

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 notifica¹ e la vigilanza del mercato² 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-legge 14 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 governative⁴. 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 ufficio⁵, 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 GPDP⁷ 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 formale⁸. 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 governance⁹,

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 DDL¹⁰.

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 anti-concorrenziali, 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 legislatore¹¹. 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 successivo¹².

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 scendono¹⁵.

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 regolatorio¹⁶, e le forme della regolazione partecipata¹⁷.

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 BEREC¹⁸ 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 partecipata¹⁹.

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.