D'Alfonso G, 'Piattaforme digitali e trattamenti algoritmici dei dati personali. La co-vigilanza delle Autorità di controllo di settore ' (2025) Special Issue 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLTSI252GDA

EJPLT
ISSN 2704-8012



Piattaforme digitali e trattamenti algoritmici dei dati personali. La co-vigilanza delle Autorità di controllo di settore

Digital platforms and algorithmic processing of personal data. Joint supervision by sectoral supervisory authorities

GIOVANNA D'ALFONSO
Professore associato di Diritto privato
Università degli Studi della Campania "Luigi Vanvitelli"

Abstract

L'impiego dell'intelligenza artificiale e lo sfruttamento dei dati personali degli utenti dei social networks online e delle piattaforme digitali in senso ampio si pongono in direzione biunivoca, ponendo problemi applicativi dovuti all'intersezione tra la disciplina del GDPR, del DSA e dell'AI ACT. Peraltro, sovente, le Autorità di vigilanza di settore si trovano, secondo le rispettive aree di competenza, a vigilare sul medesimo fenomeno di trattamento algoritmico dei dati personali, sollevando questioni relative al coordinamento delle loro attività.

The use of artificial intelligence and the exploitation of personal data belonging to users of social networks online and of digital platforms are moving in a biunivocal direction, posing application problems due to the intersection between the GDPR, DSA and AI ACT regulations. Moreover, sectoral supervisory authorities often find themselves, according to their respective areas of competence, supervising the same phenomenon of algorithmic processing of personal data, raising questions about the coordination of their activities.

Il saggio riproduce, con aggiornamenti normativi, la relazione dal titolo "*Trattamento automatizzato dei dati personali e vigilanza delle Autorità di controllo*", svolta al Convegno dal titolo "*Intelligenza artificiale e ambiti applicativi*", tenutasi a Capua, il 3 dicembre 2024, Università degli Studi della Campania Luigi Vanvitelli, in collaborazione con l'Universidad di Cadiz.
Questo lavoro è il risultato del *Proyecto de investigación "CONSERTECS. El contrato de prestación de servicios en el actual entorno tecnológico y social*" (PID2021 – 1226190B-I00), financiado por MCIN/AEI, con DOI 10.13039/501100011033 y por "*FEDER Una manera de hacer Europa*", di cui la professoressa María Dolores Cervilla Garzón, Catedrática de Derecho Civil, Universidad de Cádiz, è la *investigadora principal*.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Social networks online; piattaforme digitali; trattamenti algoritmici; dati personali; GDPR; Digital Service Act; AI Act; Autorità indipendenti; co-vigilanza.

Summary: 1. Social network online, trattamenti algoritmici dei dati personali. Primi spunti di riflessione. – 2. Il GDPR e l'incisivo controllo delle Autorità garanti della privacy sulle attività dei data controllers. – 3. Il Digital Services Act, il Coordinatore dei Servizi Digitali e la Commissione europea. – 4. Il ruolo dell'Autorità di vigilanza del mercato dell'intelligenza artificiale, ai sensi dell'AI Act. – 4.1. Il sistema di governance nella l. 132/2025. Raffronto con la legislazione spagnola e francese. – 5. Il GDPR, il DSA, l'AI Act e la co-vigilanza delle rispettive Autorità competenti. Rilievi conclusivi

1. Social network online, trattamenti algoritmici dei dati personali. Primi spunti di riflessione.

Negli ultimi anni, numerosi sono stati gli interventi delle Autorità garanti della *privacy* europee che hanno sollevato dubbi sulla legittimità dei trattamenti algoritmici dei dati personali[1] effettuati dai *social networks online* (per lo più, di grandi dimensioni e stabiliti al di fuori dell'Unione europea), rilevando il rischio di violazione dei principi generali fissati dal Regolamento 2016/679/UE (*GDPR*)[2].

È ben noto [3] che l'economia delle piattaforme digitali si basa sullo sfruttamento commerciale dei dati personali degli utenti del servizio che, sebbene abbiano valore minimo quando siano considerati individualmente, acquisiscono una rilevanza economica enorme, qualora siano assemblati nei *big data*[4]. I *social networks online*, nei quali vengono volontariamente condivisi

[1] Sui principi generali e sulle condizioni di liceità del trattamento dei dati personali, si v., *ex pluribus*, D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali,* in *Giur.it,* 2019/12, p. 2783 ss.; S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Persona e Mercato*, 2022/4, p. 536, il quale puntualizza l'importanza del controllo di liceità sulla funzione, in generale, del consenso al trattamento dei propri dati personali, nell'ottica di tutelare non solo l'interessato ma l'intera collettività che ha un interesse a che tali dati non siano impiegati per sfruttare le vulnerabilità delle persone. Accorta dottrina precisa che la tematica di tale consenso è tradizionalmente affrontata, insistendo principalmente sulla chiarezza e sulla consapevolezza delle informazioni a diversi livelli di utilizzo e amministrazione e che, secondo tale impostazione, è difficile avere cognizione delle diverse articolazioni che l'argomento assume in relazione a casi specifici o alla tipologia dei "dati" trattati. Si v. AA.VV., *Privacy and Consent. A Legal and UX&HMI Approach*, a cura di L. GATT, R. MONTANARI, I.A. CAGGIANO, Napoli, 2021.

[2] Tra i commenti al regolamento, *ex multis*, si v. F. PIZZETTI, *Il regolamento europeo 2016/679,* Torino, 2016; AA.VV., *Regolare le tecnologie: il Reg. UE 2016/679 e la protezione dei dati personali,* a cura di A. MANTELERO e D. POLETTI, Pisa, 2018; AA.VV., *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019; AA.VV., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, Bologna, 2021. Prestigiosa dottrina ha rimarcato che l'evoluzione tecnologica e la diffusione di contenuti digitali *online* costituiscono elementi di un mutamento considerevole per la tutela della persona e del mercato. A fronte della riduzione della sfera privata degli individui che diviene sempre più fragile, poiché, in ogni momento, enormi quantità dei loro dati personali sono raccolti e trattati, anche a loro insaputa, il *GDPR* assume un ruolo fondamentale, introducendo innovazioni significative rispetto alla normativa previgente statuita dalla «direttiva-madre». P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018/1, p. 481.

[3] Per le osservazioni che seguono si v. A. GENTILI, *Introduzione al diritto delle piattaforme*, in *EJPLT*, 2025/ 1, p. 2 s., consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/index.

[4] Nell'ambito del procedimento di elaborazione algoritmica, incidono in modo decisivo il volume, la variabilità e la velocità dei dati convertiti in numeri e la loro idoneità ad essere notevolmente collegati. Si v.

contenuti che includono inevitabilmente informazioni personali[5], impiegano algoritmi che provvedono alla profilazione degli utenti, per, poi, vendere, per finalità di *marketing*, le loro preferenze agli inserzionisti pubblicitari, affinché questi ultimi possano svolgere una pubblicità accuratamente personalizzata. L'elemento imprescindibile di tale operazione economica è rappresentato dalla cessione dei propri dati personali da parte degli utenti alle reti sociali *on line*, in cambio del servizio loro offerto.

Tra le piattaforme digitali e i loro utenti intercorre un rapporto contrattuale, come enunciato dall'art. 3, lett. u), Regolamento 2022/2065/UE, *Digital Services Act* (c.d. *DSA*)[6]: le stesse predispongono unilateralmente dei regolamenti a circolazione planetaria che dettano, in maniera standardizzata, le condizioni di accesso e i termini di utilizzo da parte degli utenti e la disciplina del rapporto con questi ultimi[7].

Sulla qualificazione della fattispecie contrattuale si condivide l'efficace ricostruzione di arguta dottrina che ha affrontato la questione anzitempo, con riferimento puntuale ai *social networks*, secondo la quale trattasi di un contratto atipico di scambio a titolo oneroso, in forza del quale gli utenti del servizio offerto dalla piattaforma digitale, manifestando la propria adesione alle condizioni generali d'uso, concedono alla controparte una licenza di proprietà intellettuale non esclusiva, trasferibile e ulteriormente cedibile a terzi come sotto-licenza, libera da *royalty* e valida in tutto il mondo, avente ad oggetto l'impiego di qualsiasi contenuto (dati personali, commenti, immagini, etc.) pubblicato sulla piattaforma o in connessione con essa, a fronte della licenza personale, mondiale, *royalty-free*, non cedibile e non esclusiva che il gestore concede agli utenti stessi per utilizzare il *software* fornito dal *social network*[8]. Più esattamente, in cambio del diritto di accesso allo stesso, l'utente autorizza il gestore a usare il proprio nome, l'immagine del profilo e tutte le informazioni relative alle azioni compiute sulla piattaforma per finalità di profilazione commerciale[9], rinunciando alla pretesa di un'eventuale remunerazione[10]. La configurabilità del contratto quale contratto di scambio è confermata dal collegamento con i contratti conclusi dal *social network* con gli inserzionisti pubblicitari, per valutare gli effetti finali sull'unitaria e complessa operazione economica.

P. PERLINGIERI, *Relazione conclusiva*, in AA.VV., *Internet e diritto civile*, a cura di C. PERLINGIERI, L. RUGGERI, Napoli, 2018, p. 419. In relazione al fenomeno dei *big data*, si v. A. NAZZARO, *Privacy e big data*, in *Corti fiorentine*, 2018, p. 13 ss.

[5] I «*social network on line*» sono definibili, ai sensi dell'art. 2, n. 7 del Regolamento 2022/1925/UE, c.d. *Digital Markets Act*, quali piattaforme digitali che offrono agli utenti, su loro richiesta, il servizio che consente di creare e gestire un profilo, sia pubblico che semipubblico, in un ambiente circoscritto, oltre che di entrare in contatto, comunicare, condividere contenuti con altri utenti, in particolare, attraverso *chat*, post, video e raccomandazioni.

[6] La disposizione dichiara che sono «condizioni generali» tutte le clausole, in un qualunque modo denominate e indipendentemente dalla loro forma, che regolamentano il rapporto "contrattuale" tra il prestatore dei servizi intermediari e il destinatario del servizio.

[7] G. BUTTARELLI, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, *in Giornale dir. ammin.*, 2023/ 1, p. 118.

[8] C. PERLINGIERI, *Profili civilistici dei social networks*, Napoli, 2014, pp. 88-92.

[9] F. MANOLITA, *Il grande gioco. Buon costume e buon costume stipulativo alla prova dei social network*, in *Teoria e prassi del diritto*, 2022/2, p. 563 s.

[10] Sul punto e per la considerazione che segue si v. C. PERLINGIERI, *op.ult. cit.*, p. 90, s.

In linea con tale impostazione, taluni ha parlato di «contratto di scambio di "servizi contro dati"»[11], sottolineando che, seppure i rapporti oggetto di attenzione possano sembrare apparentemente gratuiti[12], laddove gli utenti forniscono i propri dati personali in cambio dei servizi loro offerti, invece di versare un prezzo, tali dati rappresentano, in realtà, il "corrispettivo" dell'accesso al servizio e il consenso al loro trattamento può essere configurato quale controprestazione del contratto.

La natura contrattuale dei rapporti in esame e la causa di scambio sono ampiamente riconosciute dalla dottrina[13] e dalla giurisprudenza di merito[14] e, da ultimo, confermate da un'importante pronuncia della Corte di Giustizia UE, riunita nella Grande Sezione, 4.7. 2023, caso C-252/21 (condizioni generali d'uso di un *social network*)[15].

La Corte di Giustizia dell'Unione Europea si è pronunciata sul rinvio pregiudiziale presentato nell'ambito di una controversia tra *Meta Platforms Inc.* e il *Bundeskartellamt* (Autorità federale garante della concorrenza tedesca), in riferimento alla decisione di quest'ultimo di porre il divieto alla società statunitense di far assoggettare, tramite le condizioni generali di contratto, l'utilizzo di *Facebook* da parte di utenti privati residenti in Germania al trattamento dei loro dati personali per finalità di pubblicità personalizzata, procedendo a tali operazioni senza il loro consenso[16]. L'Autorità di controllo ha, altresì, posto in evidenza che un siffatto consenso non sarebbe comunque valido, perché rappresenterebbe uno sfruttamento abusivo della posizione

---

[11] Per le riflessioni che seguono, si v. V. BACHELET, *Il «contratto di scambio di "servizi contro dati" (o contro prezzo)»*, in *Riv.dir.civ.*, 2024, pp. 1130- 1132, 1139 s. Sul tema P. GALLO, *Il consenso di trattamento dei dati personali come prestazione*, *ivi*, 2022, p. 1054 ss. Per una ricostruzione innovativa delle molteplici declinazioni del contratto di prestazione di servizi nel nuovo contesto sociale e tecnologico, si v. AA.VV., *El actual contrato de prestación de servicios*, a cura di M. D. CERVILLA GARZÓN, I. ZURITA MARTÍN, Aranzadi, Navarra, 2023; AA.VV., *Nuevos tiempos, nuevos servicios*, a cura di M. D. CERVILLA GARZÓN, I. ZURITA MARTÍN, Atelier Libros Jurídicos, Barcellona, 2025.

[12] Discorre di forniture contrattuali «a titolo, o meglio a struttura gratuita» C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust.civ.*, 2019, p. 507. In precedenza, si era espresso a favore della gratuità (interessata), sia pure in maniera dubitativa, R. CATERINA, *Cyberspazio, social network e teoria generale del contratto,* in *Ann. it. dir. aut.*, 2011, p. 96.

[13] Si v., *ex multis*, A. METZGER, *Dienst gegen Daten: Ein Synallagmatischer Vertrag*, in *Archiv für die civilistische Praxis*, 2016, p. 834; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 68, il quale evidenzia che il consenso degli utenti al trattamento dei dati personali soddisfa il requisito di patrimonialità della prestazione previsto dall'art. 1174 c.c.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv.trim.dir. e proc.civ.*, 2018, p. 418; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, p. 75 ss.

[14] Trib. Bologna, 10. 3. 2021, n. 5206, in *Tecnologie e Diritto*, 2021, p. 123 ss., con nota di V. CONTE, *Recesso ad nutum nei social media, corrispettività e rilevanza della buona fede posteriore all'adempimento*, p. 133; Trib. Trieste, ord. 27. 11. 2020, n. 2032, in *Giur.it.*, 2021, p. 2090, con nota di S. MARTINELLI, *La chiusura dell'account Facebook di un'associazione: quale tutela?*, Trib. Roma, 12. 12. 2019, in *Danno e resp.*, 2020, p. 488, con nota di A. QUARTA, *Disattivazione della pagina Facebook. Il caso CasaPound tra diritto dei contratti e bilanciamento di diritti.*

[15] La sentenza è consultabile al sito https://curia.europa.eu. Per un commento si v. V. BACHELET, *La Corte di giustizia sul caso Meta: trattamento dei dati e "prezzo" del consenso*, in *Pactum*, 2023, p. 483 ss.; I. GRAEF, *Meta Platforms: How the CJEU leaves competition and data protection authorities with an assignment*, in *MJECL*, 2023, p. 325 ss.; P. G. PICHT, *CJEU on Facebook: GDPR Processing Justifications and Application Competence*, in *Gewerblicher Rechtsschutz und Urheberrecht*, 2023/16, p. 1169 ss.

[16] Per le notazioni relative alle questioni pregiudiziali sulle quali si è pronunciata la Corte di Giustizia UE, si v. C. A. TROVATO, *La sentenza CGUE del 4.7.2023 nel caso C252/21 sui rapporti tra privacy e antitrust, sulla pubblicità dei dati sensibili e sulla inadeguatezza della base del legittimo interesse per il trattamento dei dati inerenti la pubblicità comportamentale di Meta (sentenza Meta abuso di posizione dominante)*, in *Persona e mercato,* 2023/3, pp. 593- 595.

dominante di *Meta* sul mercato tedesco. *Meta* ha presentato un ricorso dinanzi all'*Oberlandesgericht* di Düsseldorf, sollevando talune questioni, tra le quali l'interpretazione e l'applicazione di alcune disposizioni del *GDPR*. La Corte d'Appello tedesca ha adito la Corte di Giustizia UE in via pregiudiziale, rinviando alcuni quesiti, tra i quali: se Meta possa usare le basi giuridiche del contratto (articolo 6, par. 1, lett. b) *GDPR*) o del legittimo interesse (articolo 6, par. 1, lett. f) *GDPR*), dell'obbligo di legge (articolo 6, par. 1, lett. c) *GDPR*) e della salvaguardia di un interesse vitale o pubblico (articolo 6, par. 1, lett. d) ed e) *GDPR*), al fine di compiere pubblicità mirata sui propri utenti; se, una volta accertato l'abuso di posizione dominante di un'impresa, possa considerarsi valido e, in special modo, 'libero' il consenso al trattamento dei propri dati personali espresso da un utente nei confronti di tale titolare.

I giudici di Lussemburgo hanno interpretato restrittivamente l'art. 6 *GDPR*, escludendo che i *social networks* possano trattare i dati personali degli utenti su basi giuridiche differenti dal consenso, con l'obiettivo di profilarli e offrire loro servizi "gratuiti", finanziati, in sostanza, dalla pubblicità individualizzata. La Corte di Giustizia UE ha, finanche, chiarito che gli utenti devono poter essere liberi di rifiutare individualmente, nell'ambito della procedura contrattuale, la prestazione del proprio consenso a operazioni peculiari di trattamento di dati che non siano necessarie all'esecuzione del contratto, senza dover, perciò, rinunciare del tutto alla fruizione del servizio offerto dal *social network online*; per, poi, imporre alle piattaforme con una posizione 'dominante' nel mercato digitale, quali *Meta* e Instagram, di proporre a tali soggetti di scegliere di accedere al servizio senza profilazione, né pubblicità mirata, in cambio, eventualmente, del pagamento di un corrispettivo ragionevole[17].

È, così, accaduto che, a seguito della decisione vincolante e urgente dell'*European Data Protection Board*, *Meta*, per ottemperare all'ordine dell'Autorità garante della *privacy* irlandese di fondare la profilazione degli utenti sul consenso, ha cambiato il modello di *business* fino a quel momento impostato, offrendo a questi ultimi la scelta di rifiutare il trattamento dei dati personali, pagando un corrispettivo mensile di Euro 12.99 per Facebook o Instagram (Euro 20.99 per entrambi i servizi)[18].

In tal caso, le parti contraenti stipuleranno un contratto di "servizi contro prezzo" e la circostanza che il pagamento di un prezzo da parte degli utenti rappresenti, per le piattaforme digitali, un'alternativa al consenso al trattamento dei dati personali avvalora il convincimento che quest'ultimo rappresenta una modalità di pagamento e che sia configurabile come controprestazione del contratto "servizi contro dati"[19].

Ciò detto, si osservi che, finora, un ruolo preminente nella vigilanza sul trattamento algoritmico dei dati personali effettuato dai *social networks on line* è stato ricoperto dalle Autorità garanti della *privacy* che, nell'esercizio dei

[17] Si v. § 150.

[18] Si fa riferimento alla Decisione vincolante d'urgenza dell'*EDPB*, 27. 10. 2023, 01/2023, richiesta dall'Autorità di controllo norvegese per l'adozione di misure definitive nei confronti di *Meta Platforms Ireland Ltd* (articolo 66, par. 2, *GDPR*), consultabile sul sito https://www.edpb.europa.eu. Con tale decisione, l'*EDPB* ha ritenuto indispensabile incaricare l'Autorità irlandese per la protezione dei dati (IE DPA) di imporre un divieto di trattamento dei dati personali, a livello di EEA, rivolto a *Meta Ireland Limited* (Meta IE).

[19] Sul punto si v. V. BACHELET, *Il «contratto di scambio di "servizi contro dati" (o contro prezzo)»*, *cit.*, p. 1131. s.

propri poteri di indagine, *ex* art. 58, par. 1[20] e/o correttivi, *ex* art. 58, par. 2[21], *GDPR*, finiscono con l'indirizzare le attività e le condotte dei soggetti controllati [22] . Molti provvedimenti delle Autorità hanno, infatti, inciso significativamente sullo svolgimento delle attività delle piattaforme digitali di grandi dimensioni, ingiungendo l'adozione di determinati comportamenti, al fine di conformare i trattamenti dei dati personali alle norme del *GDPR*, con la conseguenza che tali società hanno dovuto modificare le proprie *policies* e, quindi, talvolta (come visto con quanto accaduto con *Meta*), anche le condizioni generali di contratto[23].

[20] La norma elenca penetranti poteri di indagine, quali il potere di: ingiungere al titolare e/o al responsabile del trattamento (e, ove applicabile, al rappresentante del titolare e/o del responsabile del trattamento) di fornire ogni informazione di cui le Autorità necessitino per l'esecuzione dei propri compiti; condurre indagini sotto forma di attività di revisione sulla protezione dei dati; effettuare un riesame delle certificazioni rilasciate, ai sensi dell'art. 42, par. 7; notificare al titolare e/o al responsabile del trattamento le presunte violazioni del regolamento; ottenere, da tali soggetti, l'accesso a tutti i dati personali e a tutte le informazioni indispensabili per lo svolgimento dei propri compiti; conseguire l'accessibilità a tutti i locali di tali soggetti, compresi tutti gli strumenti e i mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri. Si v. L. CALIFANO, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in *Federalismi.it*, 2. 6. 2020, p. 9, s., consultabile al sito https://www.federalismi.it/nv14/articolo-documento.cfm?artid=44514

[21] La previsione si sofferma su tutta una serie di poteri, espressione di un'attenta e severa potestà autoritativa nei confronti dei titolari e/o responsabili dei trattamenti: la definizione "poteri correttivi" fa ben comprendere come essi siano preordinati a porre fine alle infrazioni del *GDPR* e a ripristinare la correttezza dei trattamenti. Seguendo una "gerarchia di gravità" degli interventi attivabili, si parte dagli avvertimenti e ammonimenti al titolare e/o responsabile del trattamento e dagli ordini impartiti nei loro confronti per il rispetto dei diritti degli interessati o per la comunicazione a questi ultimi di *data breach*. Si sale, di seguito, di grado fino all'ingiunzione di uniformare il trattamento dei dati personali alle regole del *GDPR* oppure di limitarlo, in via provvisoria o definitiva, o vietarlo, per concludere con l'inflizione di una sanzione amministrativa pecuniaria, ai sensi dell'art. 83 *GDPR*. Vi sono, poi, ordini in materia di certificazione o di sospensione di flussi di dati al di fuori dell'Unione europea, che attengono ad ambiti specifici. Infine, il terzo raggruppamento di poteri dell'Autorità di controllo è riunito nell'ambito dei poteri autorizzativi e consultivi. Si tratta, inevitabilmente, di funzioni che sono strettamente connesse alle competenze e ai poteri già esaminati e che spaziano dalla consulenza al titolare del trattamento a funzioni tipiche dell'Autorità, alla quale è demandato il compito di definire i poteri e i limiti anche in merito alle autorizzazioni, dalle quali dipende l'intera attività di trattamento dei dati personali. L. CALIFANO, *op. loc.ult.cit.*

[22] Si v. C. SOLINAS, *Le funzioni delle Autorità indipendenti nel trattamento algoritmico dei dati*, in AA.VV., *Intelligenza artificiale e piattaforme digitali: dalla co-regolamentazione alla co-vigilanza. Atti del Convegno 10-11 febbraio 2025. Università degli Studi di Perugia*, a cura di M. ANGELONE, C. COLOMBO, I. MARTONE, C. PERLINGIERI, A. VALONGO, Napoli, 2025, p. 261, la quale osserva che le Autorità di vigilanza o garanzia possono indirizzare le attività e i comportamenti dei soggetti vigilati, anche senza il bisogno di ricorrere, a tal fine, allo strumento regolatorio formale.

[23] A titolo esemplificativo, si riportino taluni interventi delle Autorità di controllo di grande interesse. Il 21 giugno 2024, *Meta* ha deciso di non lanciare i suoi modelli di intelligenza artificiale nel mercato europeo, a seguito della richiesta dell'Autorità irlandese per la *privacy* di rinviare il piano di utilizzo dei dati degli utenti di Facebook e Instagram. La decisione di *Meta* è stata presa successivamente alla presentazione di denunce e richieste da parte del gruppo di difesa NOYB, organizzazione *no-profit* per i diritti digitali con sede a Vienna, alle Autorità di protezione dei dati in vari Stati europei, tra i quali l'Austria, il Belgio, la Francia, la Germania, la Grecia, l'Italia, l'Irlanda, i Paesi Bassi, la Norvegia, la Polonia e la Spagna. NOYB ha deciso di procedere legalmente contro la società, sollevando il problema nodale che, benché *Meta* avesse dichiarato che avrebbe usato soltanto informazioni pubblicamente disponibili e autorizzate, il piano della società di utilizzare i dati personali per addestrare i suoi modelli *AI* sarebbe avvenuto senza ottenere il consenso degli utenti. L'Autorità irlandese ha, dunque, richiesto alla società di ritardare l'addestramento dei suoi modelli linguistici di grandi dimensioni (LLM) con i contenuti pubblici condivisi dagli utenti adulti di Facebook e Instagram. La notizia è consultabile *online*: https://www.dimt.it/news, 21 giugno 2024. La stessa Autorità irlandese, in data 24 ottobre 2024, ha comunicato di aver concluso l'indagine su *Linkedin*, dopo aver riscontrato numerose violazioni del *GDPR*, che hanno condotto ad una triplice sanzione, per un valore totale di 310 milioni di euro. La società ha compiuto attività di pubblicità mirata e di analisi comportamentale che rappresentano una prassi di *marketing* sempre più frequente nell'ambito dei servizi digitali. Il fenomeno solleva conflitti con i principi del regolamento generale sulla *privacy*, quali i principi di lealtà, correttezza e trasparenza del trattamento, di cui all'art. 5, par. 1, lett a). Per un commento, si v. L. BAUDINO BESSONE, *L'analisi*

Deve, però, considerarsi che, con l'entrata in vigore del *Digital Services Act*[24], c.d. *DSA* e del Regolamento 2024/269/UE sull'intelligenza artificiale, c.d. *AI Act*[25], è aumentato il numero delle Autorità tenute ad intervenire, in vario modo e con finalità diverse, sul medesimo fenomeno del trattamento algoritmico dei dati personali degli utenti eseguito dalle piattaforme digitali.

Il *Digital Services Act*, nel modernizzare la direttiva 2000/31/CE, c.d. direttiva *e-commerce*, ha avuto l'obiettivo di tutelare la spazio digitale dalla diffusione di beni, contenuti e servizi illegali e di garantire la protezione dei diritti fondamentali degli utenti dei servizi offerti dagli *internet service providers*[26] .

L'*AI Act* stabilisce regole armonizzate sull'immissione sul mercato, sulla messa in servizio e sull'uso dei sistemi di intelligenza artificiale, definiti dall'art. 3, n. 1. Come enunciato nell'art. 1, esso si pone la finalità di migliorare il funzionamento del mercato interno e di promuovere la diffusione di un'intelligenza artificiale 'antropocentrica' e 'affidabile', garantendo, contemporaneamente, un livello elevato di tutela della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali UE, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi intelligenti nell'Unione Europea, oltre che di promuovere l'innovazione tecnologica[27].

Le due regolamentazioni sono settoriali, ma si caratterizzano per la loro trasversalità[28], presentando numerosi punti di contatto con il *GDPR* e tra di loro, perché il legislatore europeo, nel dettarle, ha tenuto conto della circostanza che il *business* delle piattaforme digitali si fonda sulla raccolta e sullo sfruttamento dei dati personali degli utenti del servizio e che l'impiego dell'intelligenza artificiale, che si nutre dei dati stessi, ne costituisce il presupposto ed il fondamento[29]. Cosicché, una vicenda specifica di trattamento

---

comportamentale e il target advertising violano il GDPR e costano caro a LinkedIn, in *Rivista diritto di internet*, 7. 11. 2024.

[24] Il Regolamento è entrato in vigore il 16 novembre 2022 ed è applicato, dagli Stati membri, dal 17 febbraio 2024.

[25] L'*AI Act* è entrato in vigore il 2 agosto 2024 e dovrà essere applicato dal 2 agosto 2026, per dare il tempo alle aziende di adattarsi alla disciplina, salvo per quanto riguarda: i divieti di sistemi a rischio inaccettabile che sono già rispettati, a partire dal 2 febbraio 2025; i codici di buone pratiche, applicati dal 2 maggio 2025 e le norme sui sistemi di intelligenza artificiale per finalità generali, compresa la *governance*, applicate dal 2 agosto 2025. Sulla possibile proroga di termini, si v. *infra* le notazioni relative al "*Digital omnibus"*, pacchetto di proposte normative presentate dalla Commissione europea il 19 novembre 2025.

[26] Il *DSA* compone il *Digital Services Package*, insieme al *Digital Markets Act*, che prescrive una serie di doveri e divieti per arginare gli abusi degli operatori dominanti, con la finalità di dare vita a un mercato più competitivo, dove possano prosperare perfino i *players* più piccoli. Il pacchetto di misure è un intervento normativo che si inserisce nella cornice del programma strategico dell'Unione europea per la trasformazione digitale e che punta alla creazione di un ambiente digitale sicuro e competitivo che integri un solido scudo sia per la protezione dei diritti fondamentali degli utenti della rete e dei cittadini nello spazio digitale europeo, sia per il contrasto di comportamenti anticoncorrenziali delle piattaforme digitali che abbiano un impatto significativo sul mercato interno (i cc.dd. *gatekeepers*), per renderlo equo e contendibile. Si v. B. SAAVEDRA SERVIDA, *La responsabilità degli Internet Service Providers: dal Safe Harbour al principio di accountability*, in *Leggi civ. comm.*, 2024, p. 135 s.

[27] La letteratura giuridica di commento del provvedimento è già ampia. Tra i numerosi contributi, si v. G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; AA.VV, *Diritto e intelligenza artificiale, Vol. 1 e Vol. 2*, a cura di U. RUFFOLO, A. AMIDEI, Luiss, Roma, 2024; tra i più recenti commenti, si v. AA.VV., *La disciplina dell'intelligenza artificiale*, a cura di F. DONATI, G. FINOCCHIARO, F. PAOLUCCI, O. POLLICINO, Torino, 2025.

[28] C. SOLINAS, *op.cit.*, p. 257.

[29] C. PERLINGIERI, *Intelligenza artificiale tra principi e regole*, in *AI Law - International Review of Artificial Intelligence Law*, 2025, 1, p. 38, consultabile sul sito https://www.reviewofailaw.com/Article/Archive/index_html?ida=3&idn=4&idi=-1&idu=-1. Nelle proprie

algoritmico di dati personali può interessare diverse materie e questioni, tra le quali, quella dei dati, dell'intelligenza artificiale e dei servizi offerti dalle piattaforme digitali. La trasversalità, intrinseca a questi fenomeni, è, ovviamente, connaturata anche alle funzioni delle Autorità di controllo di settore[30].

Potrebbe, così, accadere che i gestori dei *social networks*, nel violare contemporaneamente il *GDPR* e/o il *DSA* e/o l'*AI Act*, siano sottoposti, *rationae materiae,* alla vigilanza delle Autorità di competenza dei diversi settori. A titolo esplicativo, in riferimento al caso Linkedin menzionato, l'utilizzo non conforme delle tecniche di *marketing* potrebbe avere un impatto negativo non solo alla luce del *GDPR*, ma anche del *Digital Services Act*[31] e, pertanto, determinare l'attivazione sia dell'Autorità di controllo della protezione dei dati personali, sia del Coordinatore dei servizi digitali, responsabile di tutte le questioni relative alla vigilanza e all'applicazione del *DSA* all'interno degli Stati membri[32].

In effetti, si assiste ad un radicale ridimensionamento della tenuta del modello di vigilanza indipendente settoriale, a causa del coinvolgimento sempre maggiore di più Autorità tenute ad occuparsi del medesimo fenomeno, in modo diverso e con obiettivi differenti, con la conseguenza che tale evoluzione può condurre a significative complessità dal punto di vista operativo, potendosi verificare rischi di sovrapposizioni di competenze e finalità delle varie Autorità[33].

In più, sussiste il pericolo di disaccordo tra le stesse, nella visione dei problemi sottostanti alle vicende sulle quali debbano decidere[34]. Al riguardo, si rammenti la questione della patrimonializzazione dei dati personali -che ha condotto alla pronuncia della Corte di Giustizia UE, cit., nel caso sulle condizioni generali d'uso di *Meta Platforms Inc.*-, in relazione alla quale si sono contrapposti il punto di vista delle Autorità *Antitrust* nazionali ed europee, propense ad una valutazione in senso economico del trattamento dei dati personali e quello delle Autorità garanti della *privacy*, diffidenti sulla possibilità di prospettare la circolazione degli stessi con le categorie dello scambio.

Ordunque, le riflessioni svolte inducono a porsi due interrogativi.

Come cambia il ruolo delle Autorità di controllo della *privacy*, a dispetto dell'esplicarsi dei compiti delle Autorità di vigilanza sull'osservanza del *DSA* e del Regolamento sull'intelligenza artificiale designate dagli Stati membri, tenendo conto del peculiare sistema di *governance* predisposto dal legislatore europeo?

---

campagne di *marketing*, le società utilizzano, ormai, *dataset* che, per la loro estensione in volume, velocità e varietà, tramite l'utilizzo degli algoritmi, permettono di estrarre informazioni aggiuntive, di elaborare risultati con elevato grado di certezza, tali da determinare modelli di *business* e mercati. Si v. I. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in *Annali- Università degli Studi Suor Orsola Benincasa*, 2018, p. 10.

[30] C. SOLINAS, *op.loc.ult.cit.*

[31] L. BAUDINO BESSONE, *op.loc.ult.cit.*

[32] In Italia, l'Autorità per le garanzie nelle comunicazioni, c.d. AGCOM, è stata designata quale Coordinatore dei Servizi Digitali, ai sensi dell'49, par. 1, *DSA*, dall'articolo 15, d. lg. 15.9. 2023, n. 123 (recante «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale»), convertito con modificazioni dalla l. 13.11. 2023, n. 159.

[33] C. SOLINAS, *op.cit.*, p. 249.

[34] Per le argomentazioni che seguono, si v. V. RICCIUTO, *AI Act, diritto dell'Unione e diritto nazionale*, in AA.VV., *Intelligenza artificiale e piattaforme digitali: dalla co-regolamentazione alla co-vigilanza*, a cura di M. ANGELONE, C. COLOMBO, I. MARTONE, C. PERLINGIERI, A. VALONGO*, cit.*, p. 97.

Come si coordina l'operato di tali Autorità, quando si trovino a decidere su questioni che comportino confluenze tra i differenti ambiti e che richiederebbero l'intervento di ciascuna di essa?

2. Il GDPR e l'incisivo controllo delle Autorità garanti della privacy sulle attività dei data controllers.

Per rispondere ai quesiti posti, *in primis*, è indispensabile puntualizzare che il legislatore europeo, in linea con quanto previsto dall'art. 16 del Trattato di funzionamento dell'UE[35], ha voluto rafforzare il ruolo di vigilanza delle Autorità di controllo della protezione dei dati personali rispetto a quello tratteggiato dalla «direttiva-madre»[36], sia ponendo, quale primo compito, quello della sorveglianza (art. 58, par. 1, lett. a), sia attribuendo loro considerevoli poteri di correzione (art. 58, par. 2), delineando, in tal guisa, un ruolo di garanzia, anzitutto, in relazione alla rispondenza dei trattamenti al Regolamento.

A ben riflettere, la ridefinizione del ruolo delle Autorità rappresenta il naturale "contrappeso" alla scelta del *GDPR* di accentuare il profilo di autoresponsabilità dei titolari del trattamento dei dati personali[37].

Invero, il legislatore europeo ha dovuto far fronte alla trasformazione radicale del contesto tecnologico, dovuto ai nuovi sviluppi delle tecnologie dell'informazione e della comunicazione (considerando 6) e che, conducendo all'interconnessione sempre più massiva e veloce dei dati personali, aumenta, in maniera esponenziale, il rischio di un loro trattamento sempre più invasivo nella sfera dell'individuo. Tutto ciò ha reso la disciplina previgente obsoleta e

[35] La norma ha conferito al legislatore europeo l'incarico di definire un nuovo quadro normativo comune all'Unione Europea, nel quale il ruolo di vigilanza del rispetto del *GDPR* sia svolto da «autorità indipendenti».

[36] Il passaggio dalla direttiva 95/46/CE che, per anni, ha rappresentato la «pietra angolare» della normativa dell'Unione Europea in materia di protezione dei dati personali, al *GDPR*, che l'ha abrogata e sostituita, ha decretato il profondo mutamento delle funzioni riconosciute alle Autorità di controllo degli Stati membri dell'Unione europea, in relazione a molteplici profili. Per un commento alla legge italiana di recepimento della «direttiva-madre» - l. 31. 12.1996, n. 675, entrata in vigore l'8 maggio 1997, c.d. legge sulla *privacy*, la cui regolamentazione è, successivamente, confluita nel Codice in materia di protezione dei dati personali, emanato con d.lg. 30. 6. 2003, n.196, ancora oggi in vigore, ancorché profondamente modificato per adeguarlo al *GDPR*- si v. AA.VV., *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 (codice della privacy),* a cura di C.M. BIANCA, F.D. BUSNELLI Padova, 2007. Il Maestro C. M. Bianca, tra i primi, colse la differenza concettuale e contenutistica tra il diritto alla riservatezza, inteso quale «diritto della persona a non vedere esposti alla pubblica curiosità dati e vicende della propria vita intima» e il diritto alla protezione dei dati personali, da intendersi quale diritto della persona alla non ingerenza di terzi nei propri dati personali, illustrando come l'evoluzione della regolamentazione abbia condotto alla qualificazione di quest'ultimo quale autonomo diritto della personalità, distinto dal tradizionale del diritto alla riservatezza e, quindi, dotato di «un proprio contenuto e una propria disciplina» e, per questa ragione, «sanzionat[o] a prescindere dall'accertamento della violazione di altri diritti». L'eminente dottrina dichiarava che un momento importante di questo cambiamento di prospettiva è stato contrassegnato, primariamente, dalla Convenzione di Strasburgo 28.1.1981, n. 108, ratificata, in Italia, dalla l. 21. 2. 1989, n. 98- che aveva enunciato il principio della protezione dei diritti e delle libertà fondamentali della persona e, precipuamente, del diritto al rispetto della vita privata a fronte del trattamento automatizzato dei dati personali-, *in secundis* dalla direttiva 95/46/CE e, in seguito, dalla Carta dei diritti fondamentali dell'Unione europea proclamata il 7.12.2000 – e vincolante dal 2009 con il Trattato di Lisbona (art. 6 TUE)- che ha previsto il diritto di ogni individuo «al rispetto della propria vita privata e familiare» e ha proclamato, con un'enunciazione separata, all'art. 8, il diritto di ogni individuo «alla protezione dei propri dati personali». Si v. C.M. BIANCA, *Note introduttive*, *ivi*, p. XIX, ss.

[37] L. CALIFANO, *op.cit.,* pp. 7, 11.

inidonea, in quanto caratterizzata da una struttura rigida e da un'idea sostanzialmente statica della protezione dei dati personali[38].

Il regolamento ha, per tale ragione, cambiato la tecnica legislativa, passando da regole molto dettagliate ad una concezione normativa "dinamica e flessibile" [39], fondata su principi e mirante alla "responsabilizzazione" del titolare del trattamento[40].

Ne discende che il ruolo di quest'ultimo è stato ridisegnato e che la regolamentazione della sua attività è permeata dal principio generale di *accountability*, enunciato nell'art. 24, ove la locuzione è stata, si ritiene impropriamente, resa nella versione italiana del regolamento con il termine "responsabilità"[41]. Tra le molte norme del Regolamento che sono espressione di tale principio, questa è forse la principale[42]. Essa statuisce che il titolare del trattamento, «tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche», è tenuto a mettere in atto misure tecniche ed organizzative "idonee" ad assicurare un livello di sicurezza confacente al rischio, come pure a dare attuazione ai principi e alle norme del regolamento. La decisione sull'appropriatezza delle risoluzioni da adottare è, in tal guisa, rimessa alla "discrezionalità" del titolare del trattamento che non sarà, però, illimitata, dal momento che dovrà essere necessariamente parametrata alle condizioni descritte.

Costui, oltre a valutare e scegliere le misure di sicurezza, fin dalla fase della loro progettazione e lungo tutto il periodo del loro svolgimento, affinché siano conformi al livello di rischio che comportano, dovrà compiere un'attività di continuo monitoraggio, anche attraverso l'elaborazione di modelli organizzativi precisi, con l'obiettivo di fornire la migliore protezione ai dati personali trattati. Parimenti, dovrà essere in grado di dimostrare tutto, provando la congruenza delle scelte di regolamentazione compiute in modo autonomo[43].

Tale metodo determina un adattamento costante del modello di gestione del rischio e si basa, certamente, sul convincimento che il titolare del

---

[38] Le tecnologie attuali consentono agli operatori economici di impiegare volumi enormi di dati personali, con modalità e finalità che un ventennio fa non erano neppure immaginabili. E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr.impr.*, 2018, p. 108, s.; G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in AA.VV., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, *cit.*, p. 13 s.

[39] F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni,* in *Media Laws. Rivista di diritto dei media*, 8. 2. 2018, p. 114, consultabile sul sito https://www.medialaws.eu/rivista/

[40] R. CATERINA, *Novità e continuità nel Regolamento generale della protezione dati*, in AA.VV., *GDPR tra novità e discontinuità*, a cura di R. CATERINA, *cit.*, p. 2777. Sul tema, si v. anche C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, Napoli, 2018, p. 89.

[41] Tale principio deve essere inteso nel senso della "responsabilizzazione" dei titolari e responsabili del trattamento, in una prospettiva dinamica. Si v. L. CALIFANO, *op.cit.*, p. 5 s.

[42] Sul punto e per le osservazioni che seguono, si v. R. CARLEO, *Il principio di accountability nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo diritto civile*, 2021, p. 357.

[43] Ponendo l'accento su tale aspetto, accreditata dottrina afferma che la locuzione "*accountability*" deve essere collocata a metà strada tra la responsabilità e la *compliance* e che la si può intendere come «garanzia della conformità» delle attività svolte alla disciplina di settore, che il titolare del trattamento dev'essere in grado di provare in qualunque momento. Si v. E. LUCCHINI GUASTALLA, *op.cit.*, p. 120 ss.

trattamento sia il soggetto nella posizione migliore per gestirlo e valutarlo[44]. Evidentemente, il legislatore europeo ha avuto di mira l'obiettivo di prevenire eventuali violazioni da parte dei titolari del trattamento, adottando un *risk based approach,* attraverso una serie di previsioni che sono finalizzate a diminuire, *ex ante*, i rischi di trattamenti non conformi al *GDPR* e cercando, per converso, di circoscrivere l'attivazione di strumenti di tutela *ex post*, quando il danno in capo al soggetto interessato si sia già realizzato[45].

Può, così, dedursi che la strada individuata dal *GDPR* è di assegnare centralità alla figura del titolare del trattamento[46], aumentando il suo potere decisionale nelle scelte tecniche e organizzative da implementare e accrescendone, in tale modo, al contempo, la responsabilità nei confronti dell'Autorità di controllo e degli interessati[47].

In questa prospettiva, a fare da «contraltare» alla maggiore discrezionalità dei titolari del trattamento, dovuta alla loro "responsabilizzazione", si è riconosciuta una presenza più forte alle Autorità di vigilanza[48], accordando loro un ruolo «strutturalmente dinamico», e non più statico, giacché l'oggetto della tutela di loro competenza è di assicurare non più unicamente i diritti dei singoli interessati, ma, finanche, quelli della società nel suo complesso[49].

Conseguentemente[50], a fronte di un titolare del trattamento che intenda avviare processi di gestione di dati personali, avremo un'Autorità di controllo meno interventista in termini di poteri preventivi di autorizzazione e di nulla osta e che lascerà più spazio alle decisioni autonome e consapevoli dei titolari del trattamento. Tuttavia, se, successivamente, dovesse emergere che i rischi siano stati sottovalutati e che le condotte di questi ultimi non siano state rispettose del regolamento, allora l'Autorità potrà attivare i propri compiti di vigilanza e di controllo, ricorrendo ai significativi poteri di indagine e, poi, in fase decisionale, ai poteri correttivi.

In merito, si rilevi che il considerando 129 *GDPR* dichiara che tutte le misure assunte dalle Autorità garanti della protezione dei dati personali devono essere «appropriate, necessarie e proporzionate».

Invero, nel *GDPR*, è frequente il riferimento al principio di proporzionalità. In particolar modo, il considerando 4 *GDPR*, pur rimarcando che il trattamento dovrebbe essere al servizio dell'uomo -ponendo, in tal guisa, l'individuo al centro della questione di tale attività e riconoscendo la preeminenza dei diritti

---

[44] G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv.trim.dir.pubbl.*, 2022, pp. 1085 ss. par. 2, consultabile *online* sul sito http://dejure.it;

[45] Sul punto e per le notazioni che seguono L. CALIFANO, *op.cit.,* p. 5.

[46] F. PIZZETTI, *op.ult.cit.,* p. 107 s.

[47] A. MANTELERO, *La riforma della data protection in Europa; un'opportunità per le imprese*, in *Giustiziacivile.com*, 3 marzo 2024. A fronte delle aumentate "responsabilità" dei titolari e dei responsabili del trattamento, si collocano le nuove garanzie assicurate agli interessati che restano, come ovvio, figure centrali anche nel nuovo regolamento. Per un'attenta analisi dei diritti dell'interessato, si v. F. PIRAINO*, I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in AA.VV., *GDPR tra novità e discontinuità*, a cura di R. CATERINA, *cit.,* p. 2789 ss.

[48] L. CALIFANO, *op.cit.*, p. 7. Si v. anche C. SOLINAS, *Autonomia privata e regolazione pubblica dei dati personali*, Bari, 2022, p. 133 ss., la quale afferma che l'Autorità garante della *privacy* ha un ruolo sempre più pregnante di regolare e promuovere la "virtuosa" circolazione dei dati personali. E. GUARDIGLI, *Le autorità di controllo*, in AA.VV., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, *cit.*, p. 491 s. sottolinea lo spazio più esteso riconosciuto alle Autorità dal regolamento, rispetto alla previgente direttiva.

[49] F. PIZZETTI, *op.ult.cit.,* 108 s.

[50] Per le riflessioni che seguono si v. L. CALIFANO, *op.cit.*, pp. 12, 7, 18 s.

fondamentali[51]-, malgrado ciò, afferma che il diritto alla protezione dei dati personali «non è una prerogativa assoluta», ma deve essere considerato «alla luce della sua funzione sociale» e deve essere bilanciato in ossequio al principio di proporzionalità[52]. Il considerando esprime, in sostanza, il principio, secondo il quale la relazione tra la tutela dei dati personali e gli altri diritti fondamentali, sanciti dalla Carta dei diritti fondamentali UE- quali la libertà di pensiero, di coscienza e religione, la libertà di espressione e d'informazione, così come la libertà d'impresa-, non può essere risolta sempre nel senso di far prevalere il diritto alla protezione dei dati personali[53]. In tale ottica, in maniera assoluta, è inviolabile solamente il valore della persona umana, il suo sviluppo e la sua dignità[54].

In conclusione, il regolamento ha profilato un modello relazionale della tutela dei dati personali[55], visto che, come rimarcato dal Maestro Cesare Massimo Bianca, il contemperamento delle contrapposte esigenze «costituisce il motivo di fondo della nuova disciplina e deve, dunque, rappresentare un punto fermo per l'orientamento per l'interprete»[56].

Pertanto, le Autorità garanti della *privacy*, come pure le autorità giudiziarie, nel valutare la legittimità di un peculiare trattamento dei dati personali, dovranno compiere il "giusto" bilanciamento tra gli interessi delle persone coinvolte che potrebbero subire un pregiudizio dall'uso delle proprie informazioni, da un lato e le esigenze sottese a tale attività, dall'altro lato[57], alla luce dei valori costituzionali interni ed europei[58].

Più specificamente, l'Autorità eserciterà il potere di comminare sanzioni pecuniarie, soltanto quando lo riterrà "necessario" ed "opportuno", ai sensi dell'art. 83, par. 2: potrà, cioè, decidere se la sanzione sia uno strumento, di per sé, sufficiente oppure se accostarla ad una misura correttiva diversa. In qualunque modo, la decisione dovrà ispirarsi ai principi generali, più

---

[51] V. RICCIUTO, *op.cit.*, p. 91.

[52] Le Autorità di protezione dei dati personali devono anche ricorrere a una soluzione che dia attuazione al principio di ragionevolezza che si combina col principio di proporzionalità. La ragionevolezza è un criterio di bilanciamento qualitativo, idoneo a bilanciare due o più interessi eterogenei. Sulla portata della ragionevolezza nell'attività di bilanciamento, si v. P. PERLINGIERI, *Equilibrio normativo e principio di proporzionalità nei contratti*, in *Rass.dir.civ.*, 2001, p. 52.

[53] E. TOSI, *Dati personali e contratto: un ossimoro apparente*, in *EJPLT*, 2025/2, p. 3.

[54] P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, *cit.*, p. 483. La nuova normativa, benché volta al contemperamento tra gli interessi economici alla libera circolazione dei dati personali e la protezione dei valori democratici e costituzionali, ha una connotazione decisamente personalistica e un'impostazione maggiormente incentrata sulla correlazione tra il diritto alla *privacy* e il diritto alla protezione dei dati personali, da un lato, e la tutela della dignità umana, dall'altro lato. Si v. O. POLLICINO, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *Rivista AIC*, 8.4.2025, p. 147. In tal senso si v., già, C.M. BIANCA, F.D. BUSNELLI, *op. cit.*, pp. LVIII – LIX, ove si sostiene che la protezione della riservatezza, dell'identità personale e del diritto alla protezione dei dati personali è compiuta attraverso il principio fondamentale della "dignità dell'interessato" che permette «un'opera di disarticolazione della generale categoria dei dati personali», al fine in di individuare «tutele graduate a seconda dei valori più o meno forti che un generico riferimento alla *privacy* necessariamente sottende».

[55] Autorevolmente, S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. priv.* 1997, p. 583 ss., afferma che non si tratta soltanto di scegliere tra valori contrapposti, facendo prevalere nettamente l'uno sull'altro, ma è necessario procedere a bilanciamenti più complessi tra gli interessi in gioco, per assicurare sia la garanzia dei diritti individuali, sia «la progressiva apertura della società»

[56] C.M. BIANCA, *op.cit.*, XXXI.

[57] Si v. M.S. ESPOSITO, *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Dir. inf. e informatica,* 2019, p. 1071 ss., § 4, consultabile sul sito https://dejure.it

[58] Si v. E. TOSI, *op.loc.ult.cit.*

esattamente al principio di proporzionalità, dovendosi tenere conto delle situazioni concrete di illiceità riscontrate, in linea con quanto stabilito dall'art. 83, par. 1, a norma del quale le sanzioni devono essere «in ogni caso effettive, proporzionate e dissuasive». Il *GDPR* ascrive, in tal modo, all'Autorità di controllo un potere discrezionale (e non un mero arbitrio) rispetto alla qualità degli interventi da compiere, quando si trovi di fronte all'accertamento di violazioni del regolamento, ispirato prioritariamente al principio di gradualità del potere sanzionatorio[59].

In tal senso, di prioritaria valenza è la sentenza della Corte di Giustizia UE, 26.9.2024, nella causa C-768/21 Land Hessen che ha, innanzitutto, chiarito che la funzione principale dell'autorità di vigilanza non è di sanzionare, bensì di controllare che l'attività del titolare del trattamento sia conforme ai principi del *GDPR*; per, poi, affermare che il discernimento dell'Autorità può condurre, legittimamente, anche ad un provvedimento non sanzionatorio, ma ad una misura differente che deve essere sicuramente proporzionata alla gravità della violazione e alla necessità di garantire la conformità al *GDPR*[60].

Conclusivamente, l'impianto normativo formulato dal legislatore europeo che, per un verso, ha imposto doveri definiti in capo ai titolari del trattamento dei dati personali e, per altro verso, ha previsto un controllo più pervasivo da parte delle Autorità di vigilanza sulle loro condotte, misure entrambe ispirate ai principi di prevenzione e precauzione[61], induce a tre ordini di considerazioni.

In primis, può affermarsi che il Regolamento si è discostato dalla «direttiva madre», per passare da una regolamentazione improntata sul consenso informato ad una concezione che si basa, in prevalenza, sul controllo[62]. Tale impostazione legislativa è stata sospinta dalla consapevolezza che il 'mero' consenso non è, di per sé, uno strumento idoneo a assicurare effettivamente la protezione dell'interessato, per due ordini di motivi: sia perché esso potrebbe non essere realmente libero, considerando che sovente è, di fatto, 'imposto'

---

[59] D. SIMONETTI, V. PRANDO, *Protezione dei dati personali: l'autorità di controllo non è obbligata a esercitare un potere correttivo in tutti i casi di violazione e, in particolare, ad imporre un'ammenda*, in *Rivista Diritto di internet*, 10 ottobre 2024, consultabile al sito https: dirittodiinternet.it. Tale discrezionalità emerge, con forza, in relazione all'ammontare delle sanzioni amministrative pecuniarie, giacché il regolamento ha fissato due gruppi di sanzioni, da irrogare a seconda che le violazioni siano di minore o maggiore gravità - nel quale ultimo caso, ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

[60] La sentenza è consultabile sul sito https://curia.europa.eu. La Corte di Giustizia UE ha deciso su una domanda pregiudiziale presentata dal Tribunale Amministrativo di Wiesbaden, relativa all'interpretazione del combinato disposto di talune norme del *GDPR*, in merito ai poteri sanzionatori delle Autorità nazionali incaricate di vigilare sulla corretta applicazione del regolamento, ai sensi degli artt. 57, par. 1, a), 58, par. 2 e 77, par. 1. La pronuncia precisa che dall'interpretazione dell'art. 58, par. 2 non può dedursi che l'Autorità di controllo è obbligata, in tutte le ipotesi in cui riscontri una violazione dei dati personali, ad irrogare una misura correttiva, segnatamente una sanzione amministrativa pecuniaria, quanto, diversamente, che la stessa dovrà compiere un'analisi approfondita del caso concreto. Di qui, qualora emergano, come nella controversia giudiziale oggetto di attenzione, elementi che manifestino un atteggiamento responsabile di risoluzione delle problematicità assunto da parte del titolare del trattamento, la discrezionalità dell'autorità può condurla, in modo legittimo, a adottare una misura differente che dovrà essere, comunque, proporzionata alla complessità della violazione e alla necessità di garantire la conformazione al Regolamento generale sulla *privacy*. Si v. D. SIMONETTI, V. PRANDO, *op.loc.ult.cit.*

[61] P. PERLINGIERI, *op.ult.cit.*, p. 481.

[62] P. PERLINGIERI, *op.ult.cit.*, p. 482. Si condivide appieno tale ricostruzione, pur dovendo rammentare che, nel *GDPR,* permane la regola principale della necessità del consenso del soggetto interessato, ai fini della liceità del trattamento, che deve essere libero ed informato. Il titolare o il responsabile devono, difatti, chiarire all'interessato le modalità ed i contenuti dell'attività del trattamento, fornendo, entro un tempo ragionevole, un'informativa chiara, concisa, trasparente e facilmente accessibile.

quale condizione per accedere ad un servizio offerto o per acquistare un bene[63]; sia poiché il consenso potrebbe non essere realmente 'informato', visto che il titolare dei dati non è sempre in grado di comprendere le comunicazioni che gli vengono presentate[64].

Secondariamente, la *policy of law* descritta ha un palese significato di carattere sistemico, giacché si è voluto disporre un quadro normativo aperto al futuro e adeguato a dare tutela a una grande pluralità di trattamenti possibili, anche in previsione delle nuove inevitabili evoluzioni che la tecnologia digitale avrà in questa materia[65].

Infine, ovviamente, l'ampliamento dei margini di discrezionalità riservati all'intervento delle Autorità è contemperato da un incisivo vaglio da parte dei giudici competenti a conoscerne le impugnazioni[66].

3. Il Digital Services Act, il Coordinatore dei Servizi Digitali e la Commissione europea.

Per comprendere il ruolo del Coordinatore dei servizi digitali e delle altre Autorità competenti istituite, a norma del *DSA*, al fine di «garantire l'efficacia dei diritti e degli obblighi» sanciti dal regolamento «e il conseguimento dei suoi obiettivi» (considerando 111), occorre prendere le mosse dalla considerazione che le piattaforme digitali di grandi dimensioni dettano le regole mediante i c.dd. *terms and conditions*, con i quali dominano intere porzioni di mercato[67] e sono detentrici dell'accesso ai servizi erogati e di tutti i poteri di organizzazione degli stessi e di *policy*. Le *tech giants* hanno, ormai, un potere enorme dal punto di vista giuridico, socio-economico e l'attività, dalle stesse svolte, è potenzialmente idonea a condizionare i comportamenti dei cittadini e ad avere effetti dirompenti sul piano pubblicistico ed istituzionale[68].

---

[63] Gli utenti, per poter accedere ai servizi offerti dai *social networks on line*, si vedono tradizionalmente costretti a fornire i propri dati personali e il consenso al trattamento degli stessi risulta essere «forzato». Si v. V. RICCIUTO, *Intelligenza artificiale e protezione dei dati*, in *EJPLT*, 2025/2, p. 2, consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/index

[64] F. FABIO, *Il consenso e le altre condizioni di liceità*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, *cit.*, p. 1318 ss. Sul punto si v. L. GATT, R. MONTINARI, I. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol.dir.*, 2017, p. 376 ss. Per l'analisi critica della valenza del consenso al trattamento dei dati personali nelle comunicazioni elettroniche, si v. M. A. BLANDINO GARRIDO, *El consentimiento del interesado al tratamiento de sus datos personales en las comunicaciones electrónicas,* in *Revista de Derecho Civil, 2022*, Vol. 9, Núm. 4, pp. 195-228.

[65] F. PIZZETTI, *op.ult.cit.*, p. 114.

[66] E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023, p. 213. Gli strumenti di tutela amministrativa e giurisdizionale sono disciplinati dagli artt. 77 ss., ove si distinguono tre forme di esercizio del diritto dell'interessato: la tutela in via amministrativa innanzi all'Autorità di controllo rispetto a un trattamento dei propri dati compiuto in violazione del regolamento, *ex* art. 77; la tutela in via giurisdizionale in riferimento ai provvedimenti ed ogni decisione vincolante dell'Autorità di controllo, *ex* art. 78; la tutela in via giurisdizionale, finalizzata a far valere un proprio diritto, riconosciuto dal *GDPR*, nei confronti di chi abbia effettuato il trattamento. Si v. A. CANDINI, *Gli strumenti di tutela*, in AA.VV., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, *cit.*, p. 570 ss.

[67] Si v. A. VALONGO, *Il potere normativo delle piattaforme digitali*, in AA.VV., *Intelligenza artificiale e piattaforme digitali: dalla co-regolamentazione alla co-vigilanza. Atti del Convegno 10-11 febbraio 2025. Università degli Studi di Perugia*, a cura di M. ANGELONE, C. COLOMBO, I. MARTONE, C. PERLINGIERI, A. VALONGO, *cit.*, p. 140 s.

[68] Si v. C. CAMARDI, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Juscivile*, 2021/4, p. 909, consultabile al sito https://www.juscivile.it/

Segnatamente, le piattaforme digitali hanno un vero e proprio potere normativo in senso ampio, laddove fissano regole che vanno oltre i confini statali e sono, in sostanza, imposte agli utenti del servizio e, quindi, obbligatorie per gli stessi[69]: trattasi di condizioni generali di contratto, relativamente alle quali il consenso non è effettivamente manifestato, dato che è "*blanket assent*" (ossia, preventivo globale); inoltre, esse si configurano secondo il modello *take it or leave it*[70], ragion per cui la mancata adesione alle medesime implica l'impossibilità di utilizzo della piattaforma, al quale molti non vogliono o non possono rinunciare.

Per di più, sia gli utenti del servizio, sia i terzi che segnalano l'illegalità di contenuti pubblicati sono destinatari delle decisioni delle piattaforme, in merito alla loro rimozione e alla disabilitazione dell'accesso. Non si tralasci che gli utenti possono contrastare tali risoluzioni, esercitando un reclamo alle piattaforme che lo gestiscono, svolgendo, di fatto, una funzione "para-giurisdizionale", riscontrabile anche nell'emersione di forme di giustizia privata, quali l'*Oversight Board* di *Meta*[71].

Si ricordi, altresì, che le piattaforme digitali, oltre ad organizzare servizi di accesso ed uso della rete per scopi di carattere economico o sociale, procedono alla raccolta e al trattamento di flussi di dati personali degli utenti (che li immettono irrimediabilmente in circolazione dal momento dell'accesso), «per essere scambiati e trasformati in altri "prodotti" e servizi»[72].

Orbene, l'impiego di assetti contrattuali, predisposti unilateralmente e uniformemente dalle *big tech*, «arrogandosi in definitiva un potere regolamentare che solo apparentemente è subordinato al consenso dei destinatari»[73], costituisce, senza dubbio, la manifestazione di «un'autorità privata». La locuzione fu coniata dal professore Cesare Massimo Bianca, negli anni Settanta, facendo riferimento a fenomeni, dalla famiglia ai gruppi sociali organizzati, in cui si rileva il «potere di imporre giuridicamente ad altri le proprie decisioni» e che, osservati dal punto di vista dei destinatari, costituiscono situazioni «di soggezione ad altrui poteri decisionali di vario contenuto, che si estrinsecano anche in specifici atti dispositivi»[74].

L'Illustre Autore, nell'elaborare tale categoria, ha messo in discussione la tradizionale contrapposizione tra diritto privato/diritto dell'autonomia e diritto pubblico/diritto dell'autorità, precisando che «la netta giustapposizione tra diritto privato e diritto pubblico con riferimento ai termini dell'autonomia e dell'autorità può tuttavia suscitare già un primo motivo di dubbio se si consideri che anche il diritto privato conosce il fenomeno dell'autorità, quale potere di imporre giuridicamente ad altri le proprie decisioni»[75].

---

[69] Si v. A. IANNOTTI DELLA VALLE, *Le «autorità private» digitali e il ruolo del diritto pubblico: attualità e trasversalità dell'opera di Cesare Massimo Bianca,* in *EJPLT*, 2025/2, pp. 5, 7, consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/index.

[70] Sul punto e per le notazioni che seguono si v. D. D'ALBERTI, *Google e le nuove autorità private: la metamorfosi dal fatto al diritto*, in *Riv.dir.civ.*, 2021, pp. 778, 780.

[71] Si v. A. IANNOTTI DELLA VALLE, *op.cit.*, p. 5 s.

[72] Si v. C. CAMARDI, *op.ult.cit.*, p. 914.

[73] Si v. C.M. BIANCA, *Le autorità private*, Napoli, 1977, p. 63.

[74] Si v. P. RESCIGNO, *Presentazione*, in C.M. BIANCA, *op.ult.cit.*, p. XI.

[75] Si v. C.M. BIANCA, *op.ult.cit.*, p. 41. Successivamente, con la globalizzazione e il progresso tecnologico, si sono dischiusi nuovi spazi al potere dei privati, conducendo all'individuazione di nuove "autorità private" nei più vari settori dell'ordinamento, con evidenti conseguenze sul sistema tradizionale delle fonti del diritto e

Tanto più, il Maestro ha distinto tra «autorità di fatto» e «autorità di diritto»: le prime esprimono poteri decisionali privati che si fondano su posizioni di forza economico-sociale[76] e le seconde sussistono quando vi sia un'attribuzione legale oppure convenzionale di poteri autoritativi privati, motivata da peculiarità giuridiche[77].

In quel momento storico, il professore Cesare Massimo Bianca non avrebbe potuto immaginare la forza socio- economica e la capacità organizzativa assunta dalle grandi società multinazionali del settore tecnologico, in forza delle quali "regolano" il fenomeno digitale; eppure, la categoria delle "autorità private" appare essere assolutamente efficace e «lungimirante», per definire la posizione delle piattaforme digitali, considerato che queste ultime si sono rapportate, sin dall'inizio, agli utenti del servizio in modo non paritario, ma asimmetrico, sia dal punto di vista giuridico, sia sul piano sociale, esercitando, in realtà, un'«autorità di fatto» a tutti gli effetti[78].

Cionondimeno, ci si domanda se provvedimenti recenti, tra i quali, in primo luogo, il *Digital Services Act* e il *Digital Markets Act* non abbiano dato luogo a una "metamorfosi" dei poteri delle piattaforme digitali da "autorità di fatto" ad "autorità di diritto"[79].

A tal proposito, l'Esimio Autore aveva, già, compreso la necessità di accertare se situazioni di assoggettamento ad un altrui potere decisionale "di fatto" richiedano l'intervento del legislatore che ha il compito di circoscrivere quei poteri dei privati che, deviando in abusi, provocano diseguaglianze inammissibili[80].

---

sul rapporto pubblico-privato. Si v. E. BELLISARIO, *Le "autorità private" nell'era della sostenibilità. Gli impatti dell'ESG Disclosure regulation e del Taxonomy regulation*, in *Actualidad Jurídica Iberoamericana* 2022, n. 16 bis, *junio*, p. 106. A quarant'anni dalla pubblicazione del volume, l'opera collettanea AA. VV. *I poteri dei privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, a cura di P. SIRENA e A. ZOPPINI, Roma, 2018 si pone l'obiettivo di analizzare gli effetti sistematici che la normativa privatistica funzionalizzata al controllo del potere privato e delle sue forme di esercizio possa avere rispetto al sistema tradizionale delle fonti del diritto e delle regole che operano in settori specifici dell'ordinamento giuridico. Si v. P. SIRENA e A. ZOPPINI, *Premessa*, *ivi*, p. 2. Si v. anche M. GRONDONA, *Poteri dei privati, fonti e trasformazioni del diritto: alla ricerca di un nuovo ordine concettuale, ivi,* p. 5 ss. che si sofferma sul rapporto tra diritto privato e diritto pubblico «spesso non oppositivo, anzi reciprocamente completivo», incentrando l'attenzione sul rapporto tra poteri dei privati, diritto della regolazione e fonti del diritto.

[76] Si v. C.M. BIANCA, *op.ult.cit.*, pp. 55-79, secondo il quale i poteri di fatto possono essere «interni»- vale a dire inerenti al settore del lavoro o dell'impresa, ove si assiste al prevalere del datore di lavoro sul lavoratore oppure a gruppi organizzati, nei quali prevale la maggioranza sulla minoranza- ovvero «esterni», quando riguardino posizioni di dominio nel campo della vita pubblica (nel campo politico o sindacale) oppure nella vita economica, in particolare quando l'impresa imponga le condizioni generali di contratto a terzi, assoggettando una categoria al proprio potere contrattuale.

[77] Tra queste, l'Autore individua l'autorità privata nei gruppi organizzati, quali le società, tenendo conto dei poteri dell'assemblea, degli amministratori e, in ultima istanza, dell'autorità dell'imprenditore. Si v. C.M. BIANCA, *op.ult.cit.*, pp. 9-54.

[78] Si v. A. IANNOTTI DELLA VALLE, *op.cit.,* p. 4 s. Si dichiara che «ad uno sguardo retrospettivo, è proprio quell'intuizione a rivelarsi la più lungimirante e capace di cogliere le vere sfide che la trasformazione dei rapporti economici e il progresso tecnologico pongono oggi al diritto privato». Si v. G. RESTA, *Poteri privati e regolazione*, in *Potere e costituzione, I tematici, Enc. dir.*, GFL, a cura di M. CARTABIA, M. RUOTOLO, Milano, 1008 ss.

[79] In tal senso D. D'ALBERTI, *op.cit.*, p. 748.

[80] Cesare Massimo Bianca aveva compreso la necessità di un sistema di garanzie nei confronti delle autorità private, a tutela dei diritti e del principio di eguaglianza sostanziale, analogo a quello esistente per quanto concerne le autorità pubbliche. Donde, si domandava se potesse immaginarsi un intervento dello Stato e dei poteri pubblici, accanto ad una tutela di stampo privatistico, giungendo alla conclusione che gli strumenti di diritto pubblico e del diritto privato possono coesistere. In sostanza, secondo tale ricostruzione, si dovrebbe ricorrere al diritto pubblico solo quando sia essenziale per il perseguimento degli obiettivi

Tale intuizione è stata colta dal legislatore europeo che ha sentito l'esigenza di disciplinare i poteri delle piattaforme digitali, spesso più potenti degli Stati nazionali[81], con l'obiettivo di limitarne i possibili abusi e di imporre la tutela dei diritti fondamentali, oltre che di garantire il migliore funzionamento del mercato digitale, operando un riconoscimento regolamentato di tali poteri, attraverso l'intermediazione legittimante dell'ordinamento giuridico[82].

Più esattamente, mentre prima del *Digital Services Act*, vi era una sorta di «immunità» delle piattaforme digitali dal potere pubblico[83], il Regolamento ha, viceversa, imposto loro doveri di *due diligence*, provvedendo alla loro graduale responsabilizzazione e statuendo il controllo delle loro attività da parte delle Autorità di vigilanza a ciò preposte. Il legislatore europeo ha, in tal guisa, decretato il primo passaggio nella loro raffigurazione da «autorità di fatto» ad «autorità di diritto»[84].

Ai fini di chiarire l'asserzione, si rimarchi che il *Digital Services Act* si è mosso su due linee direttrici: da un lato, ha ripreso l'ordito normativo della direttiva *e-commerce* sulla responsabilità civile degli *internet service providers* e ha aggiunto talune norme innovative, dal punto di vista procedurale; dall'altro lato, si è discostato da tale normativa che si imperniava sulla funzione riparatoria della responsabilità civile di tali soggetti, prevedendo, in aggiunta, una serie di doveri di *due diligence* che sono stati graduati e parametrati sulle loro *abilities* e sul ruolo dagli stessi ricoperto. Tali doveri sono stati imposti in riferimento ai comportamenti da tenere per contrastare i contenuti illegali, la disinformazione in rete e altri rischi sociali e garantire, al contempo, la libertà di espressione e di informazione, la libertà di impresa, il principio di non discriminazione e il raggiungimento di un elevato livello di tutela dei consumatori[85].

Nella regolamentazione europea degli *internet service providers* è penetrato, in maniera incisiva, il principio di *accountability*, specularmente al *GDPR*. Il *DSA* mira, infatti, alla massima responsabilizzazione dei fornitori di servizi digitali, facendo gravare su costoro il dovere di mettere in atto una serie di misure tecniche ed organizzative e di rendere conto della propria attività, dovendo poter provare di aver adempiuto i doveri di *compliance* loro imposti.

Il passaggio dalla responsabilità alla responsabilizzazione è innovativo e al passo con le peculiarità dell'innovazione tecnologica che è «inafferrabile» e caratterizzata da un tale *mix* di complessità specialistica e rapidità evolutiva che è incontestabile che siano gli *internet service providers* i soggetti più idonei a

---

disposti, lasciando, per il resto, spazio al diritto dei privati: «l'esercizio di una posizione di supremazia può essere consentito solo in stretta e necessaria funzione dell'interesse generale». Si v. C.M. BIANCA, *op.cit.*, pp. 4-8, p. 93, s.

[81] A. IANNOTTI DELLA VALLE, *op.cit.*, p. 5.

[82] D. D'ALBERTI, *op.cit.*, p. 80.

[83] G. BUTTARELLI, *op.cit.*, p. 117, il quale descrive accuratamente il passaggio dalla *private regulation* delle piattaforme digitali al recente «ritorno» della regolazione pubblica.

[84] Si v. P. STANZIONE, relazione al seminario del ciclo «*Intelligenza artificiale e diritto*», 21 novembre 2023, dal titolo «*Il diritto delle piattaforme: libertà di manifestazione del pensiero e content moderation, tra diritto dei contratti e Digital Services Act*», organizzato dal prof. Ugo Ruffolo, Università di Bologna. Sul tema, si v. EAD., *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022.

[85] M.A. ASTONE, *Digital Services Act e nuovo quadro di esenzione dalla responsabilità dei prestatori di sevizi intermediari: quali prospettive?"*, in *Contratto e impresa,* 2022, p. 1059. Si v. anche A. PURPURA, *Osservazioni sul Digital Services Act: responsabilità e gestione del rischio nella prestazione di servizi intermediari*, in *Comparazione e diritto civile*, 2022/3, p. 1035 ss.

rimuovere i contenuti illegali e, in via preventiva, a impedirne la diffusione, in quanto in possesso delle conoscenze indispensabili a svolgere il compito normativo[86].

A dire il vero, la scelta di politica del diritto di modellare la disciplina delle attività di tali soggetti sul principio di *accountability* discende dalla circostanza che i tradizionali paradigmi della responsabilità civile risultano essere inefficienti, per far fronte alle nuove sfide poste dalla conformazione tecnica delle nuove figure di *providers* e per garantire una tutela effettiva dei diritti e delle libertà fondamentali degli internauti e dei cittadini.

Per contro, la responsabilizzazione dei fornitori di servizi di intermediazione *online* è in grado di affrontare le questioni derivanti dall'incedere della tecnologia, dacché è una «forma di autocontrollo», legata ad una *compliance* intelligente che consente, *ex post*, di valutare se si sono adottate tutte le misure di prevenzione fondamentali, per assolvere ai doveri imposti *ex lege*.

Il *DSA*, al fine promuovere un comportamento diligente e responsabile dei prestatori di servizi digitali, ha, così, previsto una serie di doveri di diligenza «a cerchi concentrici» che si fanno, via via, più intensi all'aumentare del tipo di attività svolte e della loro dimensione, secondo il prisma del principio di proporzionalità [87]. Si realizza, in tale maniera, una responsabilizzazione differenziata dei *providers* che si declina in doveri incombenti su di loro e che è direttamente proporzionale all'impatto potenziale della loro attività sui diritti e sulle libertà fondamentali delle persone[88].

Allora, *in primis*, si impone a tutti i prestatori di servizi intermediari di individuare un unico punto di contatto per agevolare il dialogo con le Autorità degli Stati membri e il dovere di nominare un legale rappresentante nel territorio dell'Unione europea, quando i *providers* siano stabiliti al di fuori della stessa e offrano servizi ai cittadini europei.

Di valore significativo è l'imposizione, *ex* art. 14, di doveri di trasparenza. Gli *internet service providers* sono tenuti a fornire informazioni, nelle loro condizioni generali di servizio, su eventuali politiche, procedure, misure e strumenti impiegati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché sulle regole procedurali del loro sistema interno di gestione dei reclami. Costoro, nell'applicare e far osservare eventuali restrizioni previste nelle condizioni generali del servizio, relative a tali possibili politiche e procedure, devono agire in modo diligente, obiettivo e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio.

L'art. 15 ha anche statuito che tutti i prestatori di servizi intermediari devono mettere a disposizione del pubblico, in un formato leggibile meccanicamente e in un modo facilmente accessibile, almeno una volta all'anno, relazioni chiare e

---

[86] Sul punto e per le argomentazioni che seguono, si v. la relazione di A. GAMBINO, nell'ambito del webinar "*Il Digital Services Act: tra responsabilità e governance*", 15 dicembre 2020, consultabile al sito https://www.dimt.it/news/il-digital-services-act-tra-responsabilita-e-governance-commento-alla-proposta-di-regolamento

[87] G. MORGESE, *Proposta di Digital Services Act e rimozione dei contenuti illegali online*", in AA. VV., *Verso una legislazione europea su mercati e servizi digitali*, a cura di G. CAGGIANO, G. CONTALDI, P. MANZINI, Bari, 2021, p. 36.

[88] F. MOLLO, *La responsabilità del provider alla luce del Digital Service Act*, in *Contratto e impresa Europa,* 2022, p. 199.

facilmente comprensibili sulle attività di moderazione dei contenuti svolte durante il periodo di riferimento.

Un primo livello di responsabilizzazione degli *internet service providers* si identifica, perciò, con i doveri di trasparenza e di comunicazione posti a loro carico.

Secondariamente, il regolamento prescrive una maggiore proceduralizzazione per tutti i prestatori di servizi di *hosting*, indipendentemente dalle loro dimensioni [89]. Costoro sono obbligati ad apprestare dei meccanismi di notifica di facile accesso, che permettano a chiunque di comunicare la presenza, nel loro servizio, di informazioni ritenute pregiudizievoli, affinché i *providers* effettuino un trattamento tempestivo, diligente e obiettivo delle segnalazioni, a protezione dei diritti e delle libertà fondamentali delle parti interessate.

Colui che abbia effettuato la segnalazione ha il diritto di ricevere, senza indebito ritardo, dapprima, una conferma della sua ricezione e, successivamente, una notifica della decisione del *provider*, contenente le indicazioni sulla possibilità di effettuare un reclamo avverso la stessa[90].

In terzo luogo, il regolamento è intervenuto relativamente alle piattaforme digitali, introducendo il dovere di un *complaint mechanism* interno di gestione dei reclami, relativi alle risoluzioni assunte, riguardanti la rimozione di un contenuto, la sospensione o la terminazione del servizio, la sospensione o la rimozione dell'*account* dell'utente.

La piattaforma digitale è obbligata a sospendere dal servizio colui che, "con frequenza", fornisca contenuti manifestamente illegali.

Sono, altresì, tracciate misure tecniche e organizzative essenziali, per garantire che siano trattate e decise, in via prioritaria e senza indebito ritardo, le segnalazioni presentate dai "segnalatori attendibili", che agiscono entro il loro ambito di competenza designato, avvalendosi dei meccanismi di *notice and take down*, di cui all'articolo 16[91].

Sono previste anche disposizioni più precise che prevedono regole di trasparenza più stringenti per le piattaforme *online* che permettono ai

---

[89] Sul punto e per le osservazioni che seguono, si v. F. MOLLO, *op.cit., p.* 196 s. Ad avviso di chi scrive, la mancata osservanza dei doveri di diligenza normativamente previsti può determinare l'insorgere di fattispecie di responsabilità contrattuale. Per un approfondimento, mi si consenta di rinviare a G. D'ALFONSO, *Le piattaforme digitali tra responsabilità civile e responsabilizzazione alla luce del Digital Services Act*, in AA. VV., *Consumidores y nuevas tecnologías*, a cura di M. D. CERVILLA GARZÓN, I. ZURITA MARTÍN Atelier Libros Jurídicos, Barcellona, 2024, p. 127 ss.

[90] A salvaguardia della trasparenza dei meccanismi di segnalazione e di decisione, si è imposto all'*hosting provider* sia un dovere di motivazione analitica della stessa, per permettere ragionevolmente all'utente del servizio di esercitare, in modo effettivo, i mezzi di ricorso, sia il dovere di adottare sistemi interni di gestione dei reclami accessibili, gratuiti ed efficaci.

[91] I segnalatori attendibili possono essere raffigurati come «entità semi-pubbliche», giacché lo *status* è loro conferito dal Coordinatore dei servizi digitali nazionale, qualora dimostrino di soddisfare tutte le condizioni previste dall'art. 22, par. 2. Trattasi di enti di natura pubblica, organizzazioni non governative o organismi privati che dimostrano di possedere i requisiti essenziali per l'esercizio del ruolo di segnalatore, tra i quali, in special modo, l'indipendenza da qualsiasi fornitore di piattaforme *online*, la diligenza, l'obiettività e il possesso di competenze specifiche nella lotta ai contenuti illegali. Sotto un altro punto di vista, si potrebbe correre il rischio dell'*overdeterrence*, visto che è probabile che le richieste di *notice and take-down*, presentate dai segnalatori attendibili, siano automaticamente processate. Si v. V. ZENO ZENCOVICH, *The EU regulation of speech. A critical view,* in *Media Laws, Rivista del diritto del medi*a, 14 giugno 2023, p. 4 s. L'Autore definisce criticamente i segnalatori attendibili una «squadra privata». L'articolo è consultabile sul sito www. medialaws.eu

consumatori di concludere contratti a distanza con operatori commerciali, al fine di garantire una tutela effettiva di tali soggetti; oltre che per quelle che visualizzano pubblicità sulle proprie interfacce, in ragione del loro raggio d'azione e della loro capacità di rivolgersi ai destinatari del servizio e di raggiungerli, in base al loro comportamento all'interno e all'esterno dell'interfaccia *online* della piattaforma.

Il livello di responsabilizzazione diventa massimo con riferimento alle piattaforme *on line* ed ai motori di ricerca "di dimensioni molto grandi", *ex* art. 33, par. 1 *DSA*, per i quali sono disposte norme molto più rigorose. Tale approccio risponde all'esigenza di imporre doveri supplementari in capo a soggetti che, grazie a meccanismi di datificazione, mercificazione e selezione, sono in grado di esercitare un potere economico, politico e culturale tale da poter persuadere e dirigere i cittadini verso certi comportamenti[92].

Ebbene, ai sensi dell'art. 34, codesti *providers* sono periodicamente tenuti a individuare, analizzare e valutare, con diligenza, i potenziali "rischi sistemici" derivanti «dalla progettazione e dal funzionamento del servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi», valutandone la gravità e la probabilità di realizzazione. La valutazione del rischio deve essere accurata per i loro servizi e proporzionata ai rischi sistemici che sono raggruppati in quattro aree, appositamente individuate in maniera ampia: la prima riguarda la "diffusione di contenuti illegali" che possono essere divulgati tramite i servizi delle piattaforme; la seconda gli "eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica"; la terza gli effetti negativi, attuali o prevedibili, relativi alla "violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona"; la quarta gli "eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali", tra i quali, per l'appunto, il diritto alla protezione dei dati personali, espressamente richiamato dall'art. 34, par. 1, co. 2, lett. b).

Le piattaforme digitali e i motori di ricerca "di dimensioni molto grandi" devono agire, nello svolgimento dei loro doveri di valutazione dei rischi, secondo principi di trasparenza, della pubblicità delle loro analisi e della condivisione dei dati con le Autorità di vigilanza e con la Commissione europea[93].

In seguito al *risk assessment*, questi *internet service providers* devono esperire "misure di attenuazione" ragionevoli, proporzionate ed efficaci, adeguate ai rischi sistemici che hanno individuato e in un ambito di collaborazione rafforzata orizzontale tra le piattaforme e verticale, ovverosia con le varie Autorità di vigilanza e con la Commissione.

Si aggiunga che l'assetto dei poteri di vigilanza e controllo predisposto dal *DSA* presenta un «sistema a rete» che si articola a livello nazionale ed europeo[94].

---

[92] E. LONGO, *Libertà di informazione e lotta alla disinformazione nel Digital Services Act*, in *Giornale dir. amm.*, 2023/6, p. 741.

[93] Sul punto e per le considerazioni che seguono, si v. C. CAMARDI, *op.ult.cit.*, p. 911, s.

[94] Sul punto e per le riflessioni che seguono si v. L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv.trim.dir.pubbl.*, 2022/4, p.1107 s.

L'art. 38 ha previsto che ciascuno Stato membro deve istituire un Coordinatore dei servizi digitali che abbia la competenza di sorvegliare gli *internet service providers* che ricadono nella competenza del proprio territorio e di esercitare funzioni di coordinamento delle altre Autorità nazionali competenti. Nello svolgimento dei propri compiti, i Coordinatori dei servizi digitali dispongono, *ex* art. 51, di poteri di vigilanza, di ispezione e di monitoraggio in merito alla condotta dei fornitori di servizi intermediari. A tali Autorità di controllo deve essere garantita una posizione di indipendenza, in ragione della quale le stesse sono titolari, finanche, di funzioni giustiziali e possono ricevere e decidere reclami relativi a violazioni dei doveri regolamentari.

I Coordinatori dei servizi digitali hanno il dovere di cooperazione sia con gli altri Coordinatori nazionali, sia nei confronti del Comitato europeo per i servizi digitali e della Commissione europea[95].

Il Comitato europeo per i servizi digitali, costituito dai Presidenti dei Coordinatori dei servizi digitali e presieduto dalla Commissione europea, sul modello dell'*European Data Protection Board*, ha il compito sia di garantire un efficace raccordo tra i Coordinatori nazionali e di assisterli per l'applicazione coerente del Regolamento, sia di assicurare la collaborazione efficace tra questi ultimi e la Commissione con i portatori di interessi.

La Commissione europea ha una competenza concorrente con i Coordinatori di servizi digitali nazionali per l'esercizio di poteri di vigilanza, indagine, esecuzione e monitoraggio sulle piattaforme *digitali* e motori di ricerca "di dimensioni molto grandi" che abbiano un impatto significativo a livello europeo[96]. La Commissione può esercitare tali poteri di propria iniziativa, nel caso di violazioni durevoli. Essa ha, altresì, compiti di regolazione ed svolge varie funzioni, al fine di perseguire gli obiettivi del regolamento: può, ad esempio, incentivare le grandi piattaforme all'adozione di codici di condotta, al fine di ridurre i rischi sistemici.

L'esercizio del potere sanzionatorio costituisce oggetto di competenza concorrente fra gli Stati membri e la Commissione europea. I primi hanno il dovere di determinare le sanzioni e le penalità di mora da applicare, quando vi sia una violazione della disciplina da parte dei prestatori di servizi intermediari soggetti alla loro giurisdizione, nei limiti dei tetti prefissati dal regolamento. L'art. 52, par. 3 statuisce che l'Autorità di vigilanza competente, nei casi di inottemperanza a uno dei doveri prestabiliti dal *Digital Services Act*, potrà irrogare una sanzione pecuniaria pari al 6% del fatturato annuo mondiale del *provider*. È evidente il rilievo deterrente di tale previsione, se si tiene conto che si rivolge a colossi del mercato come Meta, Google e Apple. I Coordinatori nazionali dovranno notificare alla Commissione i provvedimenti di determinazione delle sanzioni nazionali, che devono essere, a norma del regolamento, «effettive, proporzionate e dissuasive».

Si concluda col dire che, per quanto attiene alle misure di *public enforcement* di questa complessa normativa, l'apparato sanzionatorio avrà un ruolo decisivo.

[95] Sulla ripartizione dei poteri tra i Coordinatori di servizi digitali, il Comitato europeo e la Commissione europea si v. G. SGUEO, *L'architettura istituzionale del Digital Services Act*, in *Giornale dir. amm.*, 2023/4, p. 748.
[96] Sul punto e per le notazioni che seguono, si v. L. TORCHIA, *op.loc.ult.cit.*

Ad ogni modo, per i destinatari delle misure adottate dalle Autorità di vigilanza valgono ordinarie garanzie procedimentali, quali il diritto di essere ascoltati e di accesso al fascicolo e la pubblicazione e la motivazione delle decisioni da parte delle Autorità stesse.

A ben vedere, il modello regolamentare europeo configura un sistema di controllo dell'organizzazione delle piattaforme e del loro operato, per un verso, a prescindere dalle relazioni con i destinatari del servizio e, per altro verso, combinando strumenti di autorità e di libertà, autonomia ed eteronomia dei rapporti contrattuali: il contratto è, pur sempre, imposto dalle piattaforme agli utenti, ma è integrato da diritti e rimedi che le fonti eteronome hanno imposto, di recente, alle "autorità private" [97].

In tale prospettiva, l'autonomia organizzativa delle piattaforme continua ad esplicarsi, ma in un contesto nel quale l'*accountability* e la vigilanza pubblica indipendente fanno da "contrappeso" al rischio che tale autonomia genera nella società.

In proposito, bisogna porre l'accento sulla circostanza che le attività compiute dalle piattaforme digitali implicano irrimediabilmente la raccolta e l'elaborazione dei dati personali degli utenti del servizio da loro offerto. Da ciò discende l'automatica applicazione della regolamentazione dei titolari del trattamento e, dunque, la sussistenza del dovere di rispetto di tutti gli obblighi procedurali e sostanziali fissati dal *GDPR* nell'ambito del rapporto contrattuale con l'utente del servizio; a tali obblighi corrispondono i diritti degli utenti, quali soggetti interessati, quando vantino l'esattezza della prestazione nei confronti dei gestori delle piattaforme, anche sotto questo punto di vista. Puntualmente, questi ultimi dovranno conformarsi alle prescrizioni dell'*accountability* sancite dal *GDPR*, quando, nell'esercizio della propria attività, intercettino ovvero raccolgano esplicitamente ed elaborino i dati personali degli utenti per finalità diverse dall'esecuzione del contratto (come, a titolo esplicativo, la loro condivisione a terzi), che devono essere, in ogni caso, dichiarate, per poter graduare le modalità e i termini del trattamento.

È, per questi motivi, fondamentale un efficace coordinamento non solo delle due normative, ma, tanto più, delle azioni delle diverse Autorità di controllo. La logica settoriale delle competenze delle Autorità deve essere superata a beneficio della trasversalità delle questioni, siccome, nei casi concreti di trattamento algoritmico dei dati personali, ai profili di tutela degli stessi si accompagnano quelli della normativa degli *internet service providers*[98].

D'altra parte, il *DSA* non si propone di alterare il sistema giuridico vigente, quanto, piuttosto, di implementarlo per mezzo di un apparato normativo che si aggiunge, senza eliminarle, alle regolamentazioni di alcuni settori specifici interessati, la cui applicazione viene garantita secondo il criterio di specialità: il *DSA* rappresenta, in altre parole, un quadro comune di regole, applicabile ogniqualvolta manchi una disciplina definita indirizzata alla singola fattispecie che sia presa in considerazione[99]. Più precisamente, il considerando 10, da un lato, afferma che è opportuno che il regolamento non pregiudichi una serie di

[97] Sul punto e per le argomentazioni che seguono, si v. C. CAMARDI, *op.ult.cit.*, pp. 910 s., 914-916.
[98] C. SOLINAS, *Le funzioni delle Autorità indipendenti nel trattamento algoritmico dei dati*, *cit.*, p. 253.
[99] S. SCOLA, *Digital Services Act: occasioni mancate e prospettive future nella recente proposta di regolamento europeo per il mercato unico dei servizi digitali*, in *Contratto e impresa Europa,* 2022, p. 132, s.

normative, tra le quali quelle preposte alla tutela dei dati personali delle persone fisiche (specificando che essa è dettata unicamente dal regolamento generale sulla *privacy* e dalla direttiva 2002/58/CE); dall'altro lato, riconosce che, nella misura in cui gli atti giuridici dell'Unione europea perseguono gli stessi obiettivi del *DSA*, le norme ivi previste «si dovrebbero applicare in relazione alle questioni che non sono affrontate o non sono pienamente affrontate da tali altri atti giuridici nonché alle questioni sulle quali tali altri atti giuridici lasciano agli Stati membri la facoltà di adottare determinate misure a livello nazionale»[100].

4. Il ruolo dell'Autorità di vigilanza del mercato dell'intelligenza artificiale, ai sensi dell'AI Act.

Alla stessa stregua, il considerando 9 *AI Act* chiarisce che le norme armonizzate stabilite nel regolamento dovrebbero applicarsi in tutti i settori e, in linea con la nuova cornice legislativa, non dovrebbero pregiudicare il vigente diritto dell'Unione -specificamente in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione, protezione dei lavoratori e sicurezza dei prodotti-, al quale il regolamento è complementare.

Preminentemente, il considerando 10 *AI Act* afferma che il Regolamento non mira a compromettere l'applicazione di diritto vigente dell'UE che regolamenta il trattamento dei dati personali, «inclusi i compiti e i poteri delle Autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti» e che, laddove la progettazione, lo sviluppo o l'utilizzo dei sistemi intelligenti implichino il trattamento di tali dati, restano impregiudicati i doveri degli operatori che li sviluppino o li impieghino di rispettare tali norme, nella loro qualità di titolari e/o responsabili del trattamento. Sicché, come sottolineato dal Comitato europeo per la protezione dei dati personali, il *GDPR* e il Regolamento sull'intelligenza artificiale devono essere considerati e interpretati, in linea di principio, come strumenti normativi complementari e che si rafforzano vicendevolmente, sia in termini di finalità, sia in termini di tutele offerte, compresi i diritti delle persone interessate[101].

Ciò poiché l'*AI Act* ha ad oggetto specifiche tecnologie che si basano sull'intelligenza artificiale, il cui elemento centrale è il trattamento dei dati personali[102], dal momento che non solo si nutre degli stessi, ma è anche in grado di generarne enormi quantità[103]. I sistemi intelligenti non eseguono regole, ma apprendono schemi, correlazioni e modelli statistici all'interno di una mole ingente di dati personali[104], di cui hanno bisogno per raggiungere un

---

[100] Sul punto, si v. C. SOLINAS, *op.loc.ult.cit.*

[101] EDPB, *Dichiarazione 3/2024 sul ruolo delle autorità di protezione dei dati nel quadro della legge sull'Intelligenza Artificiale*, 16 luglio 2024.

[102] V. RICCIUTO, *op.ult.cit.*, p. 4.

[103] E. PROSPERETTI, *Regole dei dati e regole dell'intelligenza artificiale: quale rapporto*?, abstract della relazione svolta al Convegno dal titolo "*Stati generali di internet e dell'AI*", 2025, p. 2, consultabile al sito https://www.dimt.it/news/online-gli-atti-digitali-degli-stati-generali-del-diritto-di-internet-e-dellintelligenza-artificiale-v-edizione/

[104] F. BARTOLOMEO, *Ai Act, legge 132/2025 e gestione dei dati nell'AI*, *abstract* della relazione svolta al Convegno dal titolo "*Stati generali di internet e dell'AI*", 2025, p. 1 consultabile al sito

elevato grado di rendimento e quanto più è ampio il loro numero posto a disposizione dei sistemi medesimi, molto più precise sono le risoluzioni elaborate[105].

Di qui è d'uopo riflettere sul rapporto tra il *GDPR* e l'*AI Act* e individuare la disciplina applicabile, nella prospettiva del bilanciamento del diritto dell'interessato alla protezione dei propri dati personali e l'esigenza del fornitore di disporne, per sviluppare le applicazioni dell'intelligenza artificiale[106] e di quella del *deployer,* per utilizzarle.

Si premetta che l'*AI Act* intende assicurare la duplice finalità di promuovere lo sviluppo e l'impiego dei sistemi intelligenti e di prevenire i rischi associati, al fine di tutelare la persona[107] e i valori su cui si fonda l'UE[108]. La normativa si basa sul principio del personalismo che si traduce nell'adozione di una logica antropocentrica (secondo la quale suddetti sistemi devono essere a servizio dell'uomo), che acquista effettività solo se integrata da un *risk based approach* che, in tale contesto, non è unicamente a tutela di un unico diritto, come il *GDPR*, né degli utenti delle sole piattaforme digitali incentrandosi sul comportamento degli *internet service providers*, come nel *DSA*, quanto, piuttosto, mira ad assicurare l'affidabilità dei sistemi[109].

Più precisamente, l'*AI Act* impiega tale approccio, fondandosi su una «piramide» ascendente dei rischi connaturati nell'impiego di sistemi di intelligenza artificiale che va, in virtù del principio di proporzionalità, da quello "medio o basso" a quello "alto", fino a quello "inaccettabile", per compiere una graduazione di regole che fissano divieti, doveri e misure di *enforcement*, modulandole in funzione del diverso livello di rischio connesso alle diverse tipologie di attività[110]. Il «rischio tipico» -inteso nel duplice aspetto della

---

https://www.dimt.it/news/online-gli-atti-digitali-degli-stati-generali-del-diritto-di-internet-e-dellintelligenza-artificiale-v-edizione/

[105] P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Riv.it.inform.dir.*, 2024, p. 126; G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, *cit.*, 2022, p. 1085 ss. La questione è stata affrontata, in riferimento ai *Big Data*, ancor prima dello sviluppo dei sistemi di intelligenza artificiale, da A. C. NAZZARO, *L'utilizzo dei Big Data e i problemi di tutela della persona*, in *Riv.dir.civ.*, 2018, p. 1239 ss.

[106] V. RICCIUTO, *op.ult.cit.*, p. 5. D'altronde, il *GDPR* rappresenta «il capostipite illustre della strategia euro-unitaria di *governance*» dei sistemi decisionali automatizzati, perché ha introdotto, per primo, una previsione fondamentale relativa alla soggezione a decisioni adottate con modalità automatizzate, cioè l'art. 22. Si v. O. POLLICINO, *Regolazione e innovazione tecnologica nell'"ordinamento della rete",* in *Rivista AIC*, 2025/2, p. 156). Il Regolamento generale sulla *privacy* non tiene, però, conto delle applicazioni di intelligenza artificiale fondate sui *big data* e, pertanto, non considera il fenomeno sempre più rilevante dei trattamenti dei dati di massa. Si v. G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?, cit.*, p. 86, s.

[107] C. PERLINGIERI, *Intelligenza artificiale tra principi e regole, cit.,* § 2, § 5.

[108] P. PERLINGIERI, *Diritto civile e intelligenza artificiale*, in *Tecnologie e diritto*, 2025, p. 136 s. Ancor prima della presentazione, nell'aprile 2021, della proposta di regolamento da parte della Commissione europea, l'insigne dottrina ha evidenziato come l'elaborazione algoritmica influisca sul procedimento decisorio e imponga, di conseguenza, una riflessione economico-giuridica e, soprattutto, etica. Si è, così, prospettata l'esigenza di monitorare i risultati prodotti dalla stessa, controllandone la compatibilità con il sistema ordinamentale e con i valori umani, sulla base di un ordine pubblico di valenza internazionale che governi sia i rapporti sostanziali, sia i rimedi giurisdizionali. Si v. P. PERLINGIERI, *Sul trattamento algoritmico dei dati personali*, in *Tecnologie e diritto*, 2020, p. 181 ss.

[109] C. PERLINGIERI, *op.ult.cit.*, § 4. L'Autrice analizza la differenza dei valori sui quali si fonda la legislazione europea, rispetto alle strategie normative della Cina e degli Stati Uniti.

[110] Per l'indagine della modulazione della regolamentazione, a seconda della classificazione del rischio e le critiche all'approccio prescelto dal legislatore europeo, si v. E. MAESTRI, *Introduzione e note di sintesi al Regolamento (UE) 2024/1680 sull'intelligenza artificiale (testo ufficiale e integrale*), Napoli, 2024, 1-60. Secondo attenta dottrina, tale approccio si caratterizza per la sua intrinseca inidoneità a regolamentare i presumibili sviluppi applicativi dell'intelligenza artificiale, giacché la classificazione *ex ante* dei sistemi,

combinazione della probabilità del verificarsi di un danno e della sua gravità, *ex.* art. 3- non è definito in corrispondenza dei valori di mercato, ma si riferisce al quadro dei valori e dei diritti fondamentali riconosciuti dall'Unione Europea[111].

Il regolamento pone, anzitutto, divieti con eccezioni e deroghe e impedisce l'ingresso nel mercato interno ai sistemi digitali che creino un rischio "inaccettabile" per la sicurezza, i mezzi di sussistenza e i diritti delle persone[112].

La regolamentazione si incentra prevalentemente sui sistemi ad "alto rischio", che potrebbero determinare danni significativi alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia e allo Stato di diritto e che vengono classificati in: quelli destinati ad essere usati come componenti di sicurezza di prodotti soggetti a valutazione della conformità *ex ante* da parte di terzi - che includono giocattoli, prodotti di aviazione, automobili, dispositivi medici e ascensori-; i sistemi automatizzati, utilizzati per le finalità previste nell'allegato III, che sarà aggiornato periodicamente dalla Commissione europea[113]. Essa, nel vagliare il livello del rischio di danno alla salute e alla sicurezza ovvero di impatto negativo sui diritti fondamentali discendente da un sistema intelligente, dovrà considerare, tra gli altri elementi: la natura e la quantità dei dati trattati e impiegati (più specificamente, la possibilità che si proceda al trattamento di categorie peculiari di dati personali), oltre che la misura in cui il sistema agisce in maniera autonoma e la possibilità che un essere umano annulli una decisione oppure una raccomandazione che potrebbe provocare un danno potenziale. In merito si esprime l'art. 7, par. 2, lett. c), d), *AI Act*[114].

Tali sistemi non sono, di per sé, vietati, ma il loro impiego è subordinato all'osservanza di determinati criteri obbligatori, che sono espressione, analogamente al *GDPR*, della logica dell'*accountability* che ispira anche l'*AI*

---

facendo riferimento alla sola finalità prevista, risulta, di per sé, incompatibile con il dinamismo intrinseco dei sistemi algoritmici, suscettibili di articolazioni che cambiano, di volta in volta, in ragione della variabilità, della complessità e della imprevedibilità computazionale. Si v. I. MARTONE, *Sulle potenzialità e sui rischi dell'attività algoritmica*, in AA.VV., *Intelligenza artificiale e piattaforme digitali: dalla co-regolamentazione alla co-vigilanza. Atti del Convegno 10-11 febbraio 2025. Università degli Studi di Perugia*, a cura di M. ANGELONE, C. COLOMBO, I. MARTONE, C. PERLINGIERI, A. VALONGO, *cit.*, p. 175.

[111] Il legislatore tratteggia, propriamente, un modello regolatorio rispondente al «paradigma dei diritti fondamentali». G. RESTA, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale*? , in *Dir. inf. e informatica*, 2022, par. 3, consultabile sul sito http://dejure.it. Sul tema, si v. G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Foro it.,* 2024, c. 208 ss.

[112] In questa categoria, rientrano i sistemi di manipolazione cognitivo- comportamentale, come pure quelli che consentono di attribuire un "punteggio sociale" (*social scoring*) per propositi pubblici e privati, classificando le persone in base al loro comportamento sociale o ai loro elementi distintivi personali; il regolamento proibisce l'uso di applicazioni di polizia predittiva, basate sulla profilazione e i sistemi che adoperino i dati biometrici per catalogare le persone, sulla base di fattori puntuali, quali la razza, la religione o l'orientamento sessuale, etc. Per la disamina critica delle «pratiche di intelligenza artificiale vietate», si v. S. ORLANDO, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, in *Persona e mercato*, 2022/3, 346 ss. Sulle tecniche subliminali si v. D. DI SABATO, G. ALFANO, *L'impiego dell'IA per condizionare e valutare le persone tra limitazioni e divieti: qualche considerazione critica sulla proposta di Regolamento sull'IA elaborata dalla Commissione europea*, in *Riv. dir. impresa*, 2022, p. 281 ss.

[113] Compongono tale categoria gli usi legati a infrastrutture critiche, istruzione e formazione professionale, occupazione, servizi pubblici e privati di base (ad esempio l'assistenza sanitaria, le banche, etc.), alcuni sistemi di contrasto, migrazione e gestione delle frontiere, giustizia e processi democratici (come nel caso di sistemi usati per influenzare le elezioni).

[114] Sul punto. C. SOLINAS, *op.ult.cit.*, p. 255.

Act[115]. Il legislatore europeo impone sia ai fornitori che sviluppano o fanno sviluppare i sistemi intelligenti, sia ai *deployers* che li utilizzano doveri di: valutazione, *ex ante*, dei rischi conosciuti e di quelli prevedibili; adozione di misure precauzionali per mitigarli; monitoraggio e aggiornamento, in via periodica, dei modelli di valutazione del rischio; impiego di misure idonee di gestione dei rischi che si presentino dopo che i sistemi siano stati immessi sul mercato[116]. I fornitori e i *deployers* dovranno, poi, essere in grado di dimostrare di aver assunto le misure prescritte, nell'ottica della loro "responsabilizzazione" e del dovere, su loro gravante, di "garantire" la congruenza del loro operato e dei sistemi intelligenti ai parametri legislativamente previsti.

L' *AI Act* disciplina, altresì, l'impiego di modelli di I.A. per "finalità generali", disponendo che, quando non comportino "rischi sistemici", saranno soggetti a parametri limitati sulla trasparenza, definiti dall'art. 53; qualora, viceversa, si tratti di modelli 'più potenti', rispetto ai sistemi ad alto rischio per finalità generali, che potrebbero procurare rischi sistemici, dovranno essere adempiuti anche altri doveri, come quelli di effettuare valutazioni dei modelli, di vagliare e mitigare tali rischi e di riferire in merito agli incidenti alle Autorità nazionali competenti, ai sensi dell'art. 55, par. 1, lett. c).

I sistemi intelligenti "a basso rischio" (come videogiochi o filtri *spam*) sono identificabili per esclusione, visto che non rientrano nelle due precedenti categorie e saranno esenti dai doveri fissati per quelli ad alto rischio: per essi, si incoraggia l'elaborazione di codici di condotta e si predispone unicamente la conformità a requisiti minimi di trasparenza, ai sensi dell'art. 50. Tale scelta è stata oggetto della censura che la normativa, nello statuire doveri di trasparenza «molto vaghi», sembra incidere «in maniera recessiva» su tale categoria, che, quantunque sia qualificata a "rischio limitato", include applicazioni che possono essere pericolose: si pensi ai rischi significativi che i videogiochi presentano per i bambini [117].

---

[115] A. C. NAZZARO, *La tutela dei dati biometrici tra GDPR e AI* ACT, in *EJPTL.,* 2024/ 2, p. 52, consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/index. Sul significato del principio di *accountability* nel regolamento sull'intelligenza artificiale, si v., ancor prima dell'emanazione della proposta da parte della Commissione europea, G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Anal.giur.econ.*, 2019, p. 182. L'A. auspicava l'adozione di modello legislativo di regolamentazione dell'intelligenza artificiale che fosse attuativo di tale principio, in considerazione della circostanza che la complessità, l'autonomia, l'opacità dei sistemi intelligenti e l'incertezza delle regole del loro funzionamento rendono i tradizionali paradigmi della responsabilità civile inefficienti, per garantire una tutela effettiva dei diritti e delle libertà fondamentali dei destinatari delle loro risoluzioni. Diversamente, secondo altra parte della dottrina, l'*AI Act* ha adottato un approccio basato sul rischio radicalmente diverso del *GDPR*: quest'ultimo si basa su un approccio "*bottom-up*", ove l'apprezzamento del rischio è conferito, in prima battuta, ad una valutazione decentralizzata del titolare del trattamento; al contrario, il primo ha prediletto un approccio *top-down*. È, difatti, il legislatore a identificare le tecnologie dell'intelligenza artificiale, a determinare le pratiche proibite e rischiose e ad individuare, *ex ante*, il diverso livello di rischio dal quale far discendere le regole applicabili, lasciando poco spazio alla valutazione dei destinatari delle stesse. Secondo tale ricostruzione, questo metodo implica il pericolo di elaborare delle categorie normative astratte che non rappresentino in modo congruo le caratteristiche ed i rischi delle tecnologie digitali emergenti. Si v. G. FINOCCHIARO, *Intelligenza artificiale. Quali regole, cit.*, pp. 121-122; G. RESTA, *op.cit.*, § 6. Per un approfondimento della questione, mi si consenta di rinviare a G. D'ALFONSO, *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules*, in *EJPLT*, 2022/2, p. 37 ss., consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/index

[116] P. FALLETTA, A. MARSANO, *op.cit*, p. 127.

[117] D. POLETTI, *Decisioni algoritmiche e diritto alla comprensione, abstract* della Relazione al convegno *"Gli Stati Generali del diritto di internet 2021*", p. 3, consultabile sul sito https://dirittodiinternet.it/atti-digitali-di-gli-stati-generali-del-diritto-di-internetluiss-161718-dicembre-2021-di-giuseppe-cassano-e-francesco-di-ciommo-direttori-scientifici-premessa-gli-atti-digitali-fanno

Il Regolamento stabilisce che i sistemi di intelligenza artificiale, dopo essere stati immessi nel mercato, devono essere controllati da una struttura di natura pubblica, al fine di garantire l'applicazione corretta ed uniforme della regolamentazione nell'Unione e, eventualmente, di intervenire repentinamente, qualora si realizzino rischi imprevisti[118]. A tal proposito, il legislatore europeo, tenendo conto della complessità e della trasversalità di tali sistemi, ha sancito un articolato assetto di *governance*, a livello sia europeo, sia nazionale[119].

Sul piano interno, si sono previsti strumenti di *enforcement*, attribuendo all'Autorità di sorveglianza nazionale poteri diretti ad assicurare la conformità ai parametri dei sistemi intelligenti e dei doveri imposti agli operatori. Ciascuno Stato membro deve istituire o designare almeno "un'autorità di notifica" e almeno "un'autorità di vigilanza del mercato". Le prime saranno responsabili di istituire e attuare le procedure imprescindibili per il vaglio e la notifica degli organismi di valutazione della conformità dei sistemi ad alto rischio e per il loro monitoraggio[120]. Le seconde saranno le Autorità nazionali competenti che dovranno esercitare i loro poteri in maniera indipendente, imparziale e senza pregiudizi, in modo tale da salvaguardare i principi di obiettività delle loro attività e dei loro compiti, promuovere un elevato livello di protezione dei diritti e delle libertà fondamentali e garantire l'applicazione e l'attuazione del regolamento (art. 70, par. 1). Gli Stati membri devono anche designare un'Autorità di vigilanza che funga da punto di contatto unico per l'*AI Act* (art. 70, par. 2).

A livello europeo, il Comitato europeo per l'intelligenza artificiale, costituito dai rappresentanti degli Stati membri e della Commissione europea, avrà il compito di raccogliere e condividere le migliori pratiche, di vigilare sull'applicazione della disciplina, nonché di facilitarne l'attuazione e di contribuire ad un'efficace coordinazione con le Autorità nazionali di sorveglianza e con la Commissione.

A quest'ultima sono stati affidati un ruolo nodale e poteri politici, conferendole numerosi compiti: dall'attuazione al monitoraggio della regolamentazione, dalla supervisione dei meccanismi di collaborazione alla partecipazione nell'ambito dei nuovi consessi di confronto istituiti *ex novo,* il controllo e il coordinamento del sistema di notifica degli Organismi notificati, etc.[121]. Di considerevole valenza è il potere di modificare l'Allegato III del Regolamento, relativamente all'elenco dei sistemi di IA ad alto rischio, riconosciuto, evidentemente, con il fine di realizzare un adeguamento e una maggiore coerenza tra le prescrizioni introdotte e le future evoluzioni tecnologiche.

---

[118] S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE- Rivista quadrimestrale*, 2024/2, pp. 4-7, consultabile sul sito https://www.aisdue.eu.

[119] L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. trim. dir. pubbl*, 2022, p. 1111 s. parla di un «sistema decentrato».

[120] Per un'analisi del tema si v. A. PALMA ORTIGOSA, *Quién es quién en el Reglamento Europeo de Inteligencia Artificial? Las autoridades notificantes y los organismos notificados*", in *Actualidad Juridica Iberoamericana*, 2024, n. 21, 598 ss.

[121] Sul punto si v. B. CAROTTI, *Le finzioni dell'intelligenza senza corpo, o dell'AI Act*, in *Giornale dir. amm.*, 2025, p. 38.

Il legislatore ha previsto, altresì, altri quattro organismi. L'Ufficio europeo per l'*IA* presso la Commissione, incaricato di sviluppare le competenze e le capacità dell'Unione in tale contesto- già istituito con decisione C/2024/390 della Commissione del 24 gennaio 2024-; il Consiglio per l'*IA* che compie consulenza e assistenza alla Commissione europea e agli Stati membri, con il fine di semplificare l'applicazione coerente ed efficace dell'*AI Act*; il *forum* consultivo, composto di *stakeholders*, il cui obiettivo è di offrire consulenza e competenze tecniche al Consiglio per l'*IA* e alla Commissione, contribuendo alle loro funzioni; il Comitato scientifico, ossia un gruppo di esperti scientifici indipendenti, con lo scopo di supportare le attività di esecuzione del regolamento.

Circa i poteri delle Autorità di vigilanza del mercato degli Stati membri[122], si consideri che le stesse potranno fornire orientamenti e consulenze sull'applicazione del regolamento, alla luce degli indirizzi del Comitato europeo per l'intelligenza artificiale e della Commissione europea (in special modo in favore delle piccole e medie imprese, comprese le *start up*), oltre che, a seconda dei casi, degli orientamenti e delle consulenze del Comitato scientifico.

In merito alla funzione ben più complessa di sorveglianza, si crede che, malgrado la maggior parte dei sistemi intelligenti non sia sottoposta a requisiti e doveri specifici, in quanto non categorizzati come "ad alto rischio", ciò nonostante, le Autorità di vigilanza del mercato potranno attuare misure in riferimento a tutti i sistemi che presentino un rischio conformemente al regolamento.

Le Autorità esercitano poteri di indagine che permettono di chiedere agli operatori informazioni e di accedere alla loro documentazione, di avere accesso a tutti i dati e alle informazioni rilevanti, tra le quali i *set* di dati di addestramento, convalida e prova impiegati dal fornitore e il codice sorgente del sistema intelligente[123].

In effetti, l'Autorità attiverà i poteri di controllo sui sistemi di intelligenza artificiale, al fine di valutare la loro corrispondenza ai parametri imposti dal regolamento o di sua iniziativa, se dovesse avere motivi sufficienti per ritenere che presentino un rischio per la salute, la sicurezza o per la tutela dei diritti fondamentali delle persone, oltre che per l'ambiente o la democrazia, ovvero in seguito alla ricezione di segnalazioni relative a gravi incidenti da parte dei fornitori di sistemi ad alto rischio, ai sensi dell'art. 73[124]; oppure su reclamo motivato presentato, ai sensi dell'art. 85, da parte di «qualsiasi persona fisica o giuridica» che abbia ragione di ritenere che vi sia stata un'inottemperanza delle norme dell'*AI Act*. Tale opportunità è da valutare molto positivamente, dato che si aggiunge ai rimedi giurisdizionali e amministrativi, miranti a garantire l'effettività del diritto ad un ricorso effettivo, riconosciuto dall'art. 47 della Carta dei diritti fondamentali UE.

Gli operatori saranno tenuti, secondo la logica dell'*accountability*, a dimostrare all'Autorità di vigilanza la rispondenza dei sistemi intelligenti al

[122] Per le osservazioni che seguono sui poteri di tali Autorità, si v. S. VILLANI, *op.cit.* pp.4-7; B. CAROTTI, *op.loc.ult.cit.*.

[123] L. TORCHIA, *op.cit.*, p. 1111 s.

[124] Di ciò l'Autorità di vigilanza dovrà informare gli organismi pubblici nazionali e la Commissione sulla base di quanto già statuito dagli artt. 19 e 20 del reg. 2019/1020/UE sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011.

regolamento. Se, poi, nel corso della valutazione effettuata, l'Autorità rileverà talune difformità, potrà esercitare poteri correttivi, adottando misure appropriate per far cessare la violazione, quali ammonimenti, fino a giungere al ritiro del sistema dal mercato o al richiamo per un tempo ragionevole, commisurato alla natura del rischio. Di tali azioni dovrà essere data comunicazione sia alla Commissione europea, sia agli altri Stati membri, per l'eventuale attivazione di corrispondenti misure di salvaguardia.

Se dovesse accadere che tali misure correttive non siano sufficienti, ai sensi dell'art. 99, le Autorità potranno irrogare sanzioni amministrative pecuniarie, applicabili nel caso di violazioni al regolamento, che dovranno essere «effettive, dissuasive e proporzionate». Il legislatore europeo, finanche in tale ambito, ha dato attuazione al principio di proporzionalità, nella prospettiva di dover valutare gli interessi dei fornitori di piccole o medie dimensioni e delle *start-up* e la loro sostenibilità economica.

L'*AI Act*, in modo speculare al *GDPR*, ha disegnato un assetto sanzionatorio che, impattando fortemente sul fatturato dei soggetti coinvolti, comprende sanzioni amministrative pecuniarie che variano a seconda della previsione contravvenuta e del tipo di violazione accertata [125]. Invero, all'Autorità di controllo è stato assegnato il potere di irrogare sanzioni pecuniarie con un ampio margine di discrezionalità: infatti, ai sensi dell'art. 99, l'Autorità esaminerà, caso per caso, l'*an* dell'irrogazione e il *quantum* dell'ammontare. Nel decidere se infliggere una sanzione e nel quantificarla, l'Autorità terrà conto di tutte le circostanze inerenti alla situazione specifica e, se del caso, di una serie di fattori, definiti dall'art. 99, par. 7, tra i quali: la natura, la gravità e la durata del mancato rispetto della normativa e delle sue conseguenze, valutando la finalità del sistema di *IA*, come pure, ove opportuno, il numero di persone interessate e il livello del danno da esse subito; il grado di responsabilità dell'operatore, analizzando le misure tecniche e organizzative attuate; il dolo o la colpa della violazione; l'eventuale azione intrapresa da costui per attenuare il danno subito dalle persone interessate. Tra gli elementi da controllare, si segnala il riferimento alla necessità di coordinamento con le Autorità di vigilanza del mercato di altri Stati membri, dovendosi verificare se hanno già applicato sanzioni amministrative pecuniarie al medesimo operatore per la stessa violazione (art. 99, par. 7, lett. b) e, significativamente, il richiamo alla circostanza che «altre autorità» abbiano già applicato sanzioni amministrative pecuniarie allo stesso operatore per l'inosservanza di altre prescrizioni del diritto dell'Unione o nazionale, quando tali infrazioni derivino dalla stessa attività o omissione che costituisce una violazione attinente al presente regolamento.

La norma ha portata molto rilevante e la si crede applicabile, per via di interpretazione logico-sistematica [126], anche in riferimento all'esercizio del potere sanzionatorio da parte delle Autorità di controllo della *privacy*.

---

[125] Per le considerazioni che seguono, si v. P. FALLETTA, A. MARSANO, *op.cit.*, p. 130.

[126] Eminente dottrina ha formulato un insegnamento ampiamente condiviso in tema di interpretazione logico-sistematica delle disposizioni normative. Si sostiene che, in ossequio al principio di legalità, ogni norma deve essere posta in «relazione dialogica» con il fatto da regolare e l'interpretazione di una previsione è il risultato del coordinamento con le altre norme dell'ordinamento giuridico e dell'armonizzazione con i principi costituzionali. Si supera, in tal modo, la tecnica della "sussunzione", in quanto il fatto non può più essere «meccanicamente incasellato» in una peculiare fattispecie astratta che, molte volte, non è neanche

Ancora, l'art. 99, par. 10, *AI Act* dichiara che l'esercizio dei poteri attribuiti alle Autorità di vigilanza sull'intelligenza artificiale è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale effettivo e il giusto processo. Donde, i provvedimenti sanzionatori adottati da queste ultime potranno essere sottoposti al sindacato delle Corti nazionali e, qualora ricorrano i presupposti, a quello della Corte di giustizia dell'Unione europea, tramite un rinvio pregiudiziale, nel rispetto dell'art. 47 della Carta dei diritti fondamentali UE.

In conclusione, il regolamento non fa alcun riferimento diretto alle questioni di responsabilità civile[127], ma è chiaro che l'osservanza di tali disposizioni preventive assumerà diretto valore, altresì, sul profilo risarcitorio.

Delineati i capisaldi dell'*AI Act*, si focalizzi, dapprima, l'attenzione sulla circostanza che il regolamento non si occupa della raccolta e del trattamento dei dati personali, i quali continuano ad essere regolati dalla normativa vigente e, in via principale, dal *GDPR*[128]. È, dunque, inevitabile che sia i fornitori, sia gli utenti debbano conformarsi alla regolamentazione applicabile ai dati e che l'ottemperanza alla stessa costituisce il vero substrato giuridico sul quale si fonda la liceità delle attività di sviluppo e di impiego dei sistemi di intelligenza artificiale[129].

Ne discende che, benché un sistema rispetti la disciplina dell'*AI Act*, sarà il *GDPR* a stabilire se esso potrà o meno essere alimentato con dati personali per l'addestramento e per il funzionamento effettivo: non potrà, così, essere messo in funzione e addestrato, finché non sia certa la conformità al Regolamento generale della *privacy*. In sostanza, le norme sui dati personali non permettono di iniziare alcun trattamento, prima di aver compiuto tutte le operazioni necessarie a garantirne l'osservanza. Il problema sussiste, specialmente, per le fasi di addestramento dei modelli di intelligenza artificiale, considerato che esso richiede l'uso di dati e, se sono personali, il loro utilizzo potrebbe essere illecito, allorché la loro elaborazione avvenga, nonostante la sicurezza del trattamento non sia sicura: potrebbe, difatti, esservi il pericolo che i dati personali usati nell'addestramento siano rivelati a terzi, in modo accidentale,

---

rinvenibile. Al fine di individuare la disciplina «più adeguata» al caso concreto, il fatto dovrà essere valutato prendendo in considerazione gli interessi ed i valori che esprime, tenendo conto del contesto storico-giuridico di riferimento. L'interprete ha, in definitiva, il compito non di garantire il rispetto della lettera della norma, quanto, viceversa, di individuare ed applicare al caso concreto la regola «più adeguata». Per tali argomentazioni, si v. P. PERLINGIERI, *Interpretazione ed evoluzione dell'ordinamento*, *Riv. dir. priv.*, 2011,160 ss. Si afferma che il «bilanciamento degli interessi e dei valori, ragionevolezza, adeguatezza, proporzionalità, valenza dei principi sono canoni ermeneutici (…) che, come tali, contribuiscono (insieme) al ridimensionamento di vecchi brocardi, duri a morire, come in *claris non fit interpretatio* e *dura lex sed lex,* che dovranno essere (…) conformi alla legalità costituzionale ed europea». Si v. P. PERLINGIERI, *Formazione dei giudici e Scuola superiore della magistratura*, in *Giusto processo civile,* 2007, 313. Sulla «ragionevolezza» quale «canone ermeneutico ed argomentativo», «filo conduttore» di ogni ragionamento giuridico, per il contemperamento di principi ed interessi, in coerenza col sistema giuridico di riferimento e tutti i suoi valori, cfr. G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile,* Napoli, 2015, pp. 16-29, 43,135.

[127] C. PERLINGIERI, *op.ult.cit.*, § 2 osserva che il regolamento lascia irrisolti taluni problemi, puntualmente sul piano rimediale, non tanto con riferimento alla necessità di costruire un nuovo modello di responsabilità, quanto in relazione all'individuazione di un modello idoneo di copertura dei danni che non sia riconducibile a meri meccanismi assicurativi. Sugli interventi normativi europei in materia della responsabilità civile algoritmica, mi si consenta di rinviare a G. D'ALFONSO, *Rischio da sviluppo scientifico- tecnologico nel nuovo quadro normativo europeo*, in *Persona e mercato* 2025/1, pp. 85-142.

[128] P. FALLETTA, A. MARSANO, *op.cit*, p. 126.

[129] Sul punto e per le riflessioni che seguono si v. E. PROSPERETTI, *op.cit.*, pp. 2, 17.

dal modello di IA risultante dall'addestramento stesso. L'*AI Act* prevede, pertanto, che i dati impiegati a tal fine siano raccolti e trattati in modo conforme al *GDPR*, con la conseguenza che, qualora vengano usati dati personali illeciti, la competenza sarà dell'Autorità garante della *privacy*.

D'altronde, l'*AI Act* opera, costantemente e continuamente, rinvii al *GDPR*, il quale assurge a «postulato logico-concettuale» della regolamentazione dell'intelligenza artificiale[130].

Un rinvio molto significativo è previsto dall'art. 26, par. 9, che stabilisce che i *deployers* dei sistemi ad alto rischio dovranno eseguire una valutazione di impatto sul trattamento dei dati personali, c.d. *DPIA*, ai sensi dell'art. 35 *GDPR*[131], oltre ad essere tenuti ad effettuare una valutazione di impatto sui diritti fondamentali, ai sensi dell'art. 27 *AI Act*. La c.d. *FRIA* è funzionale a valutare, *ex ante*, le categorie di persone fisiche e i gruppi verosimilmente interessati dall'uso del sistema, la sua congruenza al diritto europeo e nazionale in materia di diritti fondamentali e l'impatto che sia ragionevolmente prevedibile su tali diritti dal suo impiego. La *FRIA* è obbligatoria unicamente in riferimento ai sistemi ad alto rischio e deve essere effettuata soltanto da talune categorie di *deployers*, quali gli organismi di diritto pubblico e gli enti privati che forniscano servizi pubblici e dagli utilizzatori di sistemi, di cui all'allegato III.

In entrambi i casi, i *deployers* si avvarranno delle istruzioni loro comunicate dal fornitore, per informarli delle finalità previste e dell'impiego corretto dei sistemi.

A differenza della *DPIA* che è conservata dal titolare ed è esibita unicamente quando venga richiesta dall'Autorità di protezione dei dati personali, ad eccezione del caso in cui la si consulti preventivamente, ai sensi dell'art. 36; la *FRIA* è trasmessa dal *deployer* all'Autorità di vigilanza del mercato ed è, quindi, soggetta ad una conoscibilità anticipata[132].

---

[130] V. RICCIUTO, *op.ult.cit.*, p. 4, nota 26.

[131] L'art. 35, par. 1, *GDPR* regolamenta il *Data Protection impact assesment*, sancendo che il *data controller*, quando un tipo di trattamento presenti il rischio elevato per i diritti e le libertà delle persone fisiche, prima di procedere, dovrà compiere una valutazione di impatto sulla protezione dei dati personali. La valutazione della gravità del rischio sarà effettuata tenendo conto di una serie di circostanze, quali l'ambito (vale a dire la natura, l'oggetto, il contesto e le finalità del trattamento) e i mezzi impiegati, tra i quali vi è un riferimento espresso all'utilizzo delle nuove tecnologie. Nel vaglio dei rischi del trattamento, è fondamentale, dapprima, individuare gli eventi temuti e valutarli in termini di gravità e probabilità. Se essi ricorrono, allora il titolare dovrà implementare tutte le precauzioni che siano, non tanto utili, quanto "adeguate" in base alla natura dei dati personali e ai rischi del trattamento, al fine di salvaguardare la sicurezza dei dati stessi e, più precisamente, prevenire l'accesso non autorizzato, la loro alterazione o perdita, ai sensi degli artt. 5 e 32. L'art. 35, par. 2 dispone che il titolare del trattamento, allorquando svolga una *DPIA*, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno. La valutazione d'impatto sulla protezione dei dati personali non è sempre obbligatoria, ma dovrà essere effettuata da parte di tutti i titolari dei trattamenti solo se ricorrano i presupposti descritti. Quando sussista l'obbligo e il titolare del trattamento non provveda, l'Autorità di vigilanza irrogherà una sanzione, ai sensi dell'art. 83. Si v. E. M. TRIPODI, *AI Act e GDPR. Assonanze e dissonanze*, in *Diritto di internet*, 2024, p. 622 ss.

[132] D'altra parte, appare evidente che le due procedure di valutazione sono ben diverse, dato che, mentre la *DPIA* attiene all'impatto dei trattamenti 'previsti' dei dati personali, la *FRIA* concerne la tutela dei diritti e delle libertà fondamentali delle persone, unicamente in relazione al rischio presunto correlato all'impiego del sistema intelligente. Ad oggi, non è facile comprendere quanto tale distinzione terminologica sia, poi, traducibile in una differenza dal punto di vista del contenuto e della responsabilità; ciò che sicuro è che gli elementi oggetto di valutazione individuati dall'art. 35, par. 7, *GDPR* sono ben differenti da quelli desumibili dall'art. 27 dell'*AI ACT*. Si v. A. C. NAZZARO, *op.ult.cit.*, p. 52.

Per di più, l'*AI Act* sancisce una serie di disposizioni specifiche in materia di trattamento dei dati personali che dovranno essere rispettate dagli operatori del settore, per uniformarsi alla normativa sull'intelligenza artificiale.

Precipuamente, premesso che la qualità, la rappresentatività e la *governance* dei dati non sono fattori accessori, ma condizioni strutturali senza le quali l'IA non è affidabile, non è ripetibile e non è scalabile in modo sicuro, l'*AI Act* attribuisce un rilievo determinante ai dati[133]. Richiede, perciò, *dataset* di addestramento di alta qualità, rappresentativi e privi di distorsioni discriminatorie e prescrive che siano impiegati secondo pratiche rigorose di *governance* e gestione di dati. Di fatto, dalla loro qualità deriva la qualità del risultato.

I *deployers* di sistemi ad alto rischio sono, altresì, tenuti a seguire le istruzioni per l'uso predisposte dal loro fornitore, ad assicurare la correttezza dei dati di *input* per mezzo dei quali alimentarli, a controllarne il funzionamento e a segnalare eventuali rischi ed incidenti al fornitore, oltre che a conservare i *log* dei sistemi di cui si avvalgono[134].

Concludendo, si richiami il considerando 69 *AI Act* che prevede che il diritto alla vita privata e alla protezione dei dati personali devono essere garantiti durante l'intero ciclo di vita del sistema intelligente. Saranno, per tale ragione, applicabili i principi della minimizzazione dei dati e della *privacy by design* e *privacy by default*, ai sensi dell'art. 25 *GDPR*[135]. I fornitori, ai fini di garantire l'osservanza di tali principi, potranno adottare misure quali l'anonimizzazione e la cifratura, ma anche l'utilizzo di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi intelligenti, senza trasmettere tra le parti o copiare degli stessi dati grezzi o strutturati, fatti salvi i requisiti in materia di *governance* dei dati di cui all'*AI Act*.

Alla luce di quanto argomentato, si constati che - come sancito dal considerando 10, che fa salvi i compiti ed i poteri delle Autorità garanti della *privacy*-, ogni qualvolta si pongano questioni attinenti alla corretta applicazione, nell'ambito delle logiche dell'intelligenza artificiale e dei processi algoritmici, delle norme relative alla raccolta, al trattamento e alla cancellazione e, in generale, alla circolazione dei dati personali, spetterà a suddette Autorità nazionali ed europee il compito di esercitare i propri poteri di vigilanza[136]. Tali Autorità hanno una competenza orizzontale su ogni aspetto

---

[133] Sul punto e per le notazioni che seguono, si v. F. BARTOLOMEO, *op.cit.,* p. 1, s. Autorevole dottrina osserva il bisogno di garanzia della veridicità e dell'aggiornamento degli algoritmi e, più esattamente, della qualità dei dati che confluiscono in essi, allo scopo di impedire che informazioni non corrette possano condurre ad elaborazioni errate. Si v. P. PERLINGIERI, *Sul trattamento algoritmico dei dati, cit.,* p. 182.

[134] P. FALLETTA, A. MARSANO, *op.cit.,* p. 126.

[135] *Privacy by design*, protezione dei dati fin dalla progettazione e *privacy by default*, protezione dei dati per impostazione predefinita sono due principi chiave, formulati dall'art. 25 *GDPR*, per garantire la protezione dei dati personali. Il primo implica che il titolare del trattamento debba effettuare la valutazione del rischio al momento della progettazione del sistema, quindi prima che il trattamento inizi. Il secondo comporta che, per impostazione predefinita, i titolari debbano trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Si concretizza, in tale maniera, il principio di minimizzazione dei dati che impone di progettare il sistema di trattamento, garantendo la non eccessività di quelli raccolti. Sulla *privacy by design* e *privacy by default*, si v. F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in AA.VV., *I dati personali nel diritto europeo, op.cit.*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *cit.*, 789 ss.

[136] Sul punto e per le argomentazioni che seguono, si v. V. RICCIUTO, *AI Act, diritto dell'Unione e diritto nazionale, cit.*, p. 97

che concerna il trattamento dei dati personali, quand'anche lo stesso sia realizzato per mezzo degli algoritmi, come pure laddove alimenti processi di IA. Ciò implica che il fenomeno dell'intelligenza artificiale potrà essere indagato, in linea di massima, su diversi piani: dalle Autorità di controllo di cui al *GDPR*, per quanto concerne il trattamento dei dati personali e dalle Autorità di vigilanza di cui all'*AI Act*, relativamente alla corretta circolazione nel mercato dei sistemi intelligenti.

Eppure, a ben vedere, la vigilanza di tali sistemi racchiude, anch'essa, profili di valutazione del trattamento dei dati personali e degli algoritmi, come emerge, in modo particolare, dalla lettura dell'art. 10 *AI Act* che regolamenta i «dati e la *governance* dei dati». Donde, le Autorità preposte alla sorveglianza sull'applicazione del regolamento possono assumere un ruolo nel controllo del trattamento algoritmico dei dati personali svolto dai fornitori e/o dai *deployers* di sistemi intelligenti[137].

Detto ciò, appare chiaro che, per garantire il corretto funzionamento del complessivo sistema di *governance*, è fondamentale un idoneo coordinamento tra le azioni delle Autorità Garanti della *privacy* e delle Autorità di vigilanza del mercato, come pure con quelle svolte dai Coordinatori di servizi digitali, quando i gestori delle piattaforme *online* utilizzino gli algoritmi e l'intelligenza artificiale nella fornitura dei servizi digitali e nell'adozione di processi decisionali per la moderazione di contenuti pubblicati dagli utenti del servizio[138].

Può ben comprendersi che possono verificarsi sovrapposizioni di competenze, nell'esercizio delle proprie funzioni, oltre che tra l'Autorità di vigilanza del mercato dell'IA e le Autorità di controllo della protezione dei dati personali, anche tra la prima e il Coordinatore dei servizi digitali, in ragione del fatto che il considerando 119 *AI Act* riconosce che l'intelligenza artificiale può essere utilizzata per fornire "servizi intermediari" o parte di essi, come quelli indicati nell'art. 3 del *DSA* e il considerando 118 *AI Act* dispone che, in tal caso, il fornitore o il *deployer* di sistemi di IA dovrà conformarsi, oltre che a quest'ultimo, altresì, alla disciplina del *DSA*[139].

A questo proposito, densa di significato è la previsione dettata dall'art. 77, par. 1, *AI Act* in riferimento ai «poteri delle autorità che tutelano i diritti fondamentali», secondo la quale «le autorità o gli organismi pubblici nazionali 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 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 strumentale all'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione. L'autorità pubblica o l'organismo pubblico pertinente informa l'autorità di vigilanza del mercato dello Stato membro interessato di qualsiasi richiesta in tal senso».

---

[137] C. SOLINAS, *op.ult.cit.*, p. 255.

[138] V. RICCIUTO, *AI Act, diritto dell'Unione e diritto nazionale*, *cit.*, p. 97 s. Sulle ragioni che impongono il coordinamento tra il *DSA* e l'*Artificial intelligence Act*, si v. S. TOMMASI, *Digital Services Act e Artificial Intelligence Act: tentativi di futuro da armonizzare*, in *Persona e mercato* 2023/2, p. 283 ss.

[139] E. GIOMI, *Deepfake e propaganda: quali poteri ha Agcom sulle piattaforme*, consultabile al sito https://www.agendadigitale.eu/, 22.12.2025

Tale norma tocca un aspetto rimarchevole delle possibili sovrapposizioni tra le attività delle differenti Autorità di vigilanza nell'esercizio dei propri compiti, ma non è risolutiva.

Sarebbe, dunque, imprescindibile, nella designazione delle Autorità di vigilanza del mercato a livello nazionale, la previsione di una *governance* istituzionale che sia in grado di gestire l'unitarietà del fenomeno del trattamento algoritmico dei dati personali nel contesto dei sistemi intelligenti e di rappresentare un riferimento esclusivo dello stesso[140].

4.1. Il sistema di governance nella l. 132/2025. Raffronto con la legislazione spagnola e francese.

In riferimento alla *governance* a livello nazionale, l'art. 70 dell'*AI Act*, nell'imporre agli Stati membri l'istituzione o la designazione di una o più Autorità nazionali competenti, con funzioni di vigilanza del mercato e della corretta applicazione della normativa, ha statuito -rinviando espressamente al sistema istituito dal regolamento 2019/1020/UE- che gli stessi possono decidere se creare un'Autorità di controllo *ad hoc* oppure affidare le relative funzioni e responsabilità ad un'Autorità indipendente già esistente[141]. Agli Stati membri è stata conferita l'opzione di decidere di nominare qualsiasi tipo di entità pubblica, in linea con le loro specifiche caratteristiche ed esigenze organizzative nazionali**.** In ogni modo, come già detto, le Autorità dovranno agire «in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti nell'applicazione e attuazione del regolamento», *ex* art. 70 par. 2 *AI Act*. In realtà, il rinvio legislativo a tali parametri è congruente con i compiti attribuiti alle Autorità che, pur non essendo organi giurisdizionali, saranno legittimate ad esercitare poteri di indagine e correttivi. Vieppiù, il carattere imparziale delle Autorità di vigilanza è correlato al primario intento del regolamento di promuovere un elevato livello di protezione dei diritti fondamentali che potrebbero essere lesi dai sistemi di IA.

In tal guisa, si è seguita la proposta iniziale della Commissione europea di non imporre agli Stati membri la designazione dei Garanti della *privacy* (c.d. *DPA*) quali Autorità competenti per il settore dell'intelligenza artificiale.

Diversa è stata la posizione assunta dal Comitato europeo per la protezione dei dati personali, c.d. *EDPB*, che, con la Dichiarazione del 16 luglio 2024, n. 3 -che richiama il Parere congiunto del medesimo e del Garante europeo per la protezione dei dati personali del 18 giugno 2021, n. 5-, ha espresso il proprio parere sul ruolo delle Autorità garanti della *privacy* nell'impianto regolatorio dell'*AI Act*[142].

L'*EDPB* è partito dalla premessa che il trattamento di dati personali coinvolge l'intero ciclo di vita dei sistemi intelligenti, specialmente di quelli ad alto rischio e che esso è (e continuerà ad essere) un elemento centrale delle

[140] Si mutuano le considerazioni di V. RICCIUTO, *op.ult.cit.*, p. 98 s., il quale afferma la necessità di gestire l'unitarietà del rapporto tra persona e mercato nel fenomeno dell'*AI*, sottolineando la carenza dell'approccio nazionale sulla *governance* dello stesso.
[141] Sul punto e per le osservazioni che seguono, si v. S. VILLANI, *op.cit.*, p. 3.
[142] Entrambi i provvedimenti sono pubblicati in https://www.edpb.europa.eu/

diverse tecnologie coperte dalla definizione di cui all'art. 3, n. 1, *AI Act*. Ha, poi, rilevato che, di conseguenza, il regolamento dovrà essere oggetto di interpretazione logico-sistematica e che lo si dovrà coordinare con i provvedimenti che, insieme al *GDPR*, sono intesi quali atti della "Normativa *Privacy*"[143], i quali, a loro volta, dovranno essere considerati e interpretati come strumenti complementari, in grado di rafforzarsi reciprocamente.

Il parere ha, altresì, puntualizzato la necessità di attribuire un ruolo preminente alle Autorità garanti della *privacy* nella *governance* dell'*AI Act*, riconoscendo la loro esperienza e competenza maturate, negli ultimi anni, nei numerosi interventi in materia di trattamento algoritmico dei dati personali. Tale presa di posizione si è fondata su una serie di circostanze: in primo luogo, le *DPA* sono esperte, oltre che delle tecnologie delle intelligenze artificiali, in molti ambiti elencati dall'art. 70, par. 3, *AI Act* -quali quello dell'elaborazione e della sicurezza dei dati e quello della valutazione dei rischi per i diritti fondamentali posti dalle nuove tecnologie-; in secondo luogo, il regolamento (art. 74, par. 8) ha riservato alle *DPA* taluni compiti, stabilendo che gli Stati membri dovranno designarle come Autorità di vigilanza del mercato per alcune categorie di sistemi di IA ad alto rischio: quelli rientranti nel settore della biometria, nella misura in cui siano usati per attività di contrasto, gestione delle frontiere, giustizia e democrazia; quelli elencati nell'Allegato III, punti 6, 7 e 8, impiegati nell'attività di contrasto, nella migrazione, nell'asilo e nella gestione del controllo delle frontiere, nell'amministrazione della giustizia e nei processi democratici; si è, finanche, precisato che vi è un legame stretto tra la valutazione d'impatto sui diritti fondamentali, *ex* art. 35 *GDPR* e la valutazione d'impatto sulla protezione dei dati personali, *ex* art. 27 *AI Act*.

Per queste ragioni, l'*EDPB* ha raccomandato agli Stati membri di prendere in considerazione di designare le *DPA* quali Autorità di vigilanza del mercato dell'intelligenza artificiale altresì per i sistemi ad alto rischio operanti nei settori elencati nell'Allegato III del regolamento, diversi da quelli definiti nell'art. 74, par. 8.

La raccomandazione ha notevole valore nei casi in cui tali sistemi siano in grado di impattare sui diritti e sulle libertà degli interessati, per quanto riguarda il trattamento dei dati personali, escludendo quei settori dove l'*AI Act* prevede come obbligatoria la nomina di un'Autorità specifica. A tale riguardo, l'art. 74, par. 6, *AI Act* prescrive che, per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari regolamentati dal diritto dell'Unione in materia di servizi finanziari, l'Autorità di vigilanza del mercato, ai fini del regolamento stesso, è l'Autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti, secondo quanto previsto in ambito europeo, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema intelligente siano direttamente collegati alla fornitura di tali servizi finanziari.

[143] Si richiamano il Regolamento 1725/2018/UE, che concerne la protezione delle persone fisiche per quanto attiene al trattamento dei dati personali da parte delle istituzioni, organi e organismi dell'Unione Europea; la Direttiva 680/2016/UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, oltre che alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; oltre che la Direttiva 58/2002/CE, c.d. "Direttiva *e-Privacy*".

L'*EDPB* ha anche sostenuto che le *DPA*, in qualità di Autorità di vigilanza del mercato, dovrebbero essere designate quale punto di contatto unico per il pubblico e per le controparti degli altri Stati membri e dell'Unione. Ciò permetterebbe di avere un approccio unificato, coerente ed efficace nei diversi contesti di applicazione dell'intelligenza artificiale.

Da ultimo, l'*EDPB* ha insistito sull'esigenza di promuovere e predisporre un'adeguata ed efficace collaborazione tra tutte le Autorità coinvolte, individuando procedure chiare, in conformità al principio di leale cooperazione, dettato dall'art. 4, par. 3, del Trattato dell'Unione europea[144], come richiamato dalla Corte di Giustizia UE, nella pronuncia del 4. 7. 2023, C-252/21, relativa al *leading case Meta Platforms e a.*, cit., sul quale si tornerà *infra*.

Tale coordinamento non dovrebbe riguardare solo le *DPA*, ma dovrebbe avvenire anche tra le *DPA* e la Commissione europea e l'Ufficio dell'IA.

In conclusione, l'*EDPB* ha dichiarato che tali riflessioni riguardano, altresì, i modelli di IA per "finalità generali", i quali potrebbero essere addestrati su dati personali e i cui *output* sono in grado di incidere sui diritti della *privacy* e della protezione dei dati personali. Si è rimarcato, difatti, che l'*AI Act* non ha tracciato una chiara coordinazione tra l'Ufficio dell'IA e le *DPA* e/o lo stesso *EDPB* e che, in tali casi, è, al contrario, necessario un raccordo, ogni qual volta un modello di intelligenza artificiale "per finalità generali" comporti il trattamento di dati personali, ricadendo automaticamente sotto la supervisione delle *DPA*.

Le raccomandazioni dell'*EDPB* non state seguite né dall'Italia, né dalla maggioranza degli Stati membri.

La Spagna è stato il primo Paese ad istituire l'Autorità di vigilanza del mercato dell'IA, ponendosi in anticipo rispetto all'entrata in vigore del regolamento e collocandosi in una posizione di avanguardia nella cornice europea.

Il 2 settembre 2023, in applicazione di quanto previsto dalla legge di Bilancio generale dello Stato per l'anno 2022 (*Ley* 28. 12. 2021, n. 22), è stato pubblicato, sul *Boletin Oficial del Estado*, il Real Decreto del 22. 8. 2023 che ha approvato lo statuto dell'*Agencia Española de Supervisión de Inteligencia Artificial* (c.d. *AESIA*).

L'*AESIA* è responsabile dell'intera materia dell'intelligenza artificiale e, specificamente, della corretta implementazione dell'*AI Act*.

La scelta della Spagna è stata di istituire un'Autorità indipendente e di non conferire le competenze previste dal Regolamento ad un'Autorità già esistente e, in special modo, all'Autorità di controllo della protezione dei dati personali.

In merito alla natura giuridica dell'Autorità, si osservi che la stessa fa capo al Ministero degli Affari economici e della Trasformazione digitale, attraverso il Segretario di Stato sulla Digitalizzazione e Intelligenza Artificiale (al quale spetterà il ruolo di Presidente) e che sarà dotata di personalità giuridica pubblica, autonomia finanziaria e di gestione, per svolgere le proprie funzioni. L'*AESIA* agirà con piena indipendenza organica e funzionale dalle Pubbliche Amministrazioni, ispirandosi ai principi di interesse generale, autonomia, indipendenza tecnica e trasparenza, efficacia ed efficienza, uguaglianza e

[144] Sul principio di leale cooperazione tra gli Stati membri, si veda P. DE PASQUALE, *Commento all'art. 4 TUE*, in *Trattati dell'Unione europea*, a cura di A. TIZZANO, Torino, (II ed.), 2014, 28 ss.; F. CASOLARI, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020.

collaborazione interistituzionale- svolgendo azioni proprie di coordinamento con altre Autorità competenti e azioni di sostegno alle entità private[145].

L'Agenzia avrà compiti di: supervisione dell'implementazione, dell'utilizzo o della commercializzazione di sistemi che includono l'intelligenza artificiale e, più esattamente, di quelli che possono determinare rischi significativi per la salute, la sicurezza, la parità di trattamento e la non discriminazione, in modo peculiare tra donne e uomini, ed in relazione ad altri diritti fondamentali; promozione di test per i sistemi intelligenti, al fine di rafforzare la protezione degli utenti ed evitare pregiudizi discriminatori; sensibilizzazione, diffusione e promozione dello sviluppo e dell'uso responsabile, sostenibile e affidabile dell'IA; definizione dei meccanismi di consulenza e di servizio per la società e altri attori collegati all'implementazione e all'impiego della stessa; collaborazione con le altre Autorità, nazionali e sovranazionali, per la vigilanza sull'IA. In sostanza, l'Agenzia sarà tenuta a ridurre al minimo i rischi che potrebbero discendere dall'utilizzo dell'intelligenza artificiale, provando ad assicurare anche il suo corretto sviluppo e potenziamento[146].

Nell'esercizio delle proprie funzioni, l'Agenzia eserciterà poteri ispettivi, di verifica, correttivi e sanzionatori, nonché poteri di: sostenere lo sviluppo e l'uso di sistemi intelligenti in una doppia prospettiva ambientale e sostenibile, con il proposito di rafforzare le sinergie tra la transizione digitale e quella ecologica, per realizzare modelli più sostenibili; in un'ottica di genere, incorporare il principio delle pari opportunità tra donne e uomini nella progettazione, messa in servizio e impiego dei sistemi intelligenti, con lo scopo di rimuovere pregiudizi discriminatori di qualsiasi tipo, specialmente quelli di genere e di natura etnico-razziale; apporto a consolidare la fiducia nella tecnologia e nell'applicazione dell'intelligenza artificiale, creando un quadro di certificazione volontaria per i soggetti privati che permetta di offrire garanzie sulla progettazione responsabile di soluzioni digitali e assicurare standard tecnici, impedendo un'eccessiva regolamentazione e consentendo l'innovazione.

Permarranno immodificati i poteri del Ministero della Salute e dell'Agenzia spagnola per quanto attiene ai medicinali e ai prodotti sanitari, oltre che quelli del Ministero del Lavoro e dell'Economia Sociale e dell'Ispettorato del Lavoro e della Previdenza Sociale.

Diversa è stata la scelta della Francia che non ha istituito un organo nuovo *tout court*, appositamente deputato a svolgere le funzioni di Autorità di vigilanza del mercato[147]. Il 31 gennaio 2025, a pochi giorni dall'inizio del vertice mondiale sull'IA, svoltosi il 10 e l'11 febbraio 2025, è stato creato l'*Institut national pour l'évaluation et la sécurité de l'intelligence artificielle* (c.d. *Inesia*) che avrà il compito di garantire la sicurezza dei sistemi intelligenti, esercitando il controllo del loro impiego in settori sensibili (come la salute, l'istruzione, l'industria e l'informazione), oltre che di contribuire a prevenire i rischi sistemici

[145] Si v. P. FALLETTA, A. MARSANO, *op.cit.*, 131 s.; M. ANGELONE, *Crisi e regolazione «indipendente» dei mercati*, in *Diritto e processo amministrativo*, 2023, 815, nota 99.
[146] Per tali considerazioni si v. A. LOMBARDI, *La Spagna vara l'Agenzia per la supervisione dell'IA: poteri e obiettivi*, consultabile sul sito https://www.agendadigitale.eu/, 5 settembre 2023.
[147] Per le riflessioni che seguono, si v. https://www.ice.it/, 14 marzo 2025.

legati alle intelligenze artificiali, sostenendo contemporaneamente l'innovazione.

Lo Stato francese ha, pertanto, confermato il suo impegno a favore di uno sviluppo controllato dell'IA in un contesto di fiducia e sicurezza. Tale iniziativa si inserisce nell'ambito degli impegni assunti, nel maggio 2024, con la Dichiarazione di Seoul per un'IA sicura, innovativa e inclusiva, di cui la Francia è firmataria.

L'*INESIA* non avrà un proprio bilancio, né proprie risorse umane, né trarrà vantaggio da una nuova struttura giuridica separata, con la conseguenza che non avrà i poteri di un ente regolatore, ma, diversamente, un compito di vigilanza. Il ruolo dell'autorità sarà, cioè, di coordinare e strutturare la ricerca e la valutazione in materia di sicurezza dell'intelligenza artificiale e non sarà qualificabile come nuova entità giuridica. Tant'è vero che riunisce le principali istituzioni francesi già impegnate in tale contesto, quali: l'*Agence nationale de la sécurité des systèmes d'information*, l'*Institut national de recherche en informatique et en automatique*, il *Laboratoire National de Metrologie et d'Essai* e il *Pôle d'Expertise de Régulation Numérique*.

Il nuovo Istituto sarà gestito congiuntamente dal *Secrétariat général de la défense et de la sécurité nationale* e dalla *Direction générale des Entreprises*- che è la direzione della pubblica amministrazione francese e fa capo al Ministero dell'Economia e delle Finanze.

In Italia, dapprima, il Garante della *Privacy* aveva rivendicato il proprio ruolo privilegiato nell'attuazione dell'*AI Act*, nella "Segnalazione al Parlamento e al Governo sull'Autorità per l'Intelligenza Artificiale" del 25 marzo 2024 [148]. L'Autorità di controllo della *privacy* è partita dalla considerazione che l'*AI Act* si fonda sull'articolo 16 del Trattato sul funzionamento dell'Unione europea – che è la base giuridica della normativa di protezione dei dati – e che lo stesso Regolamento prevede la vigilanza delle *DPA* sui processi algoritmici che utilizzano dati personali. In aggiunta, ha sostenuto che, di conseguenza, codeste Autorità sono effettivamente destinatarie di una riserva di competenza fissata dall'*AI Act* e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori complessi, come quello delle attività di contrasto. Il Garante della *privacy* ha, quindi, motivato la sua «autocandidatura» [149] con la dichiarazione di possedere i requisiti di competenza e, assieme, di indipendenza necessari per garantire un'attuazione dell'*AI Act* coerente con l'obiettivo di garanzia di un livello elevato di protezione dei diritti fondamentali nel ricorso all'intelligenza artificiale. L'Autorità ha anche sottolineato che tale scelta implicherebbe, altresì, una semplificazione sul piano dell'effettività della tutela dei destinatari degli *output* dei sistemi intelligenti, visto che potrebbero rivolgersi ad un'unica Autorità per questioni concernenti i sistemi che trattino dati personali, senza il rischio di conflitti di competenza o di duplicazione di oneri amministrativi.

Con tutto ciò, la legge italiana del 23.9.2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", entrata in vigore il

[148] Per le notazioni che seguono, si v. P. FALLETTA, A. MARSANO, *op.cit.*, 132.
[149] B. CAROTTI, *op.cit.*, p. 39.

10.10.2025 [150] -che ha anticipato l'applicazione del regolamento europeo, integrandolo con alcune previsioni in settori caratteristici-, all'art. 20, ha designato, quali Autorità nazionali, due agenzie già operanti nel nostro ordinamento giuridico, ovverosia l'Agenzia per l'Italia digitale (c.d. all'AgID) e l'Agenzia per la cybersicurezza nazionale (c.d. ACN)[151]. Prima di definirne le rispettive competenze, si evidenzi che resta ferma l'attribuzione alla Banca d'Italia, alla Consob e all'Ivass del ruolo di Autorità di vigilanza del mercato secondo quanto statuito, in materia di operatori finanziari, dall'articolo 74, par. 6, *AI Act*.

All'AgID, qualificata come Autorità di notifica, è assegnato il compito di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, oltre che di esercitare le funzioni in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi intelligenti. La stessa è chiamata ad agire in base alle competenze maturate nel contesto di applicazione del Codice dell'amministrazione digitale e dell'adozione di linee guida di natura meramente tecnica.

L'ACN, come Autorità di vigilanza del mercato e punto di contatto unico con le Istituzioni dell'Unione europea, *ex* art. art. 70, par. 2, *AI Act*, svolgerà una funzione che esprime lo stretto collegamento tra l'impiego di sistemi intelligenti e la cybersicurezza. Più precisamente, le sono conferiti il compito di sorvegliare i sistemi di IA, nell'esercizio del quale potrà compiere attività ispettive e sanzionatorie, secondo quanto previsto dalla disciplina nazionale e dell'Unione europea; come pure i compiti di promozione e sviluppo dell'IA, relativamente ai profili di cybersicurezza.

Le due Agenzie (ciascuna secondo la pertinente competenza) devono garantire l'istituzione e la gestione congiunta di spazi di sperimentazione, sentito il Ministero della difesa per gli aspetti relativi ai sistemi intelligenti impiegabili «in chiave duale» e il Ministero della giustizia per i modelli e i sistemi applicabili all'attività giudiziaria.

L'art. 24, che ha delegato il Governo a adottare, entro un anno dall'entrata in vigore della nuova legge, uno o più decreti legislativi per l'adeguamento della normativa nazionale all'*AI Act*, ha previsto, tra i principi e criteri direttivi, l'attribuzione ad AgID e ACN dei poteri di vigilanza, ispettivi e sanzionatori previsti dall'*AI Act* per la verifica dell'osservanza del regolamento e della sua regolamentazione attuativa.

La legge stabilisce che deve essere istituito un Comitato di coordinamento, composto dai direttori generali delle due Agenzie e dal Capo del dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, volto a fornire ausilio al coordinamento e alla collaborazione delle due Agenzie tra loro e con le altre pubbliche amministrazioni e Autorità indipendenti. Si prevede, difatti, che al Comitato partecipino rappresentanti di vertice della Banca d'Italia, della Consob e dell'Ivass, quando siano trattate questioni ricadenti nella rispettiva competenza di tali enti.

---

[150] Per un commento, si v. A. AMIDEI, *Pubblicata in GU la legge 23 settembre 2025, n. 132 recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale",* in *Persona e Mercato* 2025/1, pp. 1016 ss.

[151] Per le argomentazioni che seguono sul riparto delle competenze delle due agenzie, si v. Dossier 19 giugno 2025. "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", consultabile sul sito https://www.senato.it/

Il Nucleo per la Cybersicurezza sarà composto anche da un rappresentante dell'AgID.

Di fondamentale portata è l'art. 20, comma 4 che preserva i compiti, i poteri e le competenze sia del Garante della *privacy*, sia dell'Autorità per le Garanzie nelle Comunicazioni, quale Coordinatore dei Servizi Digitali.

Si crede[152] che la scelta di affidare all'AgID e all'ACN il potere di vigilanza in materia di intelligenza artificiale sia espressione della visione strategica del Governo italiano imperniata sull'efficacia e sull'efficienza nella *governance* dell'IA, considerato che le due agenzie hanno competenze tecniche complementari e altamente specializzate, che sono da considerarsi fondamentali per affrontare le sfide poste dall'IA in ambito di cittadinanza, industria, sicurezza, protezione dei dati personali e sicurezza nazionale, proprio come per garantire l'integrazione con il sistema digitale nazionale, già in possesso dell'AgID e dell'ACN.

Sotto un altro punto di vista, entrambe le agenzie sono soggette alle funzioni di indirizzo e coordinamento della Presidenza del Consiglio. Il Governo italiano è, evidentemente, intenzionato ad assicurarsi un certo grado di orientamento dello sviluppo del settore.

In sostanza, la norma testimonia la decisione del legislatore italiano di non attribuire il ruolo di Autorità di vigilanza del mercato e di Autorità di notifica a una o più Autorità indipendenti, quali il Garante della *privacy*, se non l'Autorità per le Garanzie delle comunicazioni, quanto, invece, ad agenzie dotate di spazi minori di indipendenza politica[153].

Tale approccio non è condivisibile, dacché l'individuazione dell'AGID e dell'ACN, enti governativi di diritto pubblico, quali Autorità nazionali per l'intelligenza artificiale, crea un attrito tra la legge italiana e la logica sottesa all'*AI Act*, intervento normativo preordinato anche alla protezione dei diritti fondamentali[154]. Sarebbe stato «più coerente ed opportuno» optare per una o più Autorità amministrative indipendenti, poiché tale impostazione avrebbe assicurato un più elevato livello di tutela per i diritti dei singoli ed evitato sovrapposizioni di competenze prevedibili, specialmente con il Garante per la protezione dei dati personali[155].

---

[152] Si condividono le osservazioni di B. CAROTTI, *op.cit.*, p. 39; P. FALLETTA, A. MARSANO, *op.cit.*, p. 132.

[153] A. AMIDEI, *op.cit.*, p. 1018.

[154] Sul punto e per le considerazioni che seguono, si v. G. RESTA, G.M. RICCIO, *Il ddl AI è legge: primi spunti di riflessione*, in www.altalex.com, 18 settembre 2025, consultabile al sito https://www.altalex.com/documents/2025/09/18/ddl-legge-primi-spunti-riflessione

[155] D'altronde, la Commissione europea, nel corso di svolgimento dell'*iter* legislativo dell'iniziale disegno di legge "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" (A.C. 2316-A), il 5 novembre 2024, avvalendosi di un potere ad essa conferito dalla Direttiva 2015/1535/UE - mirante a tutelare lo spazio unico europeo anche rispetto all'attuazione da parte degli Stati membri delle regole europee nel settore delle regolamentazioni tecniche e dei servizi della società dell'informazione-, ha inviato al Governo italiano un parere molto significativo riguardo al disegno di legge sull'intelligenza artificiale. Di fatto, il parere della Commissione (in più punti analogo al contenuto del Parere del Garante italiano del 2 agosto 2024 reso sul medesimo disegno di legge) ha richiamato il bisogno di osservare il principio di indipendenza delle Autorità di verifica, messo in discussione dalla circostanza che l'intervento normativo italiano non ha conferito i compiti di vigilanza al Garante per la protezione dei dati personali, come avviene in Olanda, ma alle due agenzie AgID e ACN, entrambe sostanzialmente collegate al Governo, creando, perciò, una situazione, già più volte, criticata da parte delle Autorità di protezione dei dati personali degli altri Paesi europei. Infine, si è suggerita una profonda e complessa opera di modifica dell'impianto legislativo proposto e una garanzia in merito all'indipendenza delle Autorità designate ai sensi dell'*AI Act*. Sul punto, si v. F. PIZZETTI, *IA, perché*

In alternativa, nel solco delle indicazioni dell'*EDPB*, si sarebbe potuto creare un'unica Autorità "tecnologica" che coniugasse le funzioni, ad oggi, svolte dalle Autorità di protezione dei dati personali e i compiti delineati per quella di vigilanza del mercato dall'*AI Act*[156].

5. Il GDPR, il DSA, l'AI Act e la co-vigilanza delle rispettive Autorità competenti. Rilievi conclusivi.

Infine, in risposta ai quesiti che si sono sollevati, può dirsi che, in Italia e negli altri Stati membri, nei quali non solo le Autorità di protezione dei dati personali non sono state designate quali Autorità di vigilanza del mercato dell'intelligenza artificiale, ma non sono state neppure accolte le raccomandazioni dell'*EDPB* relative all'investitura delle prime per i compiti di controllo sui sistemi nei contesti indicati, è indispensabile promuovere la collaborazione tra le due Autorità di settore, al fine di garantire, per un verso, l'applicazione del diritto settoriale, per altro verso, la coerenza del sistema di protezione configurato dall'*AI Act*[157].

Tale l'esigenza di raccordo sussiste, altresì, tra tali due Autorità e il Coordinatore dei servizi digitali.

Vale, perciò, quanto affermato dall'*EDPB* nel parere richiamato, sull'esigenza di incentivare e realizzare un'idonea ed efficace coordinazione tra tutte le Autorità coinvolte nel trattamento dei dati personali, individuando procedure chiare, anche al fine di garantire certezza di diritto ai differenti *stakeholders* ed evitare la duplicazione di oneri ammnistrativi.

Ordunque, a livello nazionale, il nostro ordinamento giuridico ha espresso la necessità di coordinare le attività del Garante della *Privacy* sia con il Coordinatore dei servizi digitali, sia con l'Autorità di vigilanza del mercato.

Infatti, la norma istitutiva dell'Autorità per le garanzie nelle comunicazioni quale Coordinatore dei servizi digitali dispone che l'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle proprie funzioni, dovranno assicurare ogni collaborazione essenziale ai fini dell'esercizio da parte dell'AGCOM delle funzioni di Autorità di vigilanza nazionale, ai sensi del *DSA*: si lascia, così, lo spazio di coordinamento tra tale Autorità e le altre autorità amministrative indipendenti, da disciplinare con appositi protocolli di intesa.

Inoltre, la legge sull'intelligenza artificiale, all'art. 20, 4 comma, prevede che sono preservati i compiti, i poteri e le competenze sia del Garante per la protezione dei dati personali, sia dell'Autorità per le garanzie nelle comunicazioni, quale Coordinatore dei Servizi Digitali. Una disposizione puntuale di coordinamento dell'attività del Garante della *privacy* con quelle nominate dalla legge è dettata dall'art. 9, che statuisce l'obbligo di consultazione preventiva di tale Autorità, quando dati sensibili, di cui all'art. 9

l'Europa fa bene a bocciare la legge italiana (2024), consultabile sul sito https://www.agendadigitale.eu, 13 dicembre 2024. Viceversa, il legislatore italiano ha mantenuto l'impostazione iniziale.

[156] Si concorda con R. PANETTA, *Governance dell'AI Act: il ruolo delle Autorità in Italia ed Europa*, consultabile sul sito https://www.agendadigitale.eu, 21 giugno 2024

[157] S. VILLANI, *op.cit.*, p. 13.

GDPR, siano utilizzati dai sistemi intelligenti, per motivi di ricerca o di sperimentazione medica.

Ciononostante, il legislatore italiano non ha individuato strumenti regolatori specifici di raccordo delle attività dell'Autorità di protezione dei dati personali, dell'Autorità di vigilanza del mercato dell'IA e del Coordinatore dei servizi digitali.

Ed è proprio in assenza di regole procedurali puntuali in tale ambito che il protocollo d'intesa firmato il 29.7.2025 dai Presidenti del Garante *privacy* italiano e dell'Autorità Garante della Concorrenza e del Mercato può assurgere, ad avviso di chi scrive, a modello virtuoso di collaborazione tra Autorità di ambiti settoriali differenti, ma trasversali. Il fine del protocollo d'intesa è di realizzare un'azione più efficace delle due Autorità negli ambiti riguardanti le rispettive sfere di attività e di interesse comune, mediante il coordinamento dei propri interventi in casi definiti, nei quali è rilevante il trattamento e l'impiego di dati di carattere personale[158]. L'accordo, della durata di tre anni, mira a assicurare un'azione congiunta più efficace nelle ipotesi in cui il trattamento dei dati personali assuma rilievo anche sotto il profilo concorrenziale o consumeristico e dispone una serie di previsioni quali: segnalazioni reciproche tra le Autorità, nei casi in cui emergano violazioni di norme di competenze trasversali; lo scambio periodico di informazioni sulle linee di intervento e sui procedimenti di comune interesse; il coordinamento nelle indagini conoscitive e segnalazioni congiunte al Parlamento e al Governo; consultazioni reciproche durante le istruttorie che abbiano profili condivisi; l'istituzione di un tavolo tecnico permanente, che sia composto dai responsabili degli uffici competenti, con il compito di coordinare le attività e proporre eventuali modifiche o integrazioni del Protocollo e, infine, l'organizzazione di incontri periodici e attività formative miranti a promuovere una cultura comune della tutela del consumatore digitale e della protezione dei dati[159].

Si osservi, poi, che, a livello europeo, stanno emergendo gradualmente delle tendenze che mirano a superare le logiche settoriali delle normative e a promuovere un approccio sistematico[160].

Si faccia, *in primis*, riferimento a talune norme relative al coordinamento dell'Autorità di vigilanza del mercato con altre Autorità, sancite dall'*AI Act,* quali*:* l'art. 77, par. 1, in materia di «Poteri delle autorità che tutelano i diritti fondamentali» e l'art. art. 99, par. 7, lett. b), relativo all'esercizio del potere sanzionatorio dell'autorità di vigilanza[161].

In più, di importanza primaria è il principio di diritto espresso in materia di co-vigilanza dalla Corte di Giustizia UE, 4 luglio 2023, C-252/21, nel *leading case*, *Meta Platforms e a.*, cit., la cui decisione è stata menzionata nel parere del *EDPB* esaminato. La Corte europea si è dovuta pronunciare sulla questione sottopostale dall'*Oberlandesgericht* di Düsseldorf, al quale *Meta* ha presentato un ricorso, sollevando, tra le varie questioni, l'interrogativo se sia possibile, per le Autorità garanti della concorrenza, verificare e pronunciarsi sulla conformità

[158] Si v. *Comunicato Stampa- Antitrust: Firmato protocollo d'intesa con Garante Privacy,* consultabile sul sito https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10152658

[159] C.A. TROVATO, *Il protocollo d'intesa del 29.7.2025 tra il Garante privacy italiano e l'AGCM*, in *Persona e mercato* 2025/3, p. 1047.

[160] C.A. TROVATO, *op.ult.cit.*, p. 1048.

[161] Si v. *supra*, § 4.

di un trattamento di dati personali ai requisiti predisposti dal *GDPR*[162]. Il Tribunale superiore tedesco, nell'adire in via pregiudiziale i Giudici di Lussemburgo, ha loro rinviato la questione se sia compatibile con gli articoli 51 e ss. *GDPR* la circostanza che un'Autorità diversa da quella competente a garantire un controllo sulla liceità e sulla correttezza dei trattamenti di dati personali accerti, nel contesto di una verifica sul potenziale abuso di posizione dominante di un operatore, che le condizioni contrattuali applicate dallo stesso contrastino suddetto regolamento, imponendo la conseguente regolarizzazione di tali violazioni; oppure se ciò integri propriamente gli estremi di un'ingerenza nelle competenze delle Autorità della protezione dei dati personali.

La Corte Giust. UE ha, prima di tutto, preso atto della circostanza che ciascuna Autorità di settore, nell'esaminare l'inosservanza della normativa il cui rispetto è tenuta a sorvegliare, potrà, altresì, constatare la violazione di un'altra regolamentazione, qualora tale rilevazione sia fondamentale per accertare l'esistenza di un'inottemperanza di sua competenza. Dipoi, si è sostenuto che l'Autorità della concorrenza non può discostarsi da una decisione adottata dal Garante della *privacy* e che, in ogni modo, anche in assenza di un'indagine o di un provvedimento di detta Autorità, qualora la prima ritenga che il comportamento dell'impresa non sia conforme al *GDPR*, ha il dovere di consultare l' Autorità di protezione dei dati personali e di chiederne il coordinamento, al fine di valutare se si debba attendere l'adozione di una sua risoluzione, prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta entro un termine ragionevole, l'Autorità *antitrust* potrà proseguire la propria indagine.

La decisione rappresenta un punto di equilibro rilevante, siccome riconosce la legittimità di un metodo collaborativo nel valutare le pratiche di mercato, riaffermando, tuttavia, il ruolo centrale delle Autorità di controllo dei dati personali nella tutela dei diritti fondamentali.

I giudici di Lussemburgo hanno, in tal modo, affermato il principio di diritto sulla "co-vigilanza" secondo il quale alle Autorità di sorveglianza degli Stati membri è riconosciuta, a fronte di possibili sovrapposizioni di ruoli, la possibilità di esercitare "una competenza condivisa, purché non sostitutiva", evincendo una serie di doveri di collaborazione e di coordinamento tra le stesse Autorità direttamente dal principio di leale collaborazione, enunciato dall'art. 4, par. 3, TUE.

Il principio di diritto enunciato dalla Corte di Giustizia UE è, senz'altro, estensibile a qualsiasi ipotesi di "sovrapposizione di ruoli" delle Autorità di vigilanza del mercato digitale e, dunque, in riferimento al rapporto tra l'Autorità di protezione dei dati personali e l'Autorità di vigilanza del mercato dell'intelligenza artificiale; così come quando entri in gioco anche la competenza dei Coordinatori dei servizi digitali.

[162] Per le riflessioni che seguono, si v. C.A. TROVATO, *La sentenza CGUE del 4.7.2023 nel caso C252/21 sui rapporti tra privacy e antitrust, sulla pubblicità dei dati sensibili e sulla inadeguatezza della base del legittimo interesse per il trattamento dei dati inerenti la pubblicità comportamentale di Meta (sentenza Meta abuso di posizione dominante), cit.*

Dipoi, hanno un rilievo fondamentale le varie attività di *self regulation* delle Autorità di vigilanza, quali le Opinioni, gli Orientamenti o le Linee Guida da esse emanate, con le quali indirizzano i comportamenti privati e pubblici[163].

Si consideri che, senza linee guida delle Autorità di controllo competenti, gli operatori del mercato digitale, in particolar modo le piattaforme digitali di grandi dimensioni, che spesso provengono da ordinamenti giuridici dove la protezione dei dati personali non è tanto importante come in Unione europea, saranno costretti ad effettuare personalmente un contemperamento degli interessi in gioco, pervenendo a valutazioni discrezionali ed arbitrarie[164].

Ecco perché sono molto importanti le Linee guida dell'*EDPB* 3/2025 sul coordinamento tra *DSA* e *GDPR*, pubblicate l'11 settembre 2025 e aperte alla consultazione pubblica che si è conclusa il 31 ottobre 2025[165]. Le Linee guida hanno l'obiettivo di contribuire a un'interpretazione coerente del *DSA* e del *GDPR*, incentrandosi su disposizioni specifiche del *DSA* che attengono al trattamento di dati personali effettuato da parte dei fornitori dei servizi di intermediazione[166].

Principalmente, è rimarcata la centralità della cooperazione tra i Coordinatori dei servizi digitali, la Commissione europea e le Autorità di protezione dei dati personali, per garantire un'applicazione coerente del *DSA* e del *GDPR*. L'*EDPB* evidenzia che il principio di leale collaborazione impone a tali Autorità di cooperare, nel senso che le stesse devono consultarsi reciprocamente, allorquando siano tenute a verificare se la condotta di un

---

[163] Per le notazioni che seguono C. SOLINAS, *op.ult.cit.*, p. 259-262.

[164] P. FALLETTA, A. MARSANO, *op.cit.*, p. 129. Influente dottrina si è soffermata sull'esigenza della stesura di linee guida specifiche, della diffusione e dell'adozione di codici etici e di *standard* di buone pratiche in materia di *neuromarketing,* al fine di prevenire, alla luce dei principi di prevenzione e di precauzione, pratiche manipolative. Si v. I. GARACI, *Il neuromarketing nel quadro giuridico europeo: riflessioni sulle opportunità e sui rischi per i soggetti vulnerabili*, in *Persona e mercato*, 2025/3, p. 1187.

[165] Sul punto e per le argomentazioni che seguono si v. E. STRINGHI, *Le Linee guida EDPB 3/2025 aperte alla consultazione pubblica sul coordinamento tra DSA e GDPR (versione 1.1 del 12 settembre 2025*), in *Persona e mercato*, 2025/3, p. 1029 ss.

[166] Le linee guida si focalizzano sulla normativa statuita dall'art. 7 *DSA*, relativa alle attività di rilevazione e rimozione di contenuti illegali che possono determinare il trattamento di dati personali mediante diverse tecniche; sulla regolamentazione dei meccanismi di segnalazione e rimozione e dei sistemi di gestione dei reclami richiesti dal *DSA*, di cui agli artt. 16, 17, 20 e 23, che possono comportare anch'essi il trattamento di dati personali di coloro che segnalano contenuti illegali o contestano le decisioni assunte dall'intermediario. Le linee guida illustrano i principali elementi da valutare per stabilire se un *design* ingannevole delle interfacce degli *internet service providers* (disciplinato dall'art. 25 *DSA*) rientri nel *GDPR*, quali la presenza di un trattamento di dati personali o la modifica comportamentale dell'interessato dovuta a tale attività. Si analizza quanto prescritto dall'art. 26 *DSA*, secondo il quale i fornitori dei servizi di piattaforme *online* non devono trattare dati di natura particolare per presentare i messaggi pubblicitari profilati. Le linee guida si soffermano sui punti di contatto tra la regolamentazione del *GDPR* e quella del *DSA*, di cui agli artt. 27 e 38, attinenti ai sistemi di raccomandazione, nei quali i fornitori delle piattaforme *online* possono trattare i dati personali degli utenti per personalizzare l'ordine o la rilevanza dei contenuti loro mostrati. L'*EDPB* valuta in modo positivo l'intento del *DSA* di garantire un livello elevato di tutela della riservatezza, della sicurezza e della protezione per i minori utenti delle piattaforme *online* e le linee guida riconoscono che l'art. 28, par. 1 e 2, *DSA* può costituire un "obbligo legale" ai sensi dell'art. 6, par. 1 lett. c) *GDPR* e, dunque, un valido presupposto di liceità per il trattamento dei dati personali compiuto per finalità di tutela dei minori *online*, sempre che lo stesso sia necessario e proporzionato. Il Comitato europeo per la protezione dei dati personali ritiene che la verifica dell'età dovrebbe essere effettuata in funzione del rischio per i minori, considerando i principi di necessità e proporzionalità del *GDPR*, operando un'interpretazione logico-sistematica degli artt. 28 e 35 *DSA* e delle regole generali del *GDPR*. Sul punto e per le osservazioni che seguono sulla cooperazione tra le Autorità di settore si v. E. STRINGHI, *Le Linee guida EDPB 3/2025 aperte alla consultazione pubblica sul coordinamento tra DSA e GDPR (versione 1.1 del 12 settembre 2025*), in *Persona e mercato*, 2025/3, pp. 1029-1031.

prestatore di servizi di intermediazione, di un titolare o di un responsabile del trattamento sia conforme alle previsioni del quadro normativo soggetto alla vigilanza dell'altra. La consultazione reciproca è strumentale a consolidare la certezza del diritto, impedire incongruenze regolatorie e prevenire eventuali violazioni del principio di *ne bis in idem.*

In aggiunta, si richiamano gli Orientamenti sulla protezione dei minori a norma del *DSA*, pubblicati dalla Commissione europea il 14 luglio 2025 e approvati il 7 ottobre 2025[167], al fine di garantire un'esperienza *online* sicura per i bambini e gli adolescenti[168].

La Commissione si pone l'obiettivo di fissare *standard* di valutazione della conformità all'articolo 28, par. 1 *DSA*: gli Orientamenti costituiscono, cioè, un punto di riferimento per i Coordinatori dei servizi digitali e per le Autorità nazionali competenti, nel verificare se le piattaforme *online* che permettono ai minori di utilizzarle rispettino il *DSA*.

Gli Orientamenti si applicano a tutte le piattaforme digitali accessibili ai minori, escluse le microimprese e le piccole imprese.

Essi sono di un supporto ai fornitori di piattaforme *online* nell'assicurare l'implementazione di misure concrete, miranti a ridurre i rischi sistemici. Di qui, la previsione di un elenco non esaustivo di misure proporzionate e idonee a proteggere i minori dai rischi in rete quali l'adescamento, i contenuti nocivi, le condotte problematiche e che creano dipendenza, come pure il bullismo *online* e le pratiche commerciali dannose.

Gli Orientamenti toccano numerosi profili disciplinari che convergono con l'assetto normativo del *GDPR*; ragion per cui dall'adesione agli stessi discenderà una condotta dei gestori delle piattaforme *online* rispettosa del *GDPR*, oltre che del *DSA*. Ciò nondimeno, l'uniformazione agli stessi è volontaria e non garantisce automaticamente la conformità alla normativa.

Ancora, l'*EDPB*, nelle Linee Guida 3/2025 suddette, afferma che è risolutivo chiarire il rapporto tra i codici di condotta sviluppati ai sensi del *DSA* e quelli elaborati ai sensi del *GDPR* e assicurare il coinvolgimento delle Autorità di protezione dei dati nello sviluppo dei primi, qualora sia opportuno. I codici di condotta adottati ai sensi dell'una e dell'altra regolamentazione possono essere, in realtà, complementari tra di loro[169]. Tale circostanza è molto significativa, dal momento che il Garante della *privacy* «approva» i codici di

---

[167] *Communication from the Commission. Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*. Brussels, 7.10.2025, C (2025) 6826 final. Per le considerazioni che seguono, si v. *La Commissione pubblica orientamenti sulla protezione dei minori*, 14 luglio 2025, consultabile al sito https://digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-protection-minors. Le raccomandazioni principali, che presentano punti di contatto con il Regolamento generale sulla *privacy*, riguardano: l'impostazione degli *account* dei minori in privato per impostazione predefinita, affinché le loro informazioni personali, i dati e i contenuti *dei social media* non siano visibili a coloro con cui non vi sia un collegamento; la modifica dei sistemi di raccomandazione delle piattaforme, per ridurre il rischio che i bambini accedano a contenuti dannosi; permettere ai bambini di bloccare e disattivare qualsiasi utente e garantire che non possano essere aggiunti ai gruppi senza il loro esplicito consenso; impedire agli *account* di scaricare i contenuti pubblicati da minori, per evitarne la diffusione. Di notevole rilievo è la raccomandazione dell'impiego di metodi efficaci di verifica dell'età, purché siano affidabili, non intrusivi e non discriminatori.

[168] Per le riflessioni che seguono, si v. *La Commissione pubblica orientamenti sulla protezione dei minori*, 14 luglio 2025, consultabile al sito https://digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-protection-minors

[169] E. STRINGHI, *op.cit.*, p. 1031.

condotta con i quali categorie di titolari del trattamento regolamentano in autonomia, benché "sub condizione" dell'approvazione dell'Autorità, i trattamenti specifici svolti nell'esercizio delle proprie attività (art. 40 *GDPR*). Tra questi potrebbe costituire oggetto di una disciplina specifica il trattamento algoritmico effettuato da determinate categorie di soggetti, tra quali i fornitori di piattaforme digitali[170].

Per concludere, il raccordo delle funzioni delle Autorità di vigilanza del mercato digitale, in modo precipuo, delle Autorità che sono state oggetto di attenzione, è di nodale importanza, giacché le autorità amministrative indipendenti dialogano in modo proficuo con le autorità giudiziarie: non costituiscono un'alternativa, ma una forma di tutela concorrente e, qualche volta, un filtro di accesso alla giurisdizione, con finalità deflattiva[171].

Indubitabilmente, un provvedimento di un'Autorità, chiamata settorialmente a intervenire su un trattamento algoritmico dei dati personali compiuto da una piattaforma digitale, sul quale sussista, nel caso concreto, trasversalmente la competenza anche di altre Autorità, qualora venga adottato a seguito di un'ampia collaborazione tra le stesse, può, a sua volta, condurre ad un dialogo più proficuo con le corti che sono, comunque, tenute ad operare un'interpretazione logico-sistematica delle normative interessate, per pervenire ad una decisione complessa ed unitaria.

In via conclusiva, volgendo lo sguardo ad un futuro non troppo lontano, non si tralasci che, il 19 novembre 2025, la Commissione europea ha presentato un pacchetto di riforme, il "*Digital omnibus*", volto alla semplificazione e all'armonizzazione del *Digital Acquis*, apportando modifiche sia al *GDPR*, sia all'*AI Act*, oltre che alla direttiva *e-privacy* e al regolamento il Regolamento 2023/2854/UE, c.d. *Data Act*, che conducono ad un diverso equilibrio tra apparati amministrativi, poteri tecnici e diritti fondamentali [172]. Il cronoprogramma dell'*iter* legislativo si dipana tra il 2025 e 2027.

Il *Digital omnibus* si compone di due proposte di regolamento.

La prima proposta [173], comunemente definita "*Digital Omnibus*", incide trasversalmente sul complesso delle discipline europee dettate in materia di dati, tecnologie, servizi digitali e *cybersecurity*. In particolare, essa ridisegna il *GDPR*, per allinearlo all'*AI Act*, al Regolamento 2022/868/UE (c.d. *Data Governance Act*), alla direttiva 2022/2555/UE relativa alle misure per un livello comune elevato di cibersicurezza nell'Unione Europea (c.d. direttiva NIS2)[174] e al regolamento 2024/1183/UE[175]; introduce anche disposizioni che modificano le categorie concettuali e i fondamenti giuridici del trattamento dei dati

[170] Per tali notazioni, si v. C. SOLINAS, *op.ult.cit.*, pp. 260-261.
[171] A. VALONGO, *op.cit.*, p. 148 s. A ZOPPINI, *Il ruolo e le funzioni delle Authorities nel trattamento algoritmico dei dati personali*, in AA.VV., *Il trattamento algoritmico dei dati tra etica, diritto e economia*. Atti del 14° Convegno Nazionale SISDiC, a cura di P. PERLINGIERI, S. GISOVA, I. PRISCO, Napoli, 2020, p. 291 ss.
[172] Per le osservazioni che seguono, si v. A. ALÙ, *Digital Omnibus, la UE cambia metodo: addio alla giungla*, consultabile sul sito https://www.agendadigitale.eu/, 3 dicembre 2025; A. LONGO, F. VIOLA, *Digital Omnibus, GDPR e AI Act: la nuova grammatica digitale europea*, *ivi*, 25 novembre 2025.
[173] Bruxelles, 19.11.2025, COM(2025) 837 final, 2025/0360(COD)
[174] Il provvedimento ha arrecato modifiche al Regolamento 2014/910/UE e alla Direttiva 2018/1972/UE e ha abrogato la Direttiva 2016/1148/UE, c.d. Direttiva NIS.
[175] Il provvedimento ha modificato il Regolamento 910/2014/UE per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

personali e dei processi decisionali automatizzati, assetti istituzionali e perimetri operativi.

La seconda proposta di regolamento[176], definita "*Digital Omnibus on AI*", introduce una revisione normativa del regolamento sull'intelligenza artificiale, a distanza di poco più di un anno dalla sua formale entrata in vigore, prevedendo, peraltro, una proroga fino a sedici mesi dei doveri da rispettare per i sistemi ad alto rischio, con l'obiettivo di garantirne un'applicazione più chiara, semplice e "*innovation-friendly*". Tra i vari interventi, vi sono: la formulazione di misure di semplificazione, nella prospettiva di facilitare la corretta attuazione dell'*AI Act*, senza pregiudicare i parametri elevati di protezione prefissati dal legislatore; una serie di modifiche da apportare all'art. 43 del regolamento, rubricato «Valutazione di conformità», finalizzate ad "allineare i requisiti di valutazione della conformità con quelli dei fornitori di sistemi di IA ad alto rischio previsti dall'articolo 16".

Una novità particolarmente rilevante attiene al regime di *governance* dei sistemi intelligenti basati sui modelli di IA a scopo generale. Al fine di rafforzarlo, la proposta di regolamento modifica l'art. 75 *AI Act*, ridisegnando il ruolo dell'Ufficio per l'IA nel monitoraggio e nella vigilanza della conformità di tali sistemi: gli è, difatti, conferita una competenza rafforzata, in taluni casi addirittura esclusiva, per il monitoraggio e l'*enforcement* nei confronti di tali modelli, allorquando il modello e il sistema sono forniti dallo stesso *provider*, oltre che per i sistemi integrati all'interno di piattaforme digitali e motori di ricerca "di dimensioni molto grandi" [177].

Tale "accentramento" è dettato dall'esigenza di mitigare la frammentazione nazionale e garantire una sorveglianza tecnicamente congrua a sistemi particolarmente complessi, nei quali il perimetro tra modello, servizio e contesto d'uso diviene sempre più vago[178],

È ancora presto per esprimere un giudizio sulle proposte di revisione normativa, ma appare ben chiaro che incideranno, in maniera significativa, *in primis*, sui contenuti della disciplina del *GDPR* e dell'*AI Act*, con la conseguenza che indirizzeranno diversamente non solo le attività e i comportamenti di qualunque categoria di titolari di trattamento dei dati personali e dei fornitori e *deployers* dei sistemi intelligenti, ma, altresì, quelli dei gestori delle piattaforme digitali che, nello svolgimento delle proprie attività, impieghino sistemi intelligenti e/o compiano trattamenti di dati personali.

In chiusura, se verrà approvata la modifica dell'art. 75 *AI Act,* si assisterà ad una radicale modifica del sistema di *governance* attualmente vigente, che si riverbererà, ovviamente, altresì sui meccanismi di co-vigilanza delle Autorità di controllo di settore chiamate ad intervenire, in maniera trasversale, sulla

[176] Bruxelles, 19.11.2025, COM(2025) 836 final, 2025/0359(COD).

[177] Sul punto e per la considerazione che segue nel corpo del testo, si v. F. CERCIELLO, *Il pacchetto "Digital Omnibus": cosa prevede la riforma sistemica del diritto digitale dell'Unione*, consultabile sul sito https://www.agendadigitale.eu/, 21 novembre 2025.

[178] Si v. A. ALÙ, *op.cit*. L'A. precisa che l'articolo 75, come novellato, stabilisce che, l'Ufficio per l'IA, nello svolgimento dei tali compiti, ha tutti i poteri di cui dispone un'autorità di sorveglianza e che potrà, quindi, adottare misure e assumere decisioni idonee per espletare tali funzioni. A tal uopo, la Commissione europea dovrebbe definire le procedure per permettere all'Ufficio per l'IA di esercitare tali poteri, "inclusa la sua capacità di imporre sanzioni, come multe o altre sanzioni amministrative, in conformità con le condizioni e i limiti indicati nell'articolo 99".

medesima vicenda di trattamento algoritmico di dati personali compiuto da una piattaforma digitale.