Marco Cappai

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

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

1 Il rapporto tra Regolamento IA e Gdpr

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[26] Art. 88 del Regolamento IA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[33] *Infra* § 4.

[34] Art. 17, § 2 CDFUE.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

tiva privacy, doc. web n. 9978020.

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

[46] Report cit., § 17.

[47] *Ivi*, § 19.

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

[49] *Ivi*, § 27.

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

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

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

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

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

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

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

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

5 Il Ddl AI e il parere preventivo espresso dal Gpdp

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 Ulteriori proposte di modifica

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Data Governance Act [61].

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

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