anche alla carenza di competenze tecniche specifiche relative alla progettazione, all'ingegneria e alla gestione dei progetti [122].

[121] Cfr. IEA, *Enegy and AI*, cit., 230 ss.; IEA, *World Energy Employment*, 2024, 40 ss..

[122] Cfr. IEA, *World Energy Employment*, cit. Si evidenzia, in particolare, che tra il 2018 e il 2024, la concentrazione di competenze specializzate nell'IA nei servizi pubblici e nel settore petrolifero, del gas e minerario è stata in media inferiore del 40% rispetto ai settori dell'istruzione, dei servizi finanziari, dei servizi professionali e nelle aree tecnologia, in-

In secondo luogo, è necessario potenziare il coinvolgimento degli stakeholders, in grado di influire sulle serie di dati con cui vengono addestrati i sistemi di IA; sull'hardware necessario per far funzionare i sistemi di IA; nonché di orientare la comprensione del modo in cui i prodotti e i servizi che integrano l'IA possono essere positivamente utilizzati dagli operatori economici e dai consumatori[123].

In terzo luogo, emerge la rilevanza del coordinamento di ARERA con le altre Authority[124], che rappresenta una delle frontiere regolatorie allo stato non considerate come prevalente, ma da cui si ritiene di non poter prescindere nella prospettiva di realizzare quell'integrazione dei sistemi che le tecnologie dell'IA consentono e che, a regole invariate, rischierebbero di restare materiale quiescente, con una conseguente evidente perdita di opportunità per i mercati e i consumatori, nonché per le sfide politico-legislative che compongono le Agende più recenti sul piano nazionale e internazionale.

formazione e media.

[123] S. Chen, *AI's energy problem*, in Nature, 6 marzo 2025, 22 ss.

[124] In particolare, per una migliore definizione dei ruoli delle autorità a tutela dei diritti fondamentali legati alle applicazioni dell'IA, appare difficile rinunciare ad un coordinamento delle Autorità e in particolare tra Agcom e Garante della privacy, nonché di queste con ACN.

AUTORITÀ NAZIONALE ANTICORRUZIONE

Serafina Piantedosi[125]

L'intelligenza artificiale nel settore dei contratti pubblici

L'intelligenza artificiale può rivoluzionare il modo in cui operano gli appalti pubblici, migliorando l'efficienza, la trasparenza e l'efficacia in termini di costi, con conseguenti vantaggi per tutti i cittadini. Il settore dei contratti pubblici è stato interessato di recente da una vera e propria rivoluzione digitale, in cui una grande mole di dati concernenti le procedure ad evidenza pubblica diventa utilizzabile per addestrare algoritmi c.d. "machine learning". A fronte di tali innovazioni, l'impostazione umano-centrica europea valorizza il ruolo della persona-funzionario pubblico, che deve sempre garantire un controllo sulle scelte automatizzate, specie per quanto concerne l'attività discrezionale della pubblica amministrazione.

1 L'intelligenza artificiale nel Codice dei contratti pubblici

Il settore dei contratti pubblici è stato interessato di recente da una vera e propria rivoluzione digitale.

Il fondamento giuridico della digitalizzazione degli appalti pubblici lo troviamo nel PNRR, che prevede una specifica riforma, la 1.10. concernente la "*Riforma del quadro legislativo in materia di appalti pubblici e concessioni*", suddivisa fra le misure M1C1-70, finalizzata a "*definire le modalità per digitalizzare le procedure per tutti gli appalti pubblici e concessioni e definire i requisiti di interoperabilità e interconnettività*" ed M1C1-75 volta a realizzare il pieno

[125] 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.

funzionamento del Sistema Nazionale di *e-Procurement*. Quest'ultima misura, in particolare, stabilisce che il Sistema Nazionale di *e-Procurement* deve essere operativo e del tutto in linea con le pertinenti direttive UE e deve comprendere la digitalizzazione completa delle procedure di acquisto fino all'esecuzione del contratto (*Smart Procurement*), deve essere interoperabile con i sistemi gestionali delle pubbliche amministrazioni e prevedere l'abilitazione digitale degli operatori economici, sessioni d'asta digitali, *machine learning* per l'osservazione e l'analisi delle tendenze, CRM evoluto con funzioni di *chatbot*, *digital engagement* e *status chain*.

Il nuovo Codice dei Contratti pubblici (d.lgs. n. 36/2023) ha dato attuazione a tali misure nel Libro I, Parte II dedicata alla "Digitalizzazione del ciclo di vita dei contratti" (Artt. 19 a 36) e a partire dal 1° gennaio 2024 le disposizioni ivi contenute hanno acquistato efficacia. Si tratta di norme che mirano ad attuare una completa digitalizzazione di ogni fase della procedura di gara pubblica, dalla programmazione all'esecuzione e prevedono l'utilizzo in via esclusiva di piattaforme e servizi tecnologici interoperabili volti a garantire l'attuazione del principio dell'*once only*.

Il fulcro della transizione digitale è rappresentato dalla Banca Dati Nazionale dei Contratti Pubblici (BDNCP) istituita presso l'ANAC, che riunisce tutti i dati dei contratti pubblici di qualsiasi importo e tipologia per garantire trasparenza e tracciabilità delle procedure di gara e delle fasi antecedenti e successive alla stessa.

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

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

Oltre alla disciplina in materia di digitalizzazione, nel d.lgs. n. 36/2023 è contenuta per la prima volta una norma che regola l'impiego da parte della pubblica amministrazione di soluzioni tecnologiche avanzate, tra cui sistemi di intelligenza artificiale (IA) e *blockchain*.

L'art. 30 del d.lgs. n. 36/2023, infatti, prevede che, per realizzare più elevati standard di efficienza, le stazioni appaltanti e gli enti concedenti provvedano, ove possibile, ad automatizzare le proprie attività ricorrendo

a soluzioni tecnologiche, tra cui l'intelligenza artificiale e le tecnologie di registri distribuiti (c.d. *blockchain*), nel rispetto delle specifiche disposizioni in materia.

Al comma 2 e al comma 3, poi, la norma chiarisce i limiti e i confini dell'impiego di tale tecnologia, stabilendo i tre principi cui devono conformarsi le decisioni assunte mediante automazione, individuandoli nella conoscibilità e comprensibilità, nella non esclusività della decisione algoritmica e nella non discriminazione algoritmica.

L'art. 30, dunque, va oltre la digitalizzazione e riguarda non soltanto l'utilizzo da parte delle stazioni appaltanti di procedimenti algoritmici per l'aggiudicazione delle gare, c.d. "algoritmi deterministici", ma anche gli algoritmi c.d. "*machine learning*" (ML). Lo sviluppo di tali ultimi algoritmi sarà il risultato della digitalizzazione, dal momento che per effetto dell'implementazione della BDNCP saranno disponibili enormi quantità di dati (c.d. *Big Data*) relativi alle gare pubbliche e alle imprese che vi partecipano e tali dati costituiranno un prezioso patrimonio a cui le amministrazioni potranno attingere per addestrare l'intelligenza artificiale così da produrre predizioni, secondo una logica di tipo statistico-probabilistico.

A tal fine, fondamentale sarà l'integrazione tra la stessa Banca dati e la Piattaforma Unica della Trasparenza istituita presso l'ANAC, nella quale confluiranno tutti i dati oggetto di pubblicazione obbligatoria ai sensi del d.lgs. 33/2013 (decreto trasparenza), in un unico luogo virtuale, accessibile a chiunque. Ciò renderà disponibile una grande quantità puntuale di informazioni, in maniera semplificata, ma facilmente fruibile e confrontabile. Tali dati, specie quelli relativi al settore dei contratti pubblici, potranno essere utilizzati dalle P.A., anche per il tramite dell'IA, al fine di identificare eventuali anomalie o indici di pratiche corruttive o anche per predire i rischi di inadempimento di una data impresa che partecipa alla gara pubblica o, ancora, per individuare situazioni di possibile conflitto di interesse.

2 Le procedure automatizzate nell'e-Procurement e la C.D. "Riserva di umanità della scelta"

L'intelligenza artificiale, quindi, ha il potere di rivoluzionare il modo in cui operano gli appalti pubblici, migliorando l'efficienza, la trasparenza e l'efficacia in termini di costi con conseguenti vantaggi per tutti i cittadini.

L'analisi di una grande mole di dati, effettuata per il tramite dell'intelligenza artificiale, potrebbe portare ad individuare e selezionare le migliori strategie di approvvigionamento, identificando opportunità di

risparmio e mitigando i rischi.

Inoltre, l'automatizzazione delle attività di *routine* consentirebbe ai professionisti del *public procurement* di concentrarsi sulle sole decisioni strategiche da assumere durante l'iter dell'appalto pubblico.

Le potenzialità dell'IA nel settore dei contratti pubblici, però, devono essere calate in concreto nel processo di appalto. La domanda che sorge spontanea, infatti, è: "Quali tecnologie di intelligenza artificiale sono disponibili ad oggi e in quali fasi dell'appalto pubblico potrebbero essere utilizzate?".

Nell'iter dell'appalto pubblico potrebbero essere diversi i momenti in cui far uso dell'intelligenza artificiale; in particolare, l'impiego di tale tecnologia potrebbe riguardare la fase preparatoria della gara pubblica oppure la fase decisoria, preordinata quindi all'aggiudicazione.

Per quanto concerne la fase preparatoria della gara, si potrebbe immaginare l'utilizzo dell'AI per la redazione degli atti di gara. La redazione dei bandi di gara o dei capitolati tecnici, ad esempio, potrebbe essere agevolata dall'IA tramite la creazione di modelli "standard" derivanti dall'individuazione delle migliori prassi fra gli atti di gara più virtuosi delle diverse amministrazioni pubbliche.

Gli algoritmi predittivi, poi, potrebbero essere impiegati per prevedere i costi complessivi di un'opera, tenendo conto dei dati storici presenti nelle diverse banche dati sulla base del tipo di opera da eseguire o delle fluttuazioni di costo delle materie prime.

Inoltre, durante la fase di gara l'IA potrebbe facilitare i rapporti tra la stazione appaltante e le imprese, attraverso l'uso di *chatbot* e assistenti virtuali per gestire le richieste di chiarimenti delle imprese.

Nel nuovo Codice dei contratti pubblici, ancora, già si ammette l'impiego della *blockchain* per la verifica delle fideiussioni presentate dagli operatori economici per la partecipazione alla gara pubblica. Ai sensi dell'art. 106, comma 3 d.lgs. n. 36/2023, infatti, la garanzia fideiussoria deve essere emessa e firmata digitalmente e deve essere altresì verificabile telematicamente presso l'emittente ovvero gestita mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti (*Distributed Ledger Technology*) tra cui figura anche la *blockchain* a garanzia della certezza del processo.

Si tratta di tecnologie disponibili sul mercato che offrono garanzie di certificazione e immutabilità dei dati inseriti, per cui l'impresa chiedendo l'emissione della fideiussione direttamente sulla DLT può fornire alla stazione appaltante una "certificazione di origine" della stessa e rendere certo un elemento che altrimenti non sarebbe presente in banche dati della P.A.

L'IA potrebbe anche essere utilizzata nella fase di aggiudicazione, per coadiuvare la Commissione di gara nella scelta della migliore offerta.

In siffatte ipotesi, però, sono molteplici i rischi che l'impiego dell'IA potrebbe comportare e per tale ragione il terzo comma dell'art. 30 Cod. contratti pubblici prescrive precise regole per l'impiego decisorio dell'IA.

Nello specifico, l'amministrazione deve assicurare il rispetto: a) dei principi di conoscibilità e comprensibilità del sistema, per cui ciascun o.e. deve essere in grado di conoscere l'esistenza dei processi automatizzati che lo riguardano e di ricevere informazioni sulla logica di funzionamento dell'algoritmo; b) del principio di non esclusività della decisione algoritmica, per cui vi deve essere sempre nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; c) del principio di non discriminazione algoritmica,

Di primaria importanza è il disposto di cui alla lettera b) che codifica il principio della c.d. "riserva di umanità della scelta" secondo cui sarebbe impensabile affidare interamente alla "macchina" l'assunzione di provvedimenti amministrativi, per cui deve esserci sempre un controllo umano sulla decisione finale. Tale regola costituisce la trascrizione dei risultati cui era pervenuta la giurisprudenza amministrativa sull'impiego dell'algoritmo nel procedimento amministrativo. Emblematica al riguardo è la pronuncia del Consiglio di Stato n. 881/2020 in cui era stato stabilito che nel caso in cui una decisione automatizzata "*produca effetti giuridici che riguardano o che incidano significativamente su una persona*", questa ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato ma deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informativo il modello viene definito come HITL (*human in the loop*), secondo cui, per produrre il suo risultato è necessario che la macchina interagisca con l'essere umano.

Il terzo comma dell'art. 30 Cod. contratti pubblici, dunque, non sembrerebbe consentire un impiego esclusivo dell'IA nell'ambito dell'attività discrezionale della P.A., dal momento che le procedure automatizzate, sulla base del principio della c.d. "riserva di umanità della scelta", devono comunque lasciare uno spazio di intervento per l'intelligenza umana, in funzione integrativa o eventualmente correttiva.

Il principio della riserva di umanità della scelta è stato poi riportato anche nel disegno di legge n. 1146 attualmente in trattazione in Parlamento ("Disposizioni e delega al Governo in materia di intelligenza artificiale"). L'art. 13 di tale disegno di legge rubricato "Uso dell'intelligenza artificiale

nella pubblica amministrazione", infatti, dopo aver ammesso l'utilizzo delle tecnologie di IA da parte delle amministrazioni pubbliche, prevede alcune cautele nel suo impiego. In particolare, stabilisce che l'utilizzo dell'intelligenza artificiale deve avvenire in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale. Inoltre, le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo dell'intelligenza artificiale responsabile e a sviluppare le capacità trasversali degli utilizzatori.

Nella sua formulazione, quindi, l'art. 30 Cod. contratti sembra già richiamare tutte le opportunità e tutti i rischi insiti nell'utilizzo dell'intelligenza artificiale nel processo decisionale pubblico.

3 Gli appalti pubblici di Intelligenza Artificiale

Il tema dell'IA nel settore dei contratti pubblici riguarda anche l'acquisto di beni e servizi informatici aventi ad oggetto sistemi di intelligenza artificiale. Le P.A., infatti, certamente dovranno approvvigionarsi di *software* di intelligenza artificiale, così come è avvenuto per l'acquisto dei beni e servizi basati sulla tecnologia *cloud*.

La disciplina di tali acquisti è contenuta nel 2° comma dell'art. 30, il quale ne detta i limiti. Nello specifico, la norma stabilisce che nell'acquisto o sviluppo delle soluzioni di IA le stazioni appaltanti e gli enti concedenti devono introdurre negli atti di indizione delle gare clausole volte ad assicurare che i fornitori forniscano anche dopo la stipula del contratto le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori e degli effetti indesiderati derivanti dall'automazione.

È possibile ipotizzare, poi, che gli appalti pubblici di intelligenza artificiale presenteranno le stesse criticità che si sono rilevate nell'acquisto dei servizi *cloud*, specie per ciò che concerne la sicurezza dei dati.

Infatti, in materia di acquisti di servizi *cloud* da parte dell'amministrazione pubblica era stata rilevata la necessità che i dati raccolti fossero conservati in *datacenter* localizzati in Europa, così da poter garantire il rispetto delle norme europee in materia di protezione dei dati. Il rischio, infatti, riguardava il possibile trasferimento dei dati in un altro continente a seguito dell'utilizzo dei servizi *cloud* delle c.d. piattaforme "*over the top*" e di tutte le società ad esse collegate, con eventuale pregiudizio alla sicurezza del Paese.

Tali preoccupazioni sembrano animare la stessa disposizione di cui all'art. 5 del succitato Disegno di legge n. 1146 rubricata "Princìpi in materia di sviluppo economico" la quale al comma 1, lettera d) stabilisce che lo Stato e le altre autorità pubbliche indirizzano le piattaforme di *e-procurement* delle amministrazioni pubbliche in modo che, nella scelta dei fornitori di sistemi e di modelli di intelligenza artificiale, siano privilegiate quelle soluzioni che garantiscono la localizzazione e l'elaborazione dei dati critici presso *data center* posti sul territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini di trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'intelligenza artificiale generativa, nel rispetto della normativa sulla concorrenza e dei princìpi di non discriminazione e proporzionalità.

4 Conclusioni

Da quanto esposto, emerge che sono innumerevoli le potenziali applicazioni dell'IA nel settore dei contratti pubblici.

In materia di appalti, L'IA se correttamente applicata contribuirebbe certamente a semplificare e rendere più celere la procedura di gara, nonché a garantire trasparenza e controllabilità dell'ecosistema degli appalti.

Tuttavia, non tutti i progressi tecnologici sono rilevanti o vantaggiosi per la procedura di appalto. Pertanto, è essenziale sviluppare un occhio critico e imparare a valutare l'utilità e la fattibilità delle diverse applicazioni di intelligenza artificiale.

L'utilizzo dell'intelligenza artificiale, infatti, deve essere strumentale all'attività provvedimentale della p.a. e non sostitutiva delle scelte umane. Sarebbe infatti impensabile sostituire totalmente l'intelligenza umana nel processo decisionale pubblico, per cui non bisogna dimenticare la centralità della persona-funzionario pubblico a cui dovrà sempre essere garantito un controllo sulle scelte automatizzate, specie per quanto concerne l'attività discrezionale della pubblica amministrazione.

Banca D'Italia

Federico M. Gabbricci

La vigilanza sull'intelligenza artificiale in ambito bancario

Il presente lavoro si propone di esaminare le interrelazioni fra la normativa bancaria e quella in materia di intelligenza artificiale focalizzandosi sulle problematiche poste dal D.d.L. 1146/2023 e sule possibili modalità di coordinamento fra le discipline.

1 Premessa

La recente "*indagine fintech nel sistema finanziario italiano*"[126] della Banca d'Italia ha rilevato come il ricorso a tecnologie basate sull'intelligenza artificiale (IA) sia sempre più massivo in ambito bancario. Molteplici sono infatti gli utilizzi nel settore in esame, *ex multis*: l'automazione dei processi, la prevenzione delle frodi, il miglioramento della "customer experience" (mediante chatbot e assistenti virtuali) nonché l'attività di valutazione della concessione mediante credit scoring algoritmico.

L'utilizzo di tali sistemi non è scevro da rischi (ad esempio il compimento di scelte discriminatorie, la scarsa trasparenza del processo decisionale) che si sommano a quelli tradizionali dell'attività bancaria e impongono la necessità di un ripensamento dei principi di sana e prudente gestione della vigilanza.

Il quadro così delineato ha subito una fondamentale innovazione ad opera del legislatore europeo con il Regolamento (UE) 2024/1689 in materia di Intelligenza Artificiale (c.d. Regolamento IA) che ha fornito re-

[126] Banca d'Italia, *Indagine fintech nel sistema finanziario italiano*, 2024 <https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2023/2023-indagine-fintech.pdf>.

gole di utilizzo di tali tecnologie e incaricato il legislatore nazionale di individuare una o più autorità per vigilare sulla materia.

L'attività di vigilanza sulla tecnologia si interseca con l'attività di vigilanza sui soggetti e ciò comporta la necessità di trovare modalità di coordinamento fra le differenti normative.

È pertanto opportuno esaminare il framework normativo in divenire per trarne delle prime considerazioni.

2 L'IA Act e il disegno di legge 1146/2024

Sviluppo di tecnologie che rispettino i diritti fondamentali, la democrazia e i principi dello Stato di diritto e promozione dell'innovazione in materia; sono questi gli obiettivi del Regolamento sull'Intelligenza Artificiale approvato nel giugno 2024.

Punti chiave del regolamento sono l'adozione di un approccio *risk based* che differenzia i sistemi IA[127] su quattro livelli di rischio (inaccettabile, alto, limitato alla trasparenza e minimo); la predisposizione di obblighi *ex ante* ed *ex post* per fornitori[128] e *deployers*[129]; la istituzione di un'autorità europea e di autorità nazionali per garantire il rispetto delle previsioni regolamentari. Più nello specifico l'individuazione del o dei soggetti preposti all'attività di enforcement viene demandata ai singoli Stati Membri che devono attribuire due compiti:

– **la funzione di notificazione** (art. 28 del Regolamento IA): volta a verificare la regolarità delle attività di certificazione rilasciate da soggetti terzi a chi crea sistemi di intelligenza artificiale che rientrano nella categoria ad alto rischio.

[127] Ai sensi del Regolamento IA si definisce Sistema IA "un *sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti o raccomandazioni che possono influenzare ambienti fisici o virtuali*".

[128] Ai sensi del Regolamento IA si definisce *fornitore*: "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito*".

[129] Ai sensi del Regolamento IA si definisce *deployer*: "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale*".

– **la funzione di controllo** (art. 74 del Regolamento IA): volta a verificare che l'AI Act sia rispettato da parte dei produttori e dei distributori di sistemi di IA.

Per recepire tali disposizioni nonché integrare le prescrizioni regolamentari e più in generale promuovere "un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità[130]" il Governo ha presentato il disegno di legge 1146/2024, attualmente in corso di esame al Senato[131] che designa come autorità nazionali per l'intelligenza artificiale l'Agenzia per l'Italia Digitale (funzione di notificazione) e l'Agenzia per la Cybersicurezza Nazionale (funzione di controllo) e demanda loro il compito di assicurare "*il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti*" (art. 18).

L'articolo 18 rischia tuttavia di essere foriero di criticità nell'ambito della vigilanza bancaria sui soggetti che meglio possono essere comprese solo dopo aver ricostruito il quadro normativo settoriale e le interrelazioni con il regolamento IA.

3 Normativa prudenziale e Intelligenza Artificiale

L'utilizzo di tecnologie di automazione da parte delle banche rileva nella attività di vigilanza della Banca d'Italia: ancor prima della approvazione del regolamento UE l'utilizzo di sistemi IA da parte delle banche era idoneo ad essere ricompreso nel generale obbligo per le banche di dotarsi di robusti dispositivi di Governance Interna atti ad identificare e gestire i rischi a cui possono essere esposte (ex art. 74 della Direttiva 2013/36/EU c.d. CRD)[132].

Il suddetto obbligo è approfondito dalla normativa secondaria[133] con specifico riguardo alla gestione del rischio informatico (ICT): la gestione del rischio ricade, nella responsabilità dell'organo di supervisione strategica e nella competenza dell'organo di gestione che deve assicurare

[130] Art. 1 D.d.L. 1146/2024.

[131] <https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm>.

[132] R. Lener, *Vigilanza Prudenziale e Intelligenza Artificiale (Prudential Supervision and Artificial Intelligence),* in *La supervisione finanziaria dopo due crisi. Quali prospettive,* Wolters Kluwer - Cedam.

[133] Banca d'Italia, *Circolare 285/2013* ("Titolo IV – Capitolo 4 Il Sistema Informativo").

la completezza, adeguatezza e funzionalità del sistema informativo; la vigilanza sulla adeguata gestione di tale rischio spetta alla valutazione *ex post*, della Banca d'Italia, nell'ambito dello SREP, che nell'ottica dei principi di sana e prudente gestione della banca valuterà la gestione del rischio informatico anche da un punto di vista qualitativo[134].

Il framework normativo emergente, dal combinato disposto della normativa bancaria e del regolamento IA è estremamente complesso e presenta sovrapposizioni fra discipline diverse, *ratio* differenti e Autorità concorrenti con rischi di duplicazione degli obblighi a carico dei soggetti vigilati.

Il Regolamento IA ha cercato di garantire un coordinamento sia dal lato dei soggetti vigilati che delle attività di vigilanza: per quanto concerne i "controllati" gli articoli 17 e 26 del Regolamento hanno previsto che si consideri assolto, dagli enti creditizi fornitori e/o utilizzatori di sistemi di IA ad alto rischio, l'obbligo di istituire un sistema di gestione della qualità e di monitorare il sistema high risk, laddove tali enti rispettino le norme sui dispositivi, i processi e i meccanismi di governance interna stabiliti nelle rigorose disposizioni di vigilanza.

Lato vigilanza sull'intelligenza artificiale, il regolamento europeo, nei suoi considerando, ha indicato l'opportunità che le autorità competenti del controllo e dell'esecuzione della CRR[135], della CCD[136], della CRD[137] e della Direttiva 2014/17/UE venissero designate, nell'ambito delle rispettive competenze, quali autorità competenti ai fini del controllo dell'attuazione del regolamento IA stesso, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA ad alto rischio forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza[138].

---

[134] L. Donato, *Banche e Intelligenza artificiale. Sviluppi, rischi e regolamentazione* in *Bancaria* n. 7/8 2024*, pp. 63 ss.*

[135] Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012.

[136] Direttiva 2008/48/CE del Parlamento Europeo e del Consiglio del 23 aprile 2008 relativa ai contratti di credito ai consumatori e che abroga la Direttiva 87/102/CEE.

[137] Direttiva 2013/36/UE del Parlamento Europeo e del Consiglio del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE.

[138] Considerando 158 Regolamento IA.

Il suddetto considerando viene esplicitato dall'art. 74 il quale statuisce che:
«6. Per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale diritto, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di tali servizi finanziari.
7. In deroga al paragrafo 6, in determinate circostanze e a condizione che sia garantito il coordinamento, lo Stato membro può individuare un'altra autorità competente come autorità di vigilanza del mercato ai fini del presente regolamento».

Il Disegno di Legge 1146/2024 fa ricorso alla deroga di cui al comma 7 (senza motivare in alcun modo l'esistenza di particolari circostanze) ed esclude la Banca d'Italia, dalla vigilanza sui sistemi di intelligenza artificiale utilizzati dalle banche.

Non è tuttavia pensabile che la vigilanza prudenziale abdichi al compito di controllare i sistemi di intelligenza artificiale dal punto di vista della sana e prudente gestione della banca, circostanza questa confermata anche dalla Banca Centrale Europea che nel sottolineare come taluni obblighi del Regolamento IA siano da considerarsi integrativi rispetto alle disposizioni della CRD in tema di governance interna e di gestione del rischio si è riservata di emanare "aspettative di vigilanza" in merito[139].

Punto dirimente diviene allora quello di capire come coordinare la vigilanza per soggetti con la vigilanza sulla tecnologia.

4 Credit scoring algoritmico e modalità di coordinamento fra discipline

Vi è un ambito nel quale l'intelligenza artificiale si interseca non solo con la normativa prudenziale ma anche con quella di trasparenza del titolo VI del TUB: l'attribuzione del merito creditizio mediante algoritmi (c.d. credit scoring algoritmico).

Dal punto di vista del cliente/consumatore, l'utilizzo delle tecniche di IA offre opportunità in termini di inclusione finanziaria: fasce di popolazione che non hanno facile accesso ai servizi finanziari a causa della mancanza delle informazioni tradizionalmente utilizzate nella valutazione del

[139] Banca Centrale Europea, *Parere della Banca Centrale Europea del 29 dicembre 2021 relativo a una proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale.*

merito di credito possono divenire "scrutinabili" a costi ridotti dagli intermediari ai fini della concessione di un credito; ed ancora tali strumenti possono significativamente accelerare i tempi di risposta nella concessione dei prestiti arrivando in alcuni casi a permetterne l'istantanea erogazione.

Le tecniche di analisi e valutazione che consentono di conseguire questo vantaggio presentano tuttavia rischi; tra queste la possibilità che il crescente utilizzo di simili soluzioni tecnologiche porti a "nuove" esclusioni, ad esempio in conseguenza di selezioni distorte da forme di discriminazione, anche involontaria, generata da modelli non governati di cui non sono note tutte le determinanti che conducono alla decisione[140].

La normativa bancaria sulla trasparenza contiene riferimenti generali in materia di discriminazione che, seppur limitati ai temi dell'accesso ai servizi di pagamento, introducono una definizione di ciò che può essere reputato discriminatorio nel contesto bancario-finanziario:

– in materia di credito immobiliare ai consumatori, l'art. 120-*undecies* del TUB, relativo alla verifica del merito creditizio, afferma al comma 1 che «[…] *La valutazione del merito creditizio è effettuata sulla base delle informazioni sulla situazione economica e finanziaria del consumatore necessarie, sufficienti e proporzionate e opportunamente verificate*», ponendo dunque dei requisiti alle caratteristiche dei dati utilizzati dall'intermediario ai fini del credit scoring. Il comma 5 aggiunge che *«Quando la domanda di credito è respinta, il finanziatore informa il consumatore senza indugio del rifiuto e, se del caso, del fatto che la decisione è basata sul trattamento automatico di dati*», evidenziando un diritto del consumatore ad essere informato qualora il rifiuto della sua domanda di credito immobiliare sia stato basato sull'utilizzo di forme di algorithmic credit scoring[141].
– in materia di credito ai consumatori l'124-*bis* del TUB prevede che i finanziatori, debbano rispettare i principi di sana e prudente gestione, nella verifica del merito creditizio, acquisendo "*informazioni adeguate*" ricorrendo ove necessario anche a "*banche dati pertinenti*".

[140] M. Bianco, *Intelligenza artificiale nel credit scoring: analisi di alcune esperienze nel sistema finanziario italiano Presentazione del QEF in pubblicazione,* <https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2022/Bianco-12102022.pdf>.

[141] E. Bonaccorsi di Patti, F. Calabresi, B. De Varti, F. Federico, M. Affinito, M. Antolini, F. Lorizzo, S. Marchetti, I. Masiani, M. Moscatelli, F. Privitera e G. Rinna, *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, <https://www. bancaditalia.it/pubblicazioni/qef/2022-0721/QEF_721_IT.pdf>, p. 24.

La materia sarà peraltro oggetto di future integrazioni ad opera del recepimento della *Consumer Credit Directive II,* la quale all'art 18 espressamente menziona la possibilità di valutare il merito creditizio tramite strumenti automatizzati a patto che i consumatori venga dato il diritto di chiedere e ottenere l'intervento umano del creditore e una spiegazione significativa della valutazione del merito creditizio, nonché di esprimere il proprio punto di vista e contestare tale valutazione.

Oltre agli aspetti di trasparenza l'attribuzione del merito creditizio rileva anche, nell'ambito della vigilanza prudenziale dal punto di vista del rischio di credito e in quell'obbligo per gli intermediari, durante la fase istruttoria di raccogliere tutte le informazioni necessarie per valutare il merito di credito mediante l'utilizzo di sistemi di scoring o rating[142].

Allo stesso tempo, il credit scoring algoritmico è ricompreso espressamente dall'AI Act fra le attività ad alto rischio, per via dell'impatto che può avere sulla vita degli individui e del rischio di introdurre o perpetuare dinamiche di discriminazione nella valutazione dell'affidabilità creditizia delle persone. Viene pertanto imposto a tali sistemi il rispetto di specifici requisiti in materia di qualità dei dati, documentazione, trasparenza verso i clienti, monitoraggio e sorveglianza umana.

Le competenti autorità si trovano dunque a dover assicurare da un lato che tali sistemi non siano discriminatori, escludendo ad esempio dall'accesso al credito alcuni richiedenti sulla scorta di *bias* storici, magari incentrati su genere o razza, e dall'altro lato che non siano lesi i principi di sana e prudente gestione dell'intermediario finanziario, primo fra tutti quello secondo il quale il credito non va concesso a tutti coloro che lo richiedono ma solo a coloro che meritano di averlo in base alle capacità di rimborso[143].

Per assicurare che un sistema di credit scoring algoritmico sia etico, rispettoso della normativa in materia di trasparenza e al tempo stesso gestionalmente sano e prudente, sarebbe opportuno ed efficiente, che i controlli sul corretto adempimento degli obblighi degli intermediari in tema di intelligenza artificiale, venissero effettuati da un'unica autorità piuttosto che da autorità distinte.

---

[142] E. Bonaccorsi di Patti, F. Calabresi, B. De Varti, F. Federico, M. Affinito, M. Antolini, F. Lorizzo, S. Marchetti, I. Masiani, M. Moscatelli, F. Privitera e G. Rinna, *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, <https://www. bancaditalia.it/pubblicazioni/qef/2022-0721/QEF_721_IT.pdf>, p. 21.

[143] L. Ammannati, G. Grieco, *Il credit scoring "intelligente": esperienze, rischi e nuove regole*, in *Rivista di diritto bancario*, luglio/settembre 2023 p. 508.

Questa non è al momento la strada intrapresa dal legislatore italiano; ciò impone di trovare modalità differenti per contemperare le varie discipline e ripartire i compiti fra soggetti preposti alla vigilanza: una modalità potrebbe essere quella per le autorità di concordare tra loro, mediante protocolli di intesa, un riparto basato sulle finalità che ciascuna di loro persegue: garantire la sicurezza e solidità delle banche per quanto riguarda la normativa prudenziale; tutelare il contraente debole per quanto concerne la normativa in materia di trasparenza; evitare che i singoli cittadini possano vedere lesi i loro diritti fondamentali da sistemi di intelligenza artificiale.

Tuttavia, tale modalità difficilmente potrà la stessa efficacia che potrebbe avere l'attribuzione da parte del legislatore alla Banca d'Italia della vigilanza sui sistemi di intelligenza artificiale ad alto rischio utilizzati dalle banche.

5 Conclusioni

Il complesso framework normativo che emerge in queste pagine riguarda non solo l'ambito della vigilanza bancaria ma anche l'ambito assicurativo e dei mercati finanziari.

Il disegno di legge 1146/2024 aggiunge complessità al quadro senza che ciò venga compensato da alcun beneficio: aumenta il numero di autorità a cui i soggetti vigilati dovrebbero far riferimento, peraltro sulla base del tipo di tecnologia impiegata, con conseguente rischio di sovrapposizioni, incertezze applicative e potenziali incongruenze[144].

Né ciò peraltro potrebbe essere giustificato dalla mancanza di competenze in materia di nuove tecnologie da parte delle autorità di vigilanza nazionali posto che da tempo si sta assistendo ad una integrazione delle stesse, tramite l'assunzione di personale altamente specializzato in materia di data science ed intelligenza artificiale e attività di formazione in materia.

Alla luce di tale evidenza, e vista che non è ancora intervenuta l'approvazione in prima lettura sarebbe forse opportuno apportare modifiche al disegno di legge e prevedere una architettura istituzionale più in linea con l'AI ACT; il che risponderebbe a ragioni di sistema, di semplificazione e di cautela, considerata anche la velocità con cui evolvono tanto la tecnologia legata all'Intelligenza Artificiale quanto l'impiego della stessa nel settore finanziario.

F. Cornelli, Intervento al convegno "L'impatto dell'AI Act sul mondo finanziario", https://www.consob.it/documents/1912911/4049643/intervento_Cornelli_20240716.pdf/deedb827-c2bb-9108-f454-d430a3a347ba

L'auspicio è che il legislatore prenda in considerazione i suggerimenti fornitigli, al fine di implementare una soluzione normativa efficace e adeguata alle esigenze di un contesto altamente dinamico come quello dell'intelligenza artificiale.

Andrea Carrisi

Intelligenza Artificiale, architetture di vigilanza e ipotesi di conflitto

L'approccio eurounitario sul tema della regolazione della vigilanza del mercato dell'intelligenza artificiale è caratterizzato dalla tendenza ad accentrare la supervisione con autorità specializzate, pur ammettendo a certe condizioni la designazione di quelle esistenti. Nel settore finanziario, viceversa, il regolamento europeo ritiene allo scopo naturale la designazione dell'autorità nazionale responsabile della vigilanza finanziaria, salvo decisioni in deroga supportate da specifiche circostanze.
Dopo un rapido sguardo sugli ordinamenti esteri, l'articolo si sofferma sull'ordinamento italiano, che con il DDL n. 1146/2024 – diversamente dall'impostazione europea – predilige un accentramento assoluto su AgID e ACN, senza attribuire alcun specifico rilievo all'autorità di vigilanza finanziaria nazionale. Tale scelta, in deroga a quanto stabilito dall'AI Act, solleva interrogativi sui confini di competenza e sulla necessità di un raccordo per garantire una vigilanza coerente ed efficace.

1 Geometria delle competenze della vigilanza. modello eurounitario e modello italiano

Tutela della democrazia, dello Stato di diritto e della sostenibilità ambientale nonché promozione dell'innovazione.

Questi, in estrema sintesi, gli obiettivi di tutela e promozione previsti dal Regolamento (UE) 2024/1689 (d'ora in avanti, anche *AI Act*), il quale stabilisce regole armonizzate sull'intelligenza artificiale, profilando – allo scopo e per quel che qui più interessa – un potere di vigilanza delle dinamiche del relativo mercato.

L'approccio eurounitario e, a cascata, dei singoli stati europei sul tema del controllo sull'intelligenza artificiale è caratterizzato dalla tendenza ad accentrare la supervisione dei diversi mercati con l'istituzione di autorità specifiche e specializzate e che esercitino la propria attività trasversalmente.

Accentramento, però, tendenziale e non assoluto: il regolamento non impone, infatti, l'istituzione di nuove autorità ma consente l'alternativa *designazione* di autorità esistenti. Sul punto l'art. 70, par. 1, *AI Act* prevede che ciascun Stato membro «*istituisce o designa*» come autorità nazionali competenti «*almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato*».

A riguardo, con tecnica normativa di rinvio, l'art. 74, par. 3, precisa che i sistemi di IA ad alto rischio collegati ai prodotti disciplinati dalla normativa di armonizzazione elencata nell'allegato I, sez. A (ad es. dispositivi di protezione individuale, apparecchi che bruciano carburanti gassosi, dispositivi medici, ecc.) sono soggetti alla vigilanza delle autorità responsabili per i relativi mercati, salva la possibilità per gli Stati – in determinate circostanze e purché sia garantito il coordinamento con l'autorità di mercato pertinente – di designare altra autorità.

Allo stesso modo, nel settore finanziario – con riguardo ai sistemi di IA ad alto rischio – le autorità di vigilanza finanziarie sono designate quali autorità competenti ai fini del controllo dell'attuazione della disciplina sull'IA (si v. art. 74, par. 6, primo comma, *AI Act*, secondo cui l'autorità di vigilanza è «*l'autorità nazionale pertinente responsabile della vigilanza finanziaria*»), salvo, anche in questo caso, che gli Stati membri decidano «*in deroga*» ai sensi del successivo par. 7, individuando «*un'altra autorità competente come autorità di vigilanza del mercato*» ma ciò soltanto «*in determinate circostanze e a condizione che sia garantito il coordinamento*».

La preferenza dell'estensione di competenza delle autorità di vigilanza finanziaria si fonda sul presupposto (cfr. considerando n. 158, *AI Act*) che la fornitura di servizi integrati con sistemi di IA non muta la disciplina finanziaria applicabile, in particolare con riguardo alle regole e ai requisiti in materia di *governance* interna e di gestione dei rischi. Da qui, l'*AI Act* – al fine di garantire la coerenza dell'applicazione e dell'esecuzione degli obblighi previsti dallo stesso regolamento e delle regole e dei requisiti in materia di servizi finanziari – attrae nella competenza delle autorità finanziarie anche gli aspetti riguardanti l'intelligenza artificiale.

Le autorità finanziarie dovrebbero allora disporre di tutti i poteri previsti dall'*AI Act* e dal regolamento (UE) 2019/1020 (regolamento sulla vigilanza del mercato e sulla conformità dei prodotti), compresi i poteri per svolgere attività di vigilanza del mercato *ex post*.

Tuttavia, anche in relazione al settore finanziario, l'idea di accen-

trare il controllo non esclude che gli Stati membri decidano diversamente, designando – come detto – un'altra autorità per svolgere i compiti di vigilanza del mercato.

La medesima geometria delle competenze di vigilanza non si riscontra nel DDL n. 1146/2024, nel quale l'accentramento è invece assoluto: l'art. 18 del disegno individua l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) quali esclusive autorità (*rectius*, agenzie, che paiono ispirate non già al modello delle autorità indipendenti ma a quello degli organismi amministrativi) competenti per la vigilanza sul mercato dell'intelligenza artificiale.

In particolare:

a) l'AgID è responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale e provvede a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale;

b) l'ACN, invece, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale; la stessa autorità nazionale è, altresì, responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza;

c) infine, le due autorità, AgID e ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normazione nazionale ed europea.

Il comma 2 dell'art. 18 prevede poi una forma di coordinamento e collaborazione «*nonché ogni opportuno raccordo*» (con l'istituzione del "Comitato di coordinamento") tra le autorità nazionali per l'intelligenza artificiale (AgID e ACN) e le altre pubbliche amministrazioni e le autorità indipendenti.

Dunque, l'architettura immaginata dal legislatore nazionale – accentrata su due agenzie nazionali trasversali – si discosta da quella progettata dal legislatore europeo, soprattutto con riguardo all'area finanziaria: non è prevista per le autorità finanziarie alcuna riserva di vigilanza sui sistemi di IA – nemmeno ad alto rischio – impiegati nel settore finanziario. Tanto avviene con la previsione di un raccordo, almeno di principio, con le altre autorità ma senza rappresentare alcuna delle "*determinate circostanze*" richieste dal Regolamento per consentire agli Stati di decidere in deroga rispetto a quanto stabilito dall'art. 74, par. 6, *AI Act*.

2 Vigilanza del mercato dell'IA negli ordinamenti esteri

Diversi ordinamenti esteri si son posti (e tutt'ora sono in corso discussioni e approfondimenti) il tema della vigilanza sul mercato dell'intelligenza artificiale, con diversità di metodi.

In tema, il Regno Unito ha adottato un approccio settoriale, affidando alle singole autorità esistenti il compito di vigilare l'integrazione dell'IA nelle diverse attività[145].

Secondo questo approccio, l'organismo di regolamentazione finanziaria *Financial Conduct Authority* (FCA) si occupa dell'utilizzo dell'IA nel contesto dei mercati finanziari, collaborando con le altre autorità: in particolare, per i dati l'ICO, *Information Commissioner's Office*, per la concorrenza la CMA, *Competition and Markets Authority,* e, infine, per le comunicazioni l'Ofcom, *Office of Communications*; collaborazione che si realizza nel contesto del *Digital Regulation Cooperation Forum*, DRCF[146], e avente ad oggetto lo scambio di informazioni e la risoluzione congiunta di questioni intersettoriali.

Nell'area nordamericana, è in corso di approvazione l'*Artificial Intelligence and Data Act* (AIDA, Bill C-27)[147], normativa con la quale il Canada intende regolare o vietare i fenomeni collegati all'utilizzo dell'intelligenza artificiale, segnatamente:

«*(a) to regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems; and*

(b) to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests».

L'AIDA propende per un modello accentrato, attribuendo la vigilanza del mercato dell'IA al Ministro competente (sez. 31, AIDA), con la possibilità di designare un funzionario di alto livello del ministero, l'"*Artificial Intelligence and Data Commissioner*", per assistere il ministro nell'applicazione dell'AIDA (cfr. sez. 33 (1): «*The Minister may designate a senior official of the department over which the Minister presides to be called the Artificial Intelligence and Data Commissioner, whose role is to assist the Minister in the administration and enforcement of this Part*»).

[145] Cfr. *AI Regulation: A Pro-innovation Approach*, in <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>, 2023.

[146] Fca, *AI Update*, <https://www.fca.org.uk/publication/corporate/ai-update.pdf>, 2024.

[147] Consultabile su <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>.

In questo modello, l'accentramento non soffre deroghe: la disciplina canadese non prevede disposizioni diverse applicabili all'utilizzo di sistemi di IA nel settore finanziario né in altri settori.

Ancora, nell'ordinamento brasiliano è in corso di approvazione una disciplina normativa (di cui al Bill No. 2338/2023[148]) che pare propendere per un modello di vigilanza accentrata: la competenza spetterebbe ad un organo della pubblica amministrazione (si v. l'art. 4, lett. V, secondo il quale è autorità competente un «*órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional*») che dovrà inoltre regolamentare l'utilizzo di sistemi di IA che comportino l'esposizione a rischi eccessivi (art. 16).

L'autorità competente, inoltre, dovrà coordinarsi con le altre autorità dei diversi settori economici al fine di esercitare i propri poteri (art. 32, lett. VII e, soprattutto, art. 34: «*A autoridade competente e os órgãos e entidades públicas responsáveis pela regulação de setores específicos da atividade econômica e governamental coordenarão suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento desta Lei. § 1º A autoridade competente manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as suas competências regulatória, fiscalizatória e sancionatória*»).

3 Ipotesi di conflitto nell'architettura di vigilanza italiana. Confini di competenza tra Agid, Acn e Consob

L'autorità europea di vigilanza dei mercati finanziari nel *Public statement On the use of Artificial Intelligence (AI) in the provision of retail investment services*[149] del maggio 2024 ha ricondotto i potenziali rischi derivanti dall'utilizzo delle tecnologie basate sull'IA in quattro categorie problematiche:

(i) eccessivo affidamento: il rischio che fornitori di servizi e clienti si affidino eccessivamente all'IA per il processo decisionale e trascurino l'importanza del giudizio umano;

(ii) mancanza di trasparenza e di comprensibilità o interpretabilità del sistema di IA: difetti di trasparenza, comprensibilità e interpreta-

[148] Consultabile su https://clairk.digitalpolicyalert.org/documents/brazil-bill-on-the-use-of-artificial-intelligence-2338-2023-original-language/raw

[149] Consultabile su <https://www.esma.europa.eu/document/public-statement-ai-and-investment-services>.

bilità dei sistemi di intelligenza artificiale pongono problemi di giustiziabilità delle scelte;

(iiii) mancanza di sicurezza e di privacy dei dati: raccolta, archiviazione ed elaborazione dei *big data* richiesti dagli strumenti di IA sollevano preoccupazioni in materia di privacy e sicurezza.

(iv) scarsa qualità dei dati di addestramento e mancanza di affidabilità dei risultati dell'IA: nella consulenza in materia di investimenti e nella prestazione del servizio di gestione del portafoglio, *bias* algoritmici e risultati errati possono condurre a consigli finanziari fuorvianti e all'assunzione di rischi imprevisti.

Presupposto questo panorama, con riferimento al modello di vigilanza immaginato dal disegno di legge nel nostro ordinamento, in particolare sul problema della ripartizione delle competenze, possono immaginarsi alcuni scenari di conflitto.

Si pensi ad un intermediario che implementi un sistema basato sull'intelligenza artificiale per la profilazione degli investitori e che tale IA analizzi grandi quantità di dati (età, reddito, investimenti pregressi, attività sui *social network*, ecc.) per la creazione di profili di rischio molto dettagliati. L'analisi dei dati o la progettazione dell'IA potrebbe essere causa di *bias* ("*algorithmic biases*", cfr. la citata dichiarazione di Esma) e configurare di conseguenza forme di discriminazione basate su tali fattori (ad es. persone anziane avverse al rischio e loro limitazione rispetto a prodotti più redditizi).

In casi come questo, l'Agenzia per l'Italia digitale e l'Agenzia per la cybersicurezza nazionale dovrebbero ritenersi competenti a valutare la conformità del sistema di IA ai requisiti di accuratezza, non discriminazione e trasparenza previsti dall'*AI Act* e a verificare se l'algoritmo di profilazione conduca a discriminazioni nonché se l'intermediario abbia adottato tutte le misure necessarie per mitigare i rischi di *bias*. D'altra parte, l'autorità di vigilanza finanziaria, Consob, è competente a vigilare sul rispetto della normativa in materia di profilazione degli investitori e di raccomandazione degli investimenti, in particolare in ordine al rispetto del criterio di adeguatezza; dunque, a verificare in concreto la proposta da parte dell'intermediario di prodotti finanziari adatti al profilo di rischio e agli obiettivi di investimento dei clienti.

Si pensi, ancora, ad un intermediario che implementi l'intelligenza artificiale per la gestione di fondi di investimento (selezione dei titoli, bilanciamento del portafoglio) e che addestri il sistema con dati sintetici[150].

[150] I dati sintetici sono dati generati mediante algoritmi di apprendimento automatico e che replicano le proprietà statistiche dei dati reali, preservando al contempo la privacy e

In questo caso, le autorità nazionali per l'intelligenza artificiale – AgID e ACN – sarebbero competenti a valutare la qualità del *dataset* sintetico utilizzato per addestrare l'IA e a verificare il rispetto dei requisiti di accuratezza, rappresentatività e non discriminazione. Le stesse autorità, inoltre, dovrebbero poter accertare l'adozione da parte dell'intermediario delle misure di monitoraggio e di aggiornamento dei dati. Spetterebbe, invece, a Consob la valutazione sull'adeguatezza del sistema di gestione del rischio e il rapporto tra utilizzo dei dati sintetici e compromissione della tutela degli investitori. Ancora, di competenza di Consob sarebbe anche la verifica sul rispetto delle regole di trasparenza e informativa nei confronti degli investitori in relazione all'utilizzo di dati sintetici e di forme di IA.

Infine, pur senza esaurire gli scenari ipotizzabili, è possibile immaginare (o meglio, è già noto) l'utilizzo dell'IA nel campo del *trading* ad alta frequenza per l'esecuzione di ordini ad elevatissime velocità al fine di identificare e sfruttare piccole inefficienze di prezzo. Si pensi a errori di progettazione *software* o al verificarsi di particolari scenari che comportino l'esecuzione da parte dell'intelligenza artificiale di una serie di ordini anomali; ordini che amplifichino un crollo improvviso del prezzo di un titolo azionario e determinino un c.d. *flash crash*.

Le agenzie previste dal DDL dovrebbero quindi valutare la conformità del sistema di IA ai requisiti di robustezza, affidabilità e sicurezza di cui all'*AI Act* e verificare se l'algoritmo sia stato progettato e testato adeguatamente per prevenire comportamenti anomali e per gestire situazioni di mercato estreme. Viceversa, Consob dovrebbe valutare se l'intermediario abbia tenuto comportamenti in violazione della disciplina sulla manipolazione del mercato e accertare l'adozione da parte dell'intermediario di misure di gestione del rischio e di prevenzione dei *flash crash*.

La rapida rassegna di casi di implementazione dell'intelligenza artificiale nei sistemi di investimento palesa possibili sovrapposizioni e potenziali conflitti di competenza tra le autorità di vigilanza finanziaria e le autorità di vigilanza del mercato dell'intelligenza artificiale; conflitti, quindi incertezze, che non aiutano nel procedimento di costruzione dell'affidabilità dell'intelligenza artificiale.

In assenza di – invece auspicabili – disposizioni in deroga per il settore finanziario rispetto all'accentramento della vigilanza sull'intelligenza artificiale, sembra quantomeno opportuno prevedere e prestabilire chiare modalità di cooperazione tra le diverse autorità settoriali, tra cui Consob, e le autorità nazionali per l'IA e, soprattutto, meccanismi di risoluzione dei

la riservatezza delle informazioni sensibili.

possibili conflitti di competenza, anche in relazione alla tutela di interessi ritenuti preminenti.

IVASS

Andrea Aguggia

La vigilanza in ambito assicurativo e l'Intelligenza Artificiale

Il contributo considera le intersezioni e le possibili sinergie tra la normativa riguardante l'Intelligenza Artificiale e quella assicurativa esaminando, in particolare, il D.d.L. 1146/2023.

1 Premessa

L'Intelligenza Artificiale ("IA") è destinata a svolgere un ruolo di primo piano nell'evoluzione dell'industria assicurativa. In combinazione con la diffusione di dispositivi in grado di monitorare l'ambiente in cui sono collocati (l'Internet delle Cose), l'IA getta le basi per cambi di paradigma radicali: dall'analisi di rischio predittivo all'accorciamento della distribuzione dei prodotti assicurativi. Già nel 2018 il 31% delle imprese attive nei rami assicurativi auto e salute ricorreva all'uso congiunto di questi strumenti e un ulteriore 24% era pronta a integrarli nel proprio modello di impresa[151]. Si tratta di una tendenza confermata da analisi di mercato più recenti che conferma il trend di settore per oltre il 50% delle imprese che offrono servizi assicurativi contro i danni e un quarto di quelle che offrono assicurazioni vita[152]. Anche l'IA generativa pare destinata al medesimo pro-

[151] European Insurance and Occupational Pension Auhtority, Annual Report 2018, disponibile a: <https://www.eiopa.europa.eu/publications/eiopa-annual-report-2018_en>.

[152] European Insurance and Occupational Pension Auhtority, Annual Report 2023, disponibile a: <https://www.eiopa.europa.eu/publications/european-insurance_overview-

cesso di integrazione, al momento, specie per i servizi B2C quali servizi personalizzati verso gli assicurati nelle procedure di gestione dei sinistri.

Rispetto a queste traiettorie di mercato, il Regolamento sull'Intelligenza Artificiale ("Regolamento") detta per i soggetti che compongono la catena del valore dell'IA regole *ad hoc* modellate sulla piramide di rischi su cui l'intero tessuto regolamentare poggia. E così i produttori, gli sviluppatori e le imprese che a valle usano l'IA per "[valutare] rischi e la [determinare i] prezzi in relazione alle persone fisiche per assicurazioni sulla vita e assicurazioni sanitarie" sono ritenuti in grado di arrecare un significativo impatto sulle persone. Ne consegue l'obbligo di operare rispettando quei requisiti volti a minimizzare i rischi per non incidere negativamente sulla vita e la salute, specie per i soggetti vulnerabili[153]. Per contro, esula da tali preoccupazioni l'IA adoperata per rilevare frodi, soggetta a più miti requisiti[154]. Da ultimo, alcune applicazioni della tecnologia in esame destinate ad un'interazione che mima quella umana (con scrittura, con voce o con entrambe, ad esempio, le chatbot virtuali) sono soggette a obblighi di trasparenza diretti a rivelare fin dal primo contatto con il destinatario la natura artefatta della medesima[155].

2 L'IA e l'industria assicurativa. Cenni

Per comprendere le conseguenze nel settore assicurativo del Regolamento occorre in prima battuta identificare quali sistemi di IA sono regolati. La definizione fornita dal Regolamento, come noto, sconta l'inaspettata proliferazione di sistemi di IA a scopi generali che ha portato il legislatore europeo a ricalibrarne in corso d'opera il perimetro. In linea con l'OCSE, anch'essa costretta al medesimo ripensamento, nel Regolamento si intende per sistema di IA un sistema progettato per funzionare con differenti gradi di autonomia e che è in grado di generare decisioni dedotte capaci di influenzare ambienti fisici o virtuali. Questa definizione, benché

report-2023_en>.

[153] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 - Considerando 138.

[154] *Ibid.*

[155] *Ibid.* Art. 50.

analitica, patisce un certo livello di incertezza legato, in particolare, a cosa in concreto si intenda per "differenti gradi di autonomia". L'attuale sviluppo tecnico rende infatti residuali gli algoritmi che traducono il comando dello sviluppatore di agire in un determinato modo rispetto a uno scenario prestabilito (se X allora Y). Il passo in avanti risiede proprio nel fornire al sistema almeno un minimo di capacità di improvvisazione nella generazione dell'*output* rispetto a un *set* di dati. L'autonomia pare dunque un criterio fragile perché capace di catturare troppo. Allo stato attuale, e in attesa delle già annunciate precisazioni da parte della Commissione europea attese nel primo quadrimestre del 2025, non sono sistemi di IA solo quelli che operano con rigide regole predefinite per automatizzare il processo di richiesta che vengono considerati meri software.

Calato nel settore in esame e nelle applicazioni ad oggi più diffuse, il Regolamento ricomprende dunque le chatbots che permettono la comunicazione fra intermediari assicurativi e clienti, nonché i sistemi di IA usati per dedurre e differenziare i rischi degli assicurati secondo le loro differenti caratteristiche personali. È sulla scorta di tale osservazione preliminare che occorre procedere con l'analisi del vertice della piramide dei rischi, quelli vietati, e, in particolare, sempre per lo speciale rilevo assunto nell'industria in esame, i sistemi di IA che adottano tecniche subliminali o ingannevoli per distorcere il comportamento umano inducendolo ad assumere una decisione che quella persona (o gruppo di persone) non avrebbe altrimenti preso, in modo da causare un danno significativo a quella persona, a un'altra persona o a un gruppo di persone.

Non si tratta, tuttavia, di un divieto assoluto, in quanto il Regolamento consente il ricorso a sistemi di IA manipolativa a condizione che non si verifichi un "*danno significativo*". La chiosa preliminare fa ritenere che l'uso di tali sistemi sia da escludere in quanto, come previsto dall'articolo 199-bis del Codice delle Assicurazioni, i distributori che ricorrono, ove concesso, a sistemi di IA manipolativi, saranno comunque tenuti a conformarsi con disposizioni che richiedono ai distributori assicurativi di "*operare con equità, onestà, professionalità, correttezza e trasparenza nel miglior interesse dei contraenti*". Ne consegue la verosimile violazione di questo principio ogniqualvolta un'organizzazione della distribuzione strutturata sull'uso di sistemi di IA influenzi indebitamente la decisione dei clienti con cui il distributore entra in contatto, a prescindere dall'eventuale danno significativo che può derivarne (osterebbe comunque a tale tecnica, in linea di principio, la correttezza richiesta all'impresa dalla disciplina consumeristica).

3 Il coordinamento fra l'AI Act e la normativa nazionale

Il Regolamento mira a rendere l'Unione Europea un "*leader nell'adozione di un'IA affidabile*"[156]. Rileva qui l'enfasi posta sull'applicazione conforme ai valori dell'Unione sanciti dalla Carta per promuovere un'IA antropocentrica e affidabile e garantire al contempo l'uniformità del mercato unico; obiettivo raggiungibile solo se l'azione delle istituzioni europee e degli Stati Nazionali è coordinata. Anche per questo il Regolamento prevede di istituire un'autorità europea centrale e delle autorità nazionali satelliti. Gli Stati Membri, in particolare, sono tenuti a nominare, da un lato, un'autorità col compito di verificare la regolarità delle attività di certificazione che sono state rilasciate da soggetti terzi a favore di chi crea sistemi di IA che rientrano nella categoria ad alto rischio[157] e dall'altro, un'autorità di controllo, incaricata di verificare che il Regolamento sia rispettato tanto dai produttori quanto dai distributori di sistemi di IA[158].

In tale ottica il legislatore nazionale con il DDL presentato al Senato il 20 maggio 2024 attribuisce all'articolo 18 la competenza a vigilare sull'impiego di modelli e sistemi di intelligenza artificiale all'Agenzia per l'Italia digitale ("AgID"), con funzione di notificazione, e all'Agenzia per la cybersicurezza ("ACN"), con funzione di controllo. E questo anche quando i sistemi di IA vengono utilizzati nell'ambito delle attività assicurative soggette a vigilanza IVASS[159].

Alla luce della scelta fatta dal Legislatore nazionale, diviene dunque fondamentale individuare forme di coordinamento delle Agenzie nazionali competenti per l'AI con le Autorità Indipendenti di settore, per evitare sovrapposizioni di compiti potenzialmente in grado di creare inefficienze. Al riguardo, l'esclusione delle *Autorithies* da attività fondamentali, quali, ad esempio, le sperimentazioni in ambiente *Sandbox*, peraltro già in atto da tempo, contribuisce ad alimentare le perplessità.

Lo stesso DDL citato evoca la necessità di un raccordo, ma occorre comprendere se e in che limiti quest'ultimo sia sufficiente a scongiurare i rischi legati alla moltiplicazione dei "centri" di controllo. Ciò a maggior ragione considerando che il Regolamento prevede un regime parzialmente in deroga per l'industria assicurativa. Nei Considerando si legge, infatti, che

[156] *Ibid.* Considerando 2.

[157] *Ibid.* Articolo 28.

[158] *Ibid.* Articolo 74.

[159] P. Marano, *L'impatto del Regolamento Europeo sull'Intelligenza Artificiale ("AI Act") sulla distribuzione assicurativa: prime riflessioni*, Assicurazioni, fascicolo 3, 2024.

"per migliorare ulteriormente la coerenza [del Regolamento] e le regole applicabili" "alle imprese di assicurazione di riassicurazione e alle società di partecipazione assicurativa (…) nonché agli intermediari assicurativi"[160], è opportuno integrare obblighi e procedure previste nella normativa applicabile in materia di gestione dei rischi e, per evitare sovrapposizioni, prevedere deroghe sia per i fornitori di IA sia per gli obblighi di monitoraggio pendenti sugli utilizzatori.

Da ciò consegue che per i profili che non sono disciplinati dal Regolamento, l'uso dei sistemi di IA rimane soggetto alla disciplina sulla distribuzione dell'attività assicurativa[161]. Per via del combinato disposto dall'articolo 74 con il Considerando 158 del Regolamento, sembrerebbe così rientrare tra i compiti dell' EIOPA e delle Autorità di vigilanza nazionali in materia assicurativa evitare duplicazioni nell'esecuzione degli adempimenti richiesti dal Regolamento rispetto a quelli contenuti nella disciplina assicurativa, tenendo conto del principio di proporzionalità e delle specificità del settore assicurativo[162].

4 La personalizzazione dell'offerta assicurativa

La selezione e la tariffazione dei rischi, come noto, sono al centro del processo industriale assicurativo. L'incompletezza delle informazioni segna l'attività degli assicuratori, posti in condizione di svantaggio informativo nel valutare ogni caratteristica di rischio dei potenziali clienti. Finora, l'accertamento si è rivelato complesso ed incerto, affidato alle dichiarazioni su eventi passati rese in fase precontrattuale. A ciò va aggiunto che, talvolta, la rischiosità dell'assicurato aumenta una volta ottenuta la copertura assicurativa.

Il cambio radicale apportato dalla possibilità di raccogliere e analizzare i dati dei potenziali clienti risiede nella possibilità di svolgere l'attività di selezione e tariffazione con un metodo non più statico ma dinamico e, negli stadi applicativi più avanzati, prospettico. È in tale ottica che, tra le

[160] Regolamento IA, Considerando 158.

[161] E la regolazione nonché la vigilanza assicurativa dell'UE hanno come obiettivo "l'adeguata tutela dei contraenti [e] di qualsiasi persona fisica o giuridica titolare di un diritto in virtù di un contratto di assicurazione", ossia dei beneficiari; Considerando 18 e articolo 27, Direttiva 2009/138/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 in materia di accesso ed esercizio delle attività di assicurazione e riassicurazione.

[162] P. Marano, cit., n. 9.

altre cose, va esaminata la tendenza delle imprese verso la personalizzazione del premio. Secondo la metodologia tradizionale l'impresa assicuratrice distribuisce il costo dei futuri sinistri tra titolari di polizze: la stima è basata sulle perdite attese di un gruppo, e non su una valutazione individuale. Più nel dettaglio, poiché i prezzi sono determinati calcolando le *chances* che un qualsiasi gruppo di individui, accomunati dal medesimo profilo, possa subire una perdita, l'individuo è trattato come membro di un gruppo[163]. Nel complesso, abbiamo assistito alla definizione di classi di rischio per collocare la perdita attesa da ogni assicurato e per categorizzare gruppi che condividono questo medesimo valore in modo da addebitare a ciascuno la medesima tariffa.

Rispetto a tale metodo, l'impatto dell'analisi algoritmica della scia di dati del cliente non risiede nella miglior allocazione del medesimo nella categoria di rischio più consona che, a ben vedere, renderebbe solamente più efficace la prassi già in uso. Il cambio di paradigma risiederebbe nell'erogazione di servizi e premi personalizzati e flessibili che ricalcano le caratteristiche individuali dei potenziali clienti permettendo in ultima istanza di coprire con proattività nuovi scenari di rischio. È un passaggio, tuttavia, non privo di rischi. Se alla base della categorizzazione dei rischi risiede il vantaggio di compensare i premi pagati dagli assicurati con gli indennizzi versati o da uno o da più membri del medesimo *pool*, su alcune categorie di assicurati possono finire per essere apposti premi particolarmente gravosi (se non addirittura escludenti dal mercato) per via della più elevata frequenza di sinistri che li caratterizza. Ne potrebbe conseguire che, nel settore assicurativo, l'accuratezza del profilo di rischio del soggetto è inversamente proporzionale alla probabilità che la sua polizza benefici degli intrinseci effetti correttivi del risk pooling. Si pensi alla personalizzazione dei premi che, in ambito sanitario, espone soggetti affetti da patologie croniche a richieste tanto elevate da renderle insostenibili.

Solleva diverse preoccupazioni la possibilità di rendere il premio dinamico, con periodico adeguamento della sua entità al variare del profilo di rischio del cliente[164]. Pare possibile, da un lato, incentivare condotte virtuose dello stile di vita degli assicurati, influenzando il grado di sinistrosità tramite l'adozione di condotte prudenti, ad esempio con le informazioni trasmesse dalle scatole nere installate nei veicoli con cui è possibile osser-

[163] P. Manes, *Legal Challenges in the Realm of InsurTech*, European Business Law Review, v. 3(1), 2020.

[164] A. Camedda, *La digitalizzazione del mercato assicurativo: il caso della Digital Health Insurance*, Rivista di Diritto Bancario, fascicolo 3, 2018.

vare la guida, dai chilometri percorsi al monitoraggio di attività sospette. Al medesimo risultato giungono i dispositivi indossabili dagli assicurati (e.g. smart watches) che ne monitorano tanto le funzioni vitali quanto gli stili di vita e i comportamenti[165]. Specie nell'ambito delle assicurazioni sanitarie, questa tecnologia consente di accostarsi alle dichiarazioni rese dall'assicurato nel questionario anamnestico per mostrare, nel corso del rapporto o prima della scadenza del rinnovo, che egli assume uno stile di vita salutare. In questo modo è possibile correlare il raggiungimento di determinati indici di benessere prestabiliti al mantenimento di vantaggi di costo (compresi eventuali sconti applicati automaticamente all'annualità successiva). Verrebbe dunque colmata l'asimmetria informativa patita dall'impresa assicuratrice nella fase successiva alla stipulazione del contratto durante cui si è dimostrata di difficile realizzazione una costante sorveglianza dei comportamenti degli assicurati, i quali, anche con condotte omissive, possono aumentare la rischiosità. Per contro, non vanno nascoste le potenziali perplessità che la stessa innovazione può portare. In primo luogo, la dinamicità dei premi correlata al variare del profilo di rischio individuale potrebbe spingere il cliente verso soluzioni più stabili e prevedibili, anche in ottica di preliminare comparazione delle offerte in base al prezzo offerte nel mercato. In secondo luogo, non è da escludere che i costi (umani e tecnici) a carico dell'impresa per sviluppare modelli di analisi dinamici vengano fatti ricadere sul cliente nella voce di caricamento dei premi, riducendo, di fatto, i vantaggi di questo nuovo metodo di tariffazione.

5 Conclusioni

L'esempio appena esaminato delle principali tendenze di mercato va collocato nel contesto regolamentare previsto dall'AI Act. Come detto in premessa, quella assicurativa è un'attività che ricade nella categoria dell'alto rischio, per via dei possibili effetti discriminatori che potrebbe indurre o perpetuare. I requisiti imposti ai sistemi finalizzati a questo scopo riguardanti la qualità dei dati, la documentazione, la trasparenza, la tracciabilità nonché il monitoraggio e la sorveglianza umana sono la risposta a queste potenziali criticità. L'attività delle Autorità dovrà dunque essere diretta a bilanciare le ricadute positive che la personalizzazione dei premi e il monitoraggio degli assicurati possono portare con il rischio di assegnare polizze

[165] M. Loh, T. Soo, *Opportunities and use cases of AI in the insurance industry, in Artificial Intelligence in Finance*, Edward Elgar Publishing, 2023.

di fatto escludenti per alcuni individui a rischio, il tutto all'interno di un perimetro regolamentare e di vigilanza che ha come obiettivo primario la tutela degli assicurati[166].

La complessità data non solo dalla tecnologia in esame ma anche dall'articolato tessuto normativo, lascia dunque perplessi rispetto alla scelta di non sfruttare il solido *expertise* proprio dell'*Authority* di settore, anche per via dell'esplicita apertura offerta dal Regolamento per l'industria qui in esame. A fronte della scelta fatta dal Legislatore nazionale, si ritiene utile riflettere su soluzioni aggiuntive per rispettare gli interessi in gioco e rispettare i principi provenienti da diversi plessi normativi; il richiamo è non solo alla stipula di un protocollo di intesa fra le Autorità coinvolte, basato sulle diverse finalità perseguite, ma anche su forme di organizzazione e coordinamento più strutturate, non realizzabili in assenza di un intervento normativo.

[166] EIOPA, *Factsheet on the regulatory framework applicable to the AI systems in the insurance sector*, 15 luglio 2024, 2, disponible a <https://www.eiopa.europa.eu/document/download/b53a3b92-08cc-4079-a4f7>.

Il volume raccoglie una serie di contributi che rappresentano l'esito di un percorso comune di analisi sul ruolo delle autorità indipendenti e delle istituzioni nella regolazione dei sistemi di intelligenza artificiale, alla luce dell'AI Act europeo e della sua attuazione in Italia, con particolare attenzione alla tutela del consumatore. L'obiettivo della ricerca è verificare se l'attuale quadro normativo e istituzionale sia effettivamente idoneo a garantire la protezione dei diritti fondamentali nell'era dell'intelligenza artificiale o se si tratti, piuttosto, di un modello ancora in evoluzione, che riflette più le attese del legislatore che la realtà del mercato e delle tecnologie. Le opinioni emerse, espresse in relazione alla prima versione del testo, poi modificato nel dibattito parlamentare ma, al momento di andare in stampa, ancora non definitivo - risultano composite e differenziate nei diversi settori analizzati — dal credito ai trasporti, dall'energia alle comunicazioni — e offrono spunti per riflettere su un modello di vigilanza capace di coniugare innovazione e tutela dei diritti fondamentali.

MADDALENA RABITTI

è professore ordinario di diritto dell'economia presso l'Università di Roma Tre. Insegna diritto dei consumi e regole del mercato e diritto delle banche e delle assicurazioni. Esperta di diritto dei consumatori, sul piano della ricerca e della manualistica.

FABIO BASSAN

è professore ordinario di diritto internazionale e diritto dell'Unione Europea presso l'Università di Roma Tre. Autore di monografie e numerosi saggi, ha dedicato diverse ricerche ai temi di diritto dei consumatori e nuove tecnologie.

Roma Tre