RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0207 • articolo sottoposto a peer review • pubblicato in anteprima il 18 feb. 2025

Maria Chiara Pollicino

Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa

Il saggio analizza l'interazione tra il nuovo Regolamento sulle intelligenze artificiali e il GDPR al fine di valutare il complessivo impatto, frutto della sommatoria tra le due citate normative, nell'ambito dell'attività amministrativa. L'integrazione tra le due discipline risulta inevitabile, soprattutto sul piano fenomenologico, poiché l'impiego dell'intelligenza artificiale implica quasi sempre il trattamento di dati personali. A tal fine, anche per esigenze di chiarezza espositiva, i due testi saranno analizzati prima separatamente, ponendo in evidenza le peculiarità che assumono allorquando il trattamento dei dati personali o l'uso dell'intelligenza artificiale abbia luogo nella cornice dell'azione pubblica. All'esito della trattazione separata, i due Regolamenti saranno posti a confronto, evidenziandone i principali elementi comuni e differenziali. In ultimo, alla luce del confronto, si ragionerà sull'impatto della complessiva normativa sul potere pubblico.

Privacy – Pubblica amministrazione – Intelligenza artificiale – GDPR – AI Act

The effects of the "cumulative impact" of the GDPR and the new Artificial Intelligence Regulation in the context of administrative activities

This paper draws a comprehensive interaction between the new Artificial Intelligence Regulation and the GDPR, with the goal of assessing their combined impact on administrative activities. The intersection of these two frameworks is, in most cases, inevitable, particularly on a phenomenological level, as the use of artificial intelligence involves the processing of personal data. To achieve this, the two regulations will first be examined individually, emphasizing the unique characteristics each assumes when personal data processing or the use of AI occurs within the realm of public administration. Following this individual analysis, the regulations will be compared, highlighting their key similarities and differences. Finally, based on the insights from this comparison, the overall effect of these regulatory frameworks on the exercise of public authority will be carefully evaluated.

Privacy – Public Administration – Artificial Intelligence – GDPR – AI Act

L'Autrice è dottoranda in Legalità, culture politiche e democrazia, profilo di diritto amministrativo, presso l'Università degli Studi di Perugia

1. Premessa: l'impatto della regolazione nel settore digitale. Perché regolare e quanto regolare?

Prima di entrare nel merito della questione circa l'attuale quadro regolatorio del digitale e, in particolare, valutare le eventuali sovrapposizioni tra il GDPR e il nuovo regolamento sulle intelligenze artificiali[1] sotto la lente del trattamento effettuato dal soggetto pubblico, è opportuno riflettere sul perché rispondere alla domanda relativa a quale sia l'ottimo regolatorio del settore digitale nel pubblico sia diventato fondamentale[2]. Difatti, regolare adeguatamente il settore del digitale ha un immediato impatto, oltre che sui principi del procedimento amministrativo, come il principio di legalità o la trasparenza, sui diritti fondamentali dell'uomo[3] e, ancor più a monte, sulla tenuta democratica degli Stati[4].

Molti studiosi oltreoceano hanno, già da tempo, evidenziato l'impatto sociale di scelte regolatorie "errate" sulle tecnologie[5]: regolare poco o, al contrario, regolare troppo le tecnologie potrebbe avere delle conseguenze significative su larga scala, soprattutto se si considera il settore pubblico.

Regolare "poco", difatti, renderebbe possibile il concretizzarsi di tutta una serie di pericoli: tra cui la nascita di nuove forme di discriminazione nonché, a monte, un importante sbilanciamento dei rapporti di forza tra i poteri pubblici e privati, a favore dei secondi.

Sotto il primo profilo richiamato, la discriminazione che si potrebbe creare, per esempio, delegando decisioni alla macchine – in modo più o meno consapevole – senza un'adeguata normativa a sostegno che possa neutralizzare i pericoli di *bias*[6]. Più nello specifico, è stato evidenziato che

1. Regolamento (UE) 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale, di seguito detto, in breve Regolamento IA.
2. Tale domanda, sull'ottimo regolatorio, diviene ancor più interessante considerando che l'Europa si è ritagliata una funzione di *leadership* nella regolazione nel settore a livello globale. Tale ruolo trova conferma negli scritti della dottrina mondiale, *ex multis*, citando autori statunitensi, cfr. Solove–Schwarts 2022.
3. Niro 2021; Simoncini–Suweis 2019; Calzolaio 2023; Iannuzzi 2021.
4. Barocas–Selbst 2016.
5. *Ibidem*.
6. Proprio per disinnescare tale possibilità si richiede che ogni decisione algoritmica sia assistita dal controllo umano. Tuttavia, spesso, tale previsione, se non adeguatamente declinata, rischia di tradursi in un controllo formale e non sostanziale da parte dell'umano. Sul punto, si rimanda a quanto evidenziato da Carloni

potrebbero perpetrarsi fenomeni come quello della c.d. "discriminazione istituzionalizzata"[7] fondata, per l'appunto, su *bias*, ossia pregiudizi inconsci delle macchine e, poi, fatti propri dai decisori pubblici (peraltro, si tratta di errori che, per loro natura, sono destinati a ripetersi *n* volte). Uno dei problemi maggiori che pongono simili *bias* involontari – in quanto non diretto frutto di una opera dei programmatori che hanno tarato male la macchina – è che gli stessi, di sovente, sono irriconoscibili dall'uomo[8]: in questo senso, l'ingiustizia umana volontaria è un fenomeno molto più auto-evidente comparata all'ingiustizia involontaria algoritmica[9].

Per quanto concerne il secondo profilo citato, il potere privato, ad oggi, tramite la tecnologia, ha assunto una peculiare forza non solo economica[10], bensì, anche negli ambiti, tradizionalmente "riservati" al potere pubblico, sociale e politico. Come evidenziato da attenta dottrina: «non vi è dubbio (…) che i grandi fornitori di servizi digitali siano ormai poteri privati globali di grandi dimensioni, dotati di un enorme peso economico e di presenza e influenza molto pervasive sul piano sociale»[11]. Pertanto, ad oggi, la necessità di una regolazione adeguata si impone in quanto il potere pubblico è chiamato non solo a porre delle norme di contenimento del settore privato, che sfugge al controllo del pubblico, bensì si tratta di normare il settore privato – in una vera e propria lotta per la sovranità[12] – con il pubblico[13]. È stato osservato che uno dei vantaggi del potere privato rispetto al potere pubblico consiste nel fatto che è difficile regolare *ex ante* un qualcosa che non si conosce e che si sviluppa fuori dal contesto istituzionale. La tecnologia, difatti, tendenzialmente, non si sviluppa all'interno

2020, p. 281: «(i)n assenza di una disciplina legislativa ad hoc, ed in ogni caso per riflettere sui limiti e le condizioni che potrebbero accompagnare una simile regolazione, è altrove che bisogna guardare per ragionare sulla possibilità e legittimità di una decisione algoritmica, intendendo con questa una decisione non elementare assunta sulla base di un percorso decisionale non meramente meccanico ma rimesso a macchine. Dove si intende per "rimesso" il fatto che la decisione sia effettivamente adottata in assenza di un intervento umano nella fase decisionale, ma anche già solo il fatto che l'operazione automatizzata effettuata svolga un ruolo decisivo nella determinazione provvedimentale e non sia in sé suscettibile di revisione, quanto alla correttezza intrinseca del "ragionamento" seguito, da parte del funzionario istruttore».

7. Il termine è stato coniato in ambito sociologico da Pager–Shepherd 2008.
8. Cfr. anche Powell 2007.
9. Barocas–Selbst 2016, p. 674 ove si evidenzia: «(…) Because the discrimination at issue is unintentional, even honest attempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions. Furthermore, because the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address». Ancora, parte della dottrina ha sottolineato come, a monte, regolare il fenomeno tecnologico sia una sfida molto complessa per il diritto, che rischia di perdere il suo ruolo di "strumento di regolazione dei conflitti umani" cfr. Corasaniti 2022, pp. 11-12: «Il diritto rischia di non adeguarsi al passaggio, di non potere mantenere a lungo il suo tradizionale ruolo di strumento di regolazione dei conflitti umani non riuscendo a comprendere né a definire in modo tradizionale ambiti e forme di regolazione, tanto più se questi debbono svolgersi in un contesto senza confini in uno spazio cyber definito e ricompreso nelle piattaforme di servizio nelle quali i soggetti si collocano, peraltro liberamente. Le piattaforme digitali oggi operano in assoluta interconnessione e condizionano e condizioneranno sempre di più le scelte dei soggetti sociali, indirizzandole, uniformandole, facilitandole e trasformandole in un progetto di vita o di attività vitale».
10. Per dare un'idea della forza economica dei colossi del digitale, si pensi che, tra le società quotate nella borsa di Wall Street, Apple è la prima società ad avere toccato il valore di tremila miliardi di dollari. Come ben evidenziato da Torchia 2024.
11. *Ivi*, p. 18.
12. Sulla battaglia pubblico-privato si vedano: Betzu 2021.
13. Cfr. Torchia 2024.

del settore pubblico, al contrario, «si sviluppa fuori dalle grandi istituzioni di ricerca»[14].

In ogni caso, la capacità del potere privato di influenzare la società[15] è ancor più preoccupante considerando che le nuove tecnologie permettono alle intelligenze artificiali di "entrare" in aspetti profondamente intimi dell'essere umano tra cui il pensiero (ci si riferisce al tema, delicatissimo, della privacy mentale)[16].

Queste, dunque, le principali problematiche che deriverebbero da una regolazione assente, scarna o, comunque, inefficace.

Per converso, all'opposto, regolare "troppo" vorrebbe dire, nella sostanza, rendere quasi impossibile un utilizzo proficuo degli strumenti tecnologici che, invece, possono costituire un validissimo strumento per l'attività pubblica, andando ad attuare i principi di buon andamento e di efficienza previsti, in primo luogo, dalla Costituzione, all'art. 97[17].

Perché regolare troppo rende quasi impossibile l'utilizzo delle tecnologie? Sul punto, occorre svolgere una sintetica premessa. Di sovente, quando si parla di amministrazione o di esercizio delle funzioni pubbliche, si dimentica di considerare il fattore umano: ossia, sono i singoli funzionari, che portano avanti il procedimento amministrativo e, in generale, l'azione pubblica, a dover applicare, *de facto*, quella o quell'altra norma e, a monte, a scegliere *come gestire il procedimento* (naturalmente negli spazi concessi dalla legge[18]).

Orbene, proprio considerando tale fattore umano, l'eccesso di regolazione può portare alla non trascurabile difficoltà per il funzionario[19] di inquadrare correttamente la normativa applicabile alle singole fattispecie e, pertanto, si potrebbe preferire di rifuggire l'uso di tecnologie avanzate; in altri termini, se il quadro giuridico non è facilmente accessibile perché vi è una ipertrofia normativa, il funzionario pubblico[20] potrebbe essere portato: *i)* o ad allungare i tempi del procedimento che si avvale di tecnologie all'avanguardia al precipuo fine di scioglierne i dubbi giuridici (per esempio,

14. *Ivi*, p. 16 la quale evidenzia: «viene sempre citato in proposito il famoso garage in cui Bill Gates, dropout dell'Università di Harvard, diede i natali a Microsoft – ma anche grazie a esse: basti ricordare che Internet nasce come Arpanet, alla fine degli anni Sessanta, grazie al centro militare Arpa e ad alcune università della California».
15. Il tema dell'affermarsi dei poteri privati in ambiti tradizionalmente riservati ai poteri pubblici ha un immediato riflesso sulla tenuta democratica degli Stati, come evidenziato dalla dottrina in materia di moderazione dei post per il mezzo di comitati di controllo gestiti dagli stessi social networks: cfr. Pollicino 2019, p. 10 ss.
16. D'Avack 2023 a p. 1710 e ss.: «(l)e potenzialità di penetrazione della tecnica – nell'ambito della interazione tra IA e neuroscienze e neurotecnologie – nella sfera più intima del soggetto, quella del pensiero e dei suoi correlati neuronali, solleva interrogativi di natura etica e giuridica su come proteggere questi dati così sensibili, anche dai rischi di una circolazione potenzialmente discriminante; sui confini e sulle implicazioni della libertà psichica e cognitiva di un soggetto, della sua "integrità" mentale, sulla possibilità – che deve essere sempre garantita – di disconnettersi dal mezzo di interfacciamento».
17. Sulla connessione art. 97 Cost. e uso delle intelligenze artificiali si veda Cerrina Feroni 2023: «Da qui il problema se sottoporre la persona alla decisione integralmente automatizzata di un software risulti in sé lesivo della dignità della persona stessa. Non si tratta di assumere posizioni di contrarietà agli sviluppi tecnologici, forieri sicuramente del migliore perseguimento di interessi pubblici e, quindi, funzionali al buon andamento della p.a. di cui all'art. 97 Cost. Ma di porre in evidenza, già partendo dal quadro costituzionale, che la tutela della dignità della persona richiede che l'intervento dell'uomo nel compimento della scelta amministrativa non sia del tutto obliterato o marginalizzato, proprio per rispettare la gerarchia assiologica voluta dalla Costituzione e alzare un argine alla "disumanizzazione" dell'amministrazione, riportando la macchina a semplice strumento dell'azione amministrativa».
18. Sul punto, si rimanda alle innumerevoli trattazioni scientifiche sul tema legalità/discrezionalità amministrativa, *ex multis*: Police 2014.
19. Si parla di funzionario in termini non tecnici intendendosi, in tal senso, un qualsiasi dipendente pubblico chiamato a esercitare un certo potere nel concreto, sia lo stesso funzionario, dirigente etc.
20. Potrebbe essere non del tutto accessibile o alla luce di una normativa oscura o perché vi sono troppe fonti che regolano quella specifica attività.

acquisendo pareri e così via), così ponendo nel nulla uno dei vantaggi maggiori della tecnologia, ossia la velocità *ii)* o, ancor peggio, ad evitare in radice l'utilizzo di tecnologie avanzate nel timore di errori giuridici tali da concretizzare ipotesi di violazioni normative, con conseguente rischio di responsabilità amministrativa. Sul punto, è opportuno menzionare una recente pronuncia, emessa nel 2024, dalla Corte dei conti che riconosce una responsabilità erariale del *Data protection Officer*[21].

Non è un mistero, difatti, che uno dei problemi più dilaganti nell'ambito dell'amministrazione italiana è stata (ed è) la c.d. paura della firma[22]; similmente al fenomeno della paura della firma, regolare troppo, potrebbe condurre l'operatore pubblico a evitare l'utilizzo delle tecnologie più avanzate alla luce della confusione e della paura di non essere totalmente *compliant* rispetto al quadro regolatorio, evitando così in radice di correre il rischio di rispondere per eventuali danni.

La tecnologia dovrebbe velocizzare l'attività amministrativa e, il costante "dubbio giuridico", spesso alimentato dalla ipertrofia normativa, certamente non aiuta ad accelerare il procedimento.

In tale riflessione, occorre tenere presente che la amministrazione non si deve confrontare solo con il GDPR o il nuovo Regolamento IA: vi sono moltissimi testi normativi che in via diretta o indiretta trovano applicazione quando si tratta di digitalizzazione del pubblico in senso ampio: *i) in primis* il Codice sull'Amministrazione digitale, il quale norma anche le modalità di formazione o di firma del documento informatico; *ii)* le normative di settore che si applicano solo a particolari tipologie di dati oppure a determinati settori[23]; *iii)* la disciplina, anch'essa non priva di complicazione, delle norme di sicurezza informatica etc.

Sono, dunque, davvero molteplici i temi da tenere in considerazioni allorquando sia la pubblica amministrazione a trattare il dato personale.

2. Le peculiarità del trattamento dei dati da parte dei soggetti pubblici. Una ricognizione delle norme più rilevanti del GDPR in materia

Il GDPR è il testo normativo fondamentale per il trattamento dei dati personali e non perde la sua centralità nel sistema anche allorquando il trattamento sia effettuato da parte delle pubbliche amministrazioni nell'esercizio di funzioni pubbliche.

Il GDPR trova piena applicazione, difatti, anche nel settore pubblico e non solo relativamente alle

21. Cfr. Corte dei Conti, sezione giurisdizionale di Bolzano, 9 gennaio 2024, sentenza n. 1. La vicenda trae origine da una sanzione irrogata dal Garante per la protezione dei dati personali al comune di Bolzano con provvedimento n. 190 del 13 maggio 2021«per la violazione dell'art. 5, par. 1, lett. a) e c), 8, 9, 35, 13 e 88 del Regolamento europeo n. 2016/679, nonché degli artt. 113 e 114 del codice della privacy, avendo il comune posto in essere trattamenti di dati personali dei dipendenti relativi alla navigazione in internet, in assenza dei presupposti e di idonea informativa, e adottato una modulistica per la fruizione del servizio di assistenza psicologica non conforme al quadro normativo in quanto prevedeva la conoscenza di dati personali sullo stato di salute dei dipendenti da parte dei soggetti delegati allo svolgimento delle funzioni datoriali. In particolare, segnalava che i due presunti responsabili nella loro qualità, rispettivamente, di titolare del trattamento dei dati e di responsabile dei procedimenti amministrativi in materia di protezione dei dati personali e, dal 25 maggio 2018, Privacy Manager, non si sarebbero attivati per verificare la conformità della disciplina regolamentare interna a seguito dell'avvenuto mutamento del quadro normativo operato dal d.lgs. 4 settembre 2015, n. 151, neanche a seguito della pronuncia del Garante del 13 luglio 2016 (Trattamento dei dati dei dipendenti mediante posta elettronica e altri strumenti di lavoro), e non sarebbero intervenuti per eliminare le forme di trattamento dei dati personali illeciti neppure in sede di adozione delle "Linee guida per le procedure di adeguamento del GDPR 2016/679». Alla luce della vicenda così sintetizzata la Corte dei conti ha ritenuto sussistente la responsabilità erariale con riguardo alla funzionaria quale responsabile dei procedimenti amministrativi in materia di protezione dei dati personali, poi nominata Privacy Manager. La Corte ha ravvisato nei confronti di quest'ultima una colpa grave omissiva per non essersi attivata, nonostante la nomina che le imponeva di verificare la conformità normativa; di talché è stato ritenuto provato e sussistente l'elemento psicologico della "colpa grave".
22. Per un'analisi del fenomeno della burocrazia difensiva si vedano: Cantone-Carloni 2018.
23. Sul punto, ad esempio, una normativa speciale sulla digitalizzazione che si occupa anche di alcune tematiche di privacy è rappresentata dal Nuovo codice dei contratti pubblici. Cfr. Ferrari-Morbidelli 2023.

norme dedicate all'amministrazione ma anche con riferimento alle norme di carattere generale.

È stato, difatti, evidenziato che, oltre alle norme dedicate alle attività pubblicistiche, alle pubbliche amministrazioni «rimangono applicabili tutti quegli obblighi generali cui sono assoggettati i titolari di trattamento privati»[24]. Si giunge a tale considerazione in maniera abbastanza immediata ed agile sulla base dell'analisi delle norme dello stesso GDPR: a partire dalla stessa definizione di «titolare del trattamento» ove viene richiamata l'autorità pubblica senza ulteriori specificazioni «od esclusione in ragione del tipo di attività svolta»[25].

I principi generali[26], dunque, possono e devono essere applicati nell'ambito delle attività pubblicistiche; pertanto, ai sensi dell'art. 5 del GDPR[27], le amministrazioni devono rispettare:

(i) il *principio di liceità, correttezza e trasparenza*[28] in base al quale il trattamento di dati personali deve essere lecito, quindi, autorizzato dalla legge. La trasparenza viene intesa in tale contesto nel senso che le persone fisiche devono avere informazioni chiare ed esatte circa le modalità di trattamento;
(ii) il *principio di limitazione delle finalità* che impone che i dati siano raccolti «per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità» (cfr. art. 5, par. 1, lett. b) GDPR);
(iii) il *principio di esattezza* che impone alle pubbliche amministrazioni di adottare tutte le misure ragionevoli al fine di eliminare o rettificare in modo tempestivo i dati inesatti;
(iv) il *principio di minimizzazione dei dati* secondo cui è necessario limitare, il più possibile, il trattamento dei dati personali necessari al fine di raggiungere la finalità (cfr. art. 5, par. 1, lett. c) GDPR);
(v) il *principio di limitazione della conservazione*: il principio è strettamente connesso al principio di minimizzazione dei dati e implica che il tempo di conservazione sia il minimo necessario per conseguire la finalità;
(vi) *integrità e riservatezza*: le pubbliche amministrazioni devono garantire che i dati siano trattati in modo da garantire la necessaria sicurezza degli stessi, adottando le opportune misure tecniche e organizzative.

Ferma restando l'applicazione di tali principi generali sia per le attività privatistiche che pubblicistiche, come anticipato, non possono, tuttavia, essere taciute le peculiarità della normativa privacy applicabile al soggetto pubblico (o privato quando svolge attività di rilevanza pubblicistica)[29].

Una prima caratteristica generale da sottolineare è che il regime pubblicistico del trattamento dei dati, rispetto a quello privatistico, è maggiormente rimesso alla discrezionalità degli Stati membri e, dunque, le discipline nello spazio eurounitario risultano maggiormente diversificate.

Il GDPR, difatti, ha recepito l'esigenza di lasciare ampio margine di libertà agli Stati allorquando il trattamento dei dati sia connesso con la gestione di assetti pubblicistici. Ciò si deduce già dalla lettura dei considerando, in particolare, del considerando 10 nella parte in cui chiarisce che: «per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è

24. Cfr. D'Ancona 2018, p. 4 e Carullo 2020, pp. 131-163.
25. *Ivi*, p. 132.
26. In questa sede, si è scelto di soffermarsi sui principi generali in materia di privacy come selezionati nell'ambito dell'art. 5 GDPR.
27. Per una ricostruzione del contenuto dei principi evidenziati si veda Ponti 2023, p. 18.
28. Cfr. considerando 39.
29. Lo si ribadisce: la classificazione fatta propria dal GDPR per distinguere la disciplina applicabile ad un certo titolare del trattamento è sostanziale: *ex multis*, cfr. Granmar 2021, p. 230: «(a)s a starting point, any natural or legal person can shoulder the role as 'controller' since there are no inherent characteristics that distinguish the legal entity called controller from other natural or legal persons. It is the fact that the legal entity 'determines the purpose and means of the processing of personal data' that classifies a 'natural or legal person, public authority, agency or other body' among controllers. This causes the EDPB to advocate a casuistic and factual rather than formal conceptual construction».

investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento»[30].

Tale peculiarità, che stride con la volontà che ha guidato il legislatore eurounitario all'adozione del Regolamento, quella cioè di assicurare una disciplina il più possibile uniforme tra gli Stati, si spiega in considerazione di più fattori, alcuni più politici che giuridici[31].

Tuttavia, un fattore preliminare – prettamente giuridico – da considerare consiste nel fatto che le tradizioni di diritto amministrativo dei vari membri dell'Unione sono, di base, molto variegate, con una conseguente maggiore difficoltà di *reductio ad unum*.

Quindi, la prima peculiarità del trattamento dei dati personali nell'ambito pubblicistico è costituita proprio dall'assenza di una normativa europea davvero uniforme alla luce dei margini di discrezionalità lasciati, dallo stesso Regolamento, agli Stati[32].

Oltre alla menzionata peculiarità di carattere generale, la disciplina privacy, nel pubblico, assume ulteriori specificità di disciplina.

Tra queste si può citare, innanzitutto, l'aspetto della base di liceità[33]: difatti, nell'esercizio delle sue funzioni, la PA si avvale principalmente di due delle basi di liceità enucleate dall'art. 6: (*i)* l'obbligo legale e (*ii)* la necessità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di un titolare di trattamento[34] in forza dell'art. 6, par. 1, rispettivamente lett. c) ed e)[35].

Tali basi di liceità possono essere previste, oltre che dal diritto dell'Unione, anche dal diritto dello Stato membro (a riprova della rilevanza della normativa nazionale)[36].

Pertanto, mentre il privato si avvale, tradizionalmente, *in primis*, della base rappresentata dal consenso, le pubbliche amministrazioni o il privato che esercita funzioni pubbliche, solitamente, si avvalgono delle lettere c) ed e)[37].

Ciò non esclude, naturalmente, *tout court*, che la pubblica amministrazione possa trattare dati sulla scorta del consenso (o di altre basi giuridiche) ma esso presenta degli aspetti di criticità nel rapporto pubblicistico. Sul punto, è opportuno citare, oltre alla dottrina[38], il considerando 43 del GDPR laddove pone l'accento sulla minor probabilità che in un rapporto pubblicistico il privato presti un

30. Il tema dell'ampio "spazio di manovra" degli Stati è stato, a più riprese, sottolineato da attenta dottrina, *ex multis*, si veda Ponti 2023, p. 27.
31. Si rinvia, per una più compiuta ricostruzione, all'analisi di Ponti 2023.
32. Per una ricostruzione delle discipline in materia nei vari ordinamenti si veda, *ex multis*, Ponti 2023.
33. Cfr. Davies 2016, p. 294.
34. Cfr. Cardarelli 2021.
35. La lettera dispone che il trattamento è lecito quando «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento».
36. Il testo del GDPR è molto simile a quello della precedente Direttiva in materia, la n. 46 del 1995, all'art. 7, lett. e): «Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando (…) e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati». Tuttavia, nonostante le disposizioni siano pressoché identiche, molto diverso è l'impatto sui regimi nazionali delle fonti che contengono tali disposizioni (direttiva/regolamento).
37. Cfr. Carullo 2020, p. 131 «(n)é, del resto, parrebbe che tale previsione possa essere censurata alla luce del contesto normativo sovranazionale in cui si inserisce. Da un lato, la base giuridica del Regolamento è assicurata dall'art. 16 TFUE, dall'altro, l'art. 8, paragrafo 2, della Carta dei diritti fondamentali dell'Unione Europea ammette espressamente che i dati personali possano essere trattati, oltre che in base al consenso della persona interessata, anche sulla base di un altro fondamento legittimo previsto dalla legge».
38. Franca 2023, p. 341 «Si è avuto più volte modo di rilevare i limiti dovuti alla costruzione dei trattamenti sulla base di logiche consensuali, in ragione dello squilibrio informativo che contraddistingue il rapporto tra titolare e interessato».

consenso libero (cfr. considerando 43: «al fine di preservare la libertà di prestare il consenso, questo non può essere utilizzato come base giuridica qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica»)[39].

2.1. La base di liceità di cui all'art. 6, par. 1, lett. e)

Come anticipato, la lettera e) dell'art. 6, par. 1, è una delle basi di liceità più utilizzate dalle amministrazioni ed è anche una di quelle norme che ha destato maggiori tensioni con i principi di diritto amministrativo, in particolare, il principio di legalità.

È, dunque, opportuno effettuare un passo indietro per poi inquadrare tali *querelle*; il GDPR, per ritenere lecito il trattamento effettuato ai sensi della lett. e), richiede l'integrazione di specifici requisiti: innanzitutto, il trattamento in oggetto deve essere «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento». In secondo luogo, il GDPR impone il rispetto di un secondo requisito per avvalersi della lettera e) citata: l'esecuzione di tale compito pubblicistico può giustificare un trattamento se esiste una norma, nazionale o eurounitaria, di copertura (in forza dell'art. 6, par. 3, lett. b).

Il primo requisito fa riferimento alla c.d. clausola di necessarietà. Tale clausola non si applica solo in relazione alla lettera e) bensì a tutte le basi di liceità contenute nell'art. 6: essa implica che il trattamento sia lecito nella misura in cui si ponga come necessario per la realizzazione dell'attività in vista del quale viene effettuato (tale attività, come detto, può essere non solo l'esecuzione di un compito di interesse pubblico ma anche l'esecuzione di un contratto, l'adempimento dell'obbligo legale, la salvaguardia di interessi vitali e così via)[40].

Il secondo requisito, invece, chiarisce che la finalità pubblica nel trattare i dati non può essere presunta dalla mera qualifica, ad esempio, di soggetto pubblico[41] ma deve trovare un fondamento normativo[42], sia esso interno o eurounitario.

Orbene, tale secondo requisito è essenziale perché è tramite le norme – alle quali il Regolamento rinvia e che vanno a declinare il potere o lo scopo pubblico – che si riesce a comprendere quali finalità del trattamento sono perseguibili e, quindi, se è integrata o meno la base di liceità di cui alla lettera e).

Circa le caratteristiche che devono presentare le citate norme per poter fungere da adeguata base giuridica ai fini del trattamento si è sviluppato un dibattito in dottrina.

Infatti, tradizionalmente si afferma che, in forza del GDPR, è sufficiente che la base giuridica assegni all'amministrazione un certo potere pubblico o, addirittura, la tutela di un certo interesse o scopo pubblico. In altri termini, non è richiesto che la base giuridica disciplini anche il trattamento dei dati, individuando le finalità di trattamento ammissibili alla luce di un certo potere pubblico[43].

Ciò implica che se la PA ha il potere, ad esempio, di adottare un provvedimento di aggiudicazione di

39. Per una disamina del tema del consenso nell'ambito dei rapporti autoritativi privati/pubbliche amministrazioni: Carullo 2017, p. 48 ss.
40. Per approfondire si veda Ponti 2023 il quale si sofferma sul rapporto tra la clausola di necessarietà e il principio di legalità dell'azione amministrativa, ponendo altresì in luce come, in verità, il modo in cui opera la clausola di necessarietà riprende il meccanismo di funzionamento del potere implicito in quanto la norma si limita a fissare uno scopo e non il potere strumentale al raggiungimento dello scopo.
41. Sotto questo profilo, esiste una profonda differenza rispetto al regime precedente, soprattutto alla luce di come era stato declinato in Italia: la Direttiva 95/46/CE prevedeva che fossero leciti quei trattamenti necessari «per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» e, non faceva riferimento ad una norma specifica di copertura ma, era sufficiente, che quel trattamento rispondesse ad uno degli scopi pubblici perseguiti da un certo ente pubblico.
42. Il GDPR ha ripreso all'art. 6, par. 1, lett. e) il disposto della Direttiva 95/46/CE, all'art. 7 comma 1 lett. e). Tuttavia, nonostante la assimilabilità delle due disposizioni, le stesse hanno un impatto profondamente diverso.
43. Cfr. così Allena–Vernile 2022.

un bando, implicitamente ha il potere di trattare anche i dati personali a tale fine.

Tuttavia, attenta dottrina ha rilevato come una simile impostazione si ponga in violazione del principio di legalità[44].

Tale dottrina rileva sul punto che lo schema del Regolamento, se così interpretato, risponde al modello del potere implicito[45] («(t)ale potere (quello speso nel trattamento dei dati personali ai fini dell'esercizio di compiti di interesse pubblico) si declina però secondo lo schema del potere implicito, dal momento che esso non risulta attribuito esplicitamente dalla norma, ma assegnato in modo innominato: sono leciti tutti i trattamenti che risultino necessari all'esecuzione di un compito di interesse pubblico ovvero connessi all'esercizio di pubblici poteri»[46]).

Si tratta, dunque, di uno schema che, lo si ripete, non sembra totalmente conforme al principio di legalità, specie se si considera la legalità in senso forte, come declinata dalla più accreditata dottrina e giurisprudenza[47], in base al quale la legalità dell'azione pubblica – per dirsi rispettosa degli standard dello Stato di diritto – deve non solo attribuire il potere in modo esplicito ma anche descriverne le modalità di esercizio.

È pur vero che, per converso, richiedere per ogni trattamento che sia autorizzato e disciplinato da una specifica norma di legge rischia di essere molto gravoso per il sistema nel suo complesso.

A tal proposito, una parte della dottrina evidenzia come la tesi più rigida, c.d. dualista, a parte essere complessa sul piano applicativo, sarebbe *tout court* da escludersi su una base puramente teorica. Sul punto, viene sottolineato che tale interpretazione andrebbe, nella sostanza, a rendere inutile in radice la differenza tra le basi giuridiche dell'obbligo di legge e l'esecuzione del compito di rilievo pubblicistico, facendole nella sostanza coincidere e privando, in tal modo, di significato innovativo dell'ordinamento la base giuridica costituita dall'esecuzione del compito pubblicistico[48].

Vale la pena evidenziare che la richiamata impostazione sembra muovere, in radice, da una diversa categorizzazione del potere di trattamento dei dati da parte dei soggetti pubblici. Più nello specifico,

44. Per una puntuale ricostruzione della questione si veda Ponti 2023, p. 48 ss.

45. La teoria dei poteri impliciti deve molto alla tradizione giuridica statunitense: difatti, all'art. 1, sez.8, ult. comma della Costituzione Usa, viene riconosciuto al Congresso il potere di emanare ogni legge necessaria e opportuna al fine di esercitare i poteri tipici: «(t)o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof».

46. Ponti 2023, p. 47.

47. Per quanto concerne il principio di legalità nel diritto amministrativo, il tema ha una portata molto ampia e non può essere trattato in tale contesto e sul punto si rimanda alla enorme letteratura sul punto. Tuttavia, in sintesi, si rileva che, come noto, il principio di legalità può essere concepito in tre diverse accezioni: la prima è la c.d. legalità debolissima, la seconda quella debole e la terza c.d. forte. Per la prima accezione, l'amministrazione può fare tutto quello che non è vietato dalla legge. Per la seconda, il potere amministrativo deve avere un fondamento legale. In ultimo, l'accezione della legalità in senso forte, anche detta in senso sostanziale, implica che non sia sufficiente che vi sia una legge che riconosce il potere ma la stessa deve disciplinare il potere in questione, disciplinando le modalità di esercizio dello stesso. Tale accezione è stata confermata dalla Corte costituzionale in molteplici occasioni (cfr. *ex multis*, sentenze 307/2003, 32/2009, 115/2011). La ragione di tale posizione della Corte si spiega in quanto un principio di legalità solo formale andrebbe a lasciare troppa discrezionalità in capo alla PA così, *de facto*, non andando a tutelare i soggetti destinatari dell'azione amministrativa.

48. Franca 2023, p. 90 laddove evidenzia che: «(s)e, infatti, il trattamento per l'esecuzione di un compito a rilevanza pubblica richiede una norma espressa che lo legittimi, non si capirebbe in che modo una simile norma si differenzierebbe da quella che disciplina come obbligatorio un trattamento. È evidente invece che in un caso (quello dell'obbligo di legge) c'è una norma che disciplina un obbligo di trattamento, consumando qualsiasi valutazione in ordine all'*an* del trattamento, mentre nell'altro caso (compito a rilevanza pubblicistica) la norma rileva per disciplinare il compito a rilevanza pubblicistica in sé, mentre il trattamento è consentito se necessario a perseguire il compito a rilevanza pubblicistica previsto dalla norma».

tale lettura, sembra ritenere che il potere di trattare il dato personale non costituisca un autonomo potere pubblicistico ma una sorta di potere "neutro", strumentale a quello pubblicistico. Dunque, aderendo alla predetta tesi, si supera in radice la *querelle* della conformità del suddetto potere di trattamento con il principio di legalità o, in generale, con i tradizionali canoni pubblicistici[49].

Sulla base di tale premessa, sarebbe solo il potere pubblico "effettivo", che è quello che attribuisce la finalità pubblicistica al trattamento, che deve rispondere ai canoni imposti per l'attività amministrativa[50].

In ogni caso, a prescindere dalla menzionata questione, il GDPR chiarisce che le norme, su cui si fonda il trattamento, possono poi andare ad aggiungere ulteriori elementi da tenere in considerazione; per esempio, esse possono prevedere: condizioni di liceità del trattamento, categoria di dati suscettibili di trattamento, periodi di conservazione dei dati, misure di garanzie e di protezione del dato personale etc.

È proprio nella fase di dettaglio che si esplica il potere degli Stati, il loro spazio di manovra (in Italia, il legislatore ha deciso di esercitare il suo spazio di manovra, scelta opzionale e non necessitata, a differenza del precedente regime delineato dalla Direttiva 95/46/CE, da ultimo, con il d.lgs. n. 101 del 2018, come modificato nel 2021[51]).

Si noti che, alla stregua di quanto chiarito al considerando 41 del regolamento, la base giuridica non deve essere necessariamente una fonte primaria ma è sufficiente che tale base giuridica, anche di altro livello nella gerarchia delle fonti, sia chiara, precisa e accessibile e la sua applicazione possa essere prevedibile per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo. In questo senso, il legislatore italiano, nel 2021, nel riformulare l'art. 2-*ter*, co. 1 del Codice privacy, *sembrerebbe* aver previsto che la base giuridica rilevante per i trattamenti relativi all'esecuzione di compiti a rilevanza pubblicistica possa essere disciplinata non solo da una norma di legge o regolamento, ma da atti amministrativi generali[52].

Sempre in quel contesto riformatore del 2021, lo stesso è andato poi anche a specificare, affermando la bontà della prima tesi esposta che riprende il

49. Ad esempio, se l'amministrazione tratta i dati personali nell'ambito della procedura concorsuale, il trattamento dei dati *ex se*, non costituirebbe un vero e proprio potere autoritativo e, quindi, non sarebbe soggetto ai canoni del diritto amministrativo.

50. Franca 2023, p. 99: «(i)n particolare, il fatto che l'azione della pubblica amministrazione sia soggetta al principio di legalità spiega perché non sia necessario (e, anzi, si riveli pleonastico) richiedere che la norma di disciplina dell'attività amministrativa sia "doppiata" da una norma che disciplina i trattamenti ad essa connessa: in tal modo, infatti, si perverrebbe ad un aggravio eccessivo e ingiustificato. Se la norma disciplina un potere o un compito dell'amministrazione rispetto a cui il trattamento di dati si pone in chiave di strumentalità necessaria, è giocoforza che la norma stessa costituisca la base del trattamento».

51. Per una ricognizione dell'esperienza italiana, la quale ha oscillato da un estremo all'altro nelle scelte regolatorie del settore si rimanda a Ponti 2023, p. 92 ss. L'autore, sul punto, a p. 95 del citato scritto evidenzia che: «(m)entre in precedenza si statuiva che il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari fosse consentito anche in mancanza di una norma di legge o di regolamento che lo prevedesse espressamente, la nuova formulazione utilizza l'avverbio esclusivamente, ciò che è stato inteso nel senso di attrarre nella base giuridica non solo la qualificazione della fonte ("esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento"), ma anche ciò che in precedenza poteva restare fuori dalla fonte legislativa ("Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito (…) anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente"). In base a questa lettura, pertanto, la base giuridica (legislativa, o regolamentare, se a ciò espressamente abilitata) non può limitarsi ad individuare ed affidare al titolare del trattamento l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri, ma deve (quantomeno) prevedere espressamente quale trattamento (di quali dati, e per quale finalità) possa essere realizzato».

52. Per una sintesi dei tratti distintivi tra regolamento e atto amministrativo generale si veda Consiglio di Giustizia amministrativa per la Regione siciliana, 14 marzo 2011, n. 200, che a sua volta richiama l'Adunanza Plenaria del Consiglio di Stato.

meccanismo di funzionamento dei poteri impliciti, che il trattamento «è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti» (cfr. art. 2-*ter* co. 1-*bis*)[53].

Recente dottrina ha, tuttavia, evidenziato che la riforma italiana non sarebbe pienamente conforme al GDPR in quanto lo stesso «pur lasciando agli Stati membri la scelta su quali misure adottare per specificare l'applicazione del Regolamento 2016/679/UE, richiede tassativamente che la base giuridica del trattamento dei dati personali sia proporzionata all'obiettivo legittimo perseguito»[54]. In altri termini, secondo la citata impostazione, la normativa italiana non sarebbe compatibile con la fonte eurounitaria in quanto, *de facto*, con l'ultimo intervento normativo del 2021, il legislatore italiano ha autorizzato, in via generale, il trattamento di dati personali e lo scambio di tali dati tra autorità pubbliche ogniqualvolta questo sia necessario per il perseguimento di fini istituzionali, senza menzionare il principio proporzionalità tra trattamento dei dati e fini pubblici perseguiti, espressamente richiesto dal GDPR.

Peraltro, la riflessione dottrinaria riportata può costituire spunto per effettuare un'ulteriore valutazione relativa al rispetto del canone di proporzionalità interno sotteso all'azione amministrativa[55].

L'amministrazione è, inoltre, tenuta: (i) a fornire corretta informativa circa le finalità del trattamento, i tipi di dati raccolti, i destinatari e i loro diritti di protezione dei dati; (ii) alla nomina di un responsabile della protezione dei dati; (iii) a predisporre le opportune misure di sicurezza per proteggere i dati dall'esterno (attacchi *hacker* etc.).

Ancora, norma fondamentale per il corretto rispetto dall'assetto delineato dal GDPR da parte delle pubbliche amministrazioni è l'art. 30. In base a tale disposizione, le pubbliche amministrazioni devono adottare il registro dei trattamenti che deve contenere: il nome e i dati di contatto del titolare del trattamento e del DPO; le finalità del trattamento; la descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; i termini ultimi previsti per la cancellazione delle diverse categorie di dati; una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione.

Già in base a tale breve ricognizione del sistema del GDPR si possono dedurre due aspetti: il primo è che il regime pubblicistico del trattamento dei dati, ferma l'applicazione dei principi generali, presenta delle peculiarità molto rilevanti; il secondo è che tale regime, anche solo osservando la disciplina del GDPR, non è del tutto lineare e, spesso, non combacia con i principi generali (per esempio, principio di legalità) dell'azione amministrativa.

3. Il Regolamento sulle intelligenze artificiali: la filosofia di fondo

Come è noto, l'Unione europea ha adottato[56] la prima regolamentazione in materia di intelligenza artificiale[57].

L'adozione del Regolamento si colloca nell'ambito di una più ampia strategia europea volta a governare il mercato dei dati[58]. In questo senso, il

53. Francario 2021.

54. Carullo 2024.

55. Tuttavia, la preoccupazione evidenziata dalla dottrina richiamata cfr. Carullo 2024 sembra essere superata considerando che l'art. 2-*ter* del Codice privacy, come risultante dall'ultima modifica intercorsa, richiama espressamente l'art. 6 GDPR, il quale richiama, a sua volta, il principio di proporzionalità.

56. Si tratta del Regolamento n. 1689/2024.

57. Nonostante sia recente il massivo riferimento al concetto di *Artificial Intelligence* (AI) sia a livello mediatico che accademico, tale concetto non è così nuovo. Il termine è stato coniato negli anni Cinquanta del secolo scorso, in un contesto accademico, per indicare un campo di ricerca emergente che studia: (i) la capacità delle macchine di svolgere compiti mostrando un comportamento intelligente simile a quello umano; e (ii) la capacità delle macchine di comportarsi come agenti intelligenti percependo l'ambiente e prendendo decisioni per raggiungere determinati obiettivi cfr. Medaglia–Gil-Garcia–Pardo 2023.

58. La strategia europea per i dati ha preso le mosse da una comunicazione della Commissione europea del 19 febbraio 2020, COM(2020) 66, ove si evidenziava la centralità dei dati in quanto gli stessi rappresentano «(…) la

Regolamento è solo una delle iniziative che dovrebbe concorre a creare una gestione unica del mercato dei dati nello spazio dell'Unione europea[59]. Uno dei comuni denominatori delle iniziative citate è il riconosciuto valore patrimoniale del dato quale linfa vitale per il funzionamento delle nuove tecnologie: il legislatore eurounitario, difatti, sebbene tuteli il diritto alla privacy e, quindi, i dati personali[60], è consapevole delle istanze delle imprese europee e dell'esigenza di renderle competitive a livello mondiale. Il riconosciuto valore patrimoniale del dato emerge già in sede di considerando (in particolare dai considerando 3 e 4) laddove si evidenzia la centralità strategica nell'implementazione della tecnologia e, in particolare, della famiglia delle intelligenze artificiali «contribuendo al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi»[61].

Chiarito che il Regolamento sulle IA non è un'iniziativa *stand alone*, bisogna pur evidenziare che la stessa assume un particolare significato anche considerata singolarmente, un significato prima politico che giuridico[62] poiché, come evidenziato da gran parte della dottrina intervenuta anche ante adozione del testo definitivo[63], soprattutto alla luce del fatto che si tratta del prima fonte di carattere

linfa vitale dello sviluppo economico: sono la base di molti nuovi prodotti e servizi e generano guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici, rendendo possibili prodotti e servizi più personalizzati, un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici. Sono, inoltre, una risorsa essenziale per le start-up e le piccole e medie imprese (PMI) per quanto concerne lo sviluppo di prodotti e servizi. La disponibilità di dati è essenziale per l'allenamento dei sistemi di intelligenza artificiale, con prodotti e servizi in rapida evoluzione, da riconoscimento morfologico e insight generation a tecniche di previsione più sofisticate e, di conseguenza, decisioni migliori».

59. Tra gli atti normativi che confluiscono nella regolazione del settore si possono citare: il *Data Governance Act*; il *Data Act*; il *Digital Services Act* e il *Digital Markets Act*. Si rimanda, per un'analisi più approfondita a Falletta–Marsano 2024, p. 121.

60. *In primis* tramite il GDPR ma anche, come noto, negli anni, un importantissimo strumento di protezione è stata (ed è) la Convenzione europea dei diritti dell'uomo, in particolare in forza dell'art. 8, insieme alle relative pronunce della CEDU.

61. Cfr. considerando 4 Regolamento IA.

62. L'Europa, come evidenziato in premessa, si è attribuita il ruolo di leader mondiale di regolazione del fenomeno. La definizione di sistema di intelligenza artificiale di cui all'articolo 3, paragrafo 1 è stata modificata per allinearla maggiormente al lavoro delle organizzazioni internazionali che si occupano di intelligenza artificiale, in primis l'OCSE. Di ciò si ritrova traccia nel considerando 12 del Regolamento: «la nozione di «sistema di IA» di cui al presente regolamento dovrebbe essere definita in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale (…)».

63. De Gregorio–Paolucci–Pollicino 2021.

generale e di *hard law* al mondo[64], l'Unione europea si è posta come leader nella regolazione del settore a livello mondiale. A riprova del ruolo di *leadership che ha assunto il diritto unionale*, occorre evidenziare, senza pretese di completezza, come l'esperienza di altre legislazioni mondiali, sebbene intervenute in materia, abbiano un impatto minore. Per esempio, negli Stati Uniti, nell'ottobre 2023, l'amministrazione Biden ha emesso un *Executive Order* avente ad oggetto l'uso sicuro e protetto dell'intelligenza artificiale: *Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*[65].

Orbene, tale intervento, non ha la medesima forza dell'*AI Act* e ciò sotto almeno due punti di vista.

In primo luogo, non è equivalente dal punto di vista della qualità della fonte: difatti, l'*executive order* non ha la forza e la stabilità di un Regolamento eurounitario. L'*executive order* è un atto dotato di coattività ma è imputabile al solo esecutivo, in particolare al Presidente degli Stati Uniti, senza che vi sia alcuna "ratifica" da parte del Parlamento. Ciò significa che è, per sua natura, meno stabile. Inoltre, tale fonte può rivolgersi solo agli organi dell'esecutivo stesso e, quindi, non può regolare direttamente gli organi posti al di fuori dell'esecutivo o i soggetti privati[66].

Sotto il profilo, invece, contenutistico mentre l'*AI Act* pone numerosi e specifici obblighi, l'*Executive Order* non contiene particolari oneri o prescrizioni ma, tendenzialmente, si "limita" ad esporre dei principi generali e a prevedere lo sviluppo di linee guida e di *best practices* da parte delle amministrazioni. Si può, quindi, affermare che l'approccio statunitense al tema sia più *soft*[67].

L'impatto del Regolamento IA, tuttavia, non si esaurisce nel significato politico e di *leadership* europeo: infatti, lo stesso sottende una precisa scelta regolatoria che possa bilanciare le esigenze di avanzamento tecnologico con il rispetto dell'uomo. Rispetto dell'uomo che non pare intendersi solo come rispetto dei diritti umani ma anche come tutela della "centralità umana" in ogni processo che abbia un impatto rilevante.

In questo senso, almeno "a parole", il regolamento sembra richiamare dei concetti di diritto naturale volendo «rimodulare il perimetro del tecnicamente possibile sulla base di quello che si ritiene giuridicamente ed eticamente accettabile»[68].

La nuova disciplina, dunque, ha recepito un'impostazione antropocentrica dell'intelligenza artificiale[69]: l'uomo dovrebbe essere al centro della rivoluzione tecnologica. Ciò viene confermato anche dall'art. 14 del Regolamento, dedicato alla

64. Prima dell'adozione del regolamento vi erano stati molteplici tentativi, anche europei, di regolare tramite *soft law*: tra questi, le *Linee guida relativa ai principi sull'intelligenza artificiale* dell'OCDE e la raccomandazione del Consiglio d'Europa adottata il 14 maggio 2019 (si tratta di una regolamentazione che «aveva mantenuto il livello della discussione sul piano dei principi»). Nel 2021, si è compiuto poi il passaggio cruciale mediante la Risoluzione del Parlamento europeo sull'intelligenza artificiale e con la presentazione del Regolamento IA poi approvato, in via definitiva, dal Parlamento europeo, il 13 marzo del 2024.

65. Oderlberg 2024.

66. Cfr. Esposito 2023 e Pollicino 2023.

67. Colpisce, inoltre, la considerazione del peso dei privati nello sviluppo regolatorio sul tema. Si legge, nel testo del provvedimento del Presidente Biden, che «executive departments and agencies shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations».

68. Anche se il valore etico ed antropocentrico è stato oggetto di riflessioni della dottrina ante adozione, cfr. De Gregorio–Paolucci–Pollicino 2021.

69. Il primo considerando del Regolamento indica, in questo senso, che il suo scopo è quello di «migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»),

"Sorveglianza umana", nell'ambito del quale si evidenzia la necessità, per i sistemi di alto rischio, di un pregnante controllo da parte dell'uomo.

3.1. Le norme del Regolamento IA più rilevanti per l'attività pubblicistica

Il Regolamento, già nei suoi considerando, si dimostra sensibile al tema del rapporto tra gli interessi pubblici ed i connessi rischi applicativi delle intelligenze artificiali.

Il considerando 5, difatti, evidenzia come l'intelligenza artificiale possa «(…) a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico»[70].

In questo senso, il considerando 7 rileva che è fondamentale costituire un quadro giuridico armonizzato in tale materia al fine di garantire che lo sviluppo delle IA non vada a sacrificare «un elevato livello di protezione degli interessi pubblici».

Ancora, il considerando 167 afferma che i soggetti chiamati ad applicare il regolamento devono fare in modo di operare nel rispetto della riservatezza al fine di garantire «l'integrità del procedimento amministrativo».

Alla luce di ciò, è possibile evidenziare la piena consapevolezza, da parte del legislatore eurounitario, della specialità del settore pubblico, soprattutto in considerazione dei maggiori rischi sull'impatto dei diritti, che l'utilizzo di una tecnologia avanzata nel settore pubblico potrebbe comportare.

Ciononostante, l'impalcatura del Regolamento non prevede dei regimi apertamente differenziati tra l'uso delle tecnologie nell'attività privata o nell'attività pubblicistica ma li regola insieme, sebbene vi siano delle norme, come si vedrà, che hanno principalmente una vocazione pubblicistica.

È opportuno, dunque, in estrema sintesi, muovere dall'analisi delle principali norme del Regolamento.

L'art. 3 del Regolamento reca la definizione di sistema di IA da intendersi come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[71].

Alla luce di ciò, un sistema di IA rientra nell'ambito di applicazione del Regolamento allorquando (i) presenti un qualche livello di autonomia rispetto all'uomo, (ii) abbia una qualche capacità di apprendimento, potendo generare sulla base degli input, degli output, (iii) gli output devono poter influenzare un ambiente fisico o virtuale.

La normativa neo approvata si fonda su un *risk based approach*: ossia, vengono distinte le intelligenze artificiali a seconda del pericolo che le stesse potrebbero causare ai diritti fondamentali[72].

Più alto è il rischio più la regolamentazione è stringente.

Il considerando 48 chiarisce che, per valutare l'impatto in termini di rischio, uno strumento importante è rappresentato dalla Carta dei diritti fondamentali dell'Unione europea: «(l)a portata dell'impatto negativo del sistema di IA sui diritti

compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione (…)» (cfr. anche art. 1 del Regolamento).

70. Cfr. considerando 5.

71. Sulla definizione di IA cfr. Martinez 2019 e Wang 2019.

72. Puckzo 2024: «The European Union (EU) has been at the forefront of regulating AI ethics, primarily through the General Data Protection Regulation (GDPR) and the proposed AI Act. The GDPR, enacted in 2018, sets stringent guidelines on data protection and privacy, directly impacting AI systems that process personal data. Key principles of the GDPR include data minimization, purpose limitation, and the right to be informed about automated decision-making. These principles ensure that AI systems are designed with privacy in mind, protecting individuals' data from misuse and unauthorized access. In addition to the GDPR, the EU has proposed the AI Act, which seeks to establish a comprehensive legal framework for AI. The AI Act categorizes AI applications into different risk levels (unacceptable, high, and minimal risk) and imposes corresponding regulatory requirements».

fondamentali protetti dalla Carta è di particolare rilevanza ai fini della classificazione di un sistema di IA tra quelli ad alto rischio. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione».

Andando più nello specifico, all'interno del Regolamento, si distinguono quattro principali tipologie di rischio:

(i) *Il rischio è inaccettabile* e, dunque, l'uso delle IA è totalmente vietato. A tal fine, è l'art. 5 che elenca le pratiche IA vietate. In base alla citata norma sono vietati, *ex multis*: i sistemi di IA che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli volte a distorcere il comportamento delle persone (cfr. art. 5, par. 1, lett. a); i meccanismi di sfruttamento delle persone vulnerabili (cfr. art. 5, par. 1, lett. b); i sistemi di IA che introducano meccanismi di *scoring* sociale (cfr. art. 5, par. 1, lett. c)[73]; i sistemi che effettuino indagini di polizia predittiva, con alcune eccezioni (cfr. art. 5, par. 1, lett. d)[74]; categorizzazione biometriche da cui dedurre razza, convinzioni religiose politiche o filosofiche, orientamenti sessuali etc. (cfr. art. 5, par. 1, lett. g); i sistemi che possano interferire relativamente alla privacy mentale delle persone, sui luoghi di lavoro o di istruzione, decodificando emozioni e così via, con alcune eccezioni costituiti da motivi di salute o di sicurezza (cfr. art. 5, par. 1, lett. f); i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a meno che la ricerca non sia volta a fini specifici collegati alla sicurezza pubblica; tra i fini specifici, per esempio, si annoverano la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; la prevenzione di una minaccia specifica, come un attacco terroristico; ricerca di soggetti sospettati di aver commesso un reato grave etc. (cfr. art. 5, par. 1, lett. h).

(ii) *Il rischio è alto* e, dunque, si pongono a carico di produttori e sviluppatori di tali sistemi stringenti obblighi *ad hoc* che riguardano ogni fase del ciclo di vita della IA (progettazione, collaudo, monitoraggio, nonché responsabilità aggiuntive)[75]. il Regolamento impone poi, per i sistemi ad alto rischio, l'adozione di un sistema di gestione del rischio nonché l'obbligo di effettuare dei test e di garantire, oltre

73. Più precisamente, l'art. 5, par. 1, lett. c) si riferisce alla «(…) immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità».

74. La norma così dispone: «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»; la lettera f) che vieta «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza».

75. Cfr. artt. 9 e ss. del Regolamento.

alla citata sorveglianza umana, anche l'accuratezza, robustezza e cybersecurity. Il rispetto di tutti i menzionati requisiti è richiesto per il rilascio, da parte dell'Autorità competente, della valutazione di conformità dell'IA.

(iii) *Il rischio è basso* o minimo; simili tecnologie non sono sottoposte a particolari obblighi ma devono, comunque, garantire i principi della trasparenza e robustezza.

(iv) Sussiste un rischio specifico attinente alla tutela della trasparenza.

In base alla riassunta classificazione, si può effettuare, anche se "a caldo", con tutte le approssimazioni del caso, il seguente ragionamento.

Innanzitutto, è possibile notare che alcune tecnologie inaccettabili (IA a rischio inaccettabile) diventano accettabili allorquando siano volte a realizzare dei fini pubblicistici. Per esempio, come detto, il Regolamento vieta, all'art. 5, par. 1, lett. f), «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione» a meno che l'uso del sistema di IA sia volto a realizzare interessi pubblici della tutela della salute e della sicurezza (testualmente si legge nel Regolamento «motivi medici o di sicurezza»).

Quindi, talvolta, l'interesse pubblico potrebbe rendere più permissiva la disciplina applicabile.

Tuttavia, per converso, come ben esplicitato dal soprariportato considerando 48, per parametrare il rischio accettabile e il rischio non accettabile bisogna valutare anche l'impatto sui diritti fondamentali e, in particolare, anche il diritto ad una buona amministrazione. In questo senso, l'inserimento dell'uso dell'intelligenza artificiale nel procedimento amministrativo può rappresentare qualche complessità in più.

Quindi, in forza dei sintetici ragionamenti svolti, lo si ripete, con buona approssimazione, sebbene sia senz'altro vero che l'attività pubblicistica non presenti una disciplina generale differente o rafforzata rispetto a quella privata (come detto, il Regolamento non prevede che l'uso delle IA nell'ambito del potere pubblico comporti *ex se* un rischio più elevato) è pur vero che, sul piano della realtà, una intelligenza artificiale utilizzata per esercitare il potere pubblico presenterà, il più delle volte, un rischio maggiore per i diritti enucleati nella Carta dei diritti fondamentali dell'Unione europea.

Le peculiarità dell'attività pubblicistica nell'economia del Regolamento IA vengono in rilievo anche ai sensi dell'art. 27 dello stesso, relativa ai sistemi ad alto rischio. L'articolo 27 prevede che: «(p)rima di utilizzare un sistema di IA ad alto rischio (…) i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici (…) effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre». La norma chiarisce, inoltre, che tale valutazione debba comprendere una serie di elementi: a) una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

In base alla citata norma i *deployer* che esercitano attività pubblica e che utilizzano sistemi di IA ad alto rischio devono effettuare una valutazione di impatto sui diritti fondamentali (c.d. *Fundamental Rights Impact Assessment*, in breve FRIA)[76].

4. Il Regolamento IA e GDPR a confronto: analogie e differenze tra le due fonti

Porre a confronto il Regolamento IA e il GDPR è una operazione necessaria perché, come detto, l'utilizzo di IA presuppone, nella quasi totalità dei casi, trattare dati personali.

Per esigenze di chiarezza espositiva, nel prosieguo, si analizzeranno quelli che appaiono, a caldo, i principali punti di contatto nonché di divergenza.

76. La "vicinanza" tra la FRIA e l'obbligo descritto dal GDPR ai fini della redazione del *Data Protection Impact Assessment* sarà oggetto di trattazione nel paragrafo 4.1.

Relativamente alle similitudini, oltre alla forma normativa prescelta, il regolamento, i due testi condividono diverse caratteristiche.

Su un piano più politico che giuridico, in entrambe le esperienze regolatorie, l'Unione europea, adottando tali legislazioni molto innovative, ha dato prova del suo ruolo di *leadership* nella regolazione del fenomeno tecnologico a livello mondiale. In questo senso, si può ragionevolmente immaginare che il Regolamento IA, così come è stato per il GDPR[77], assumerà la funzione non solo di normare lo spazio europeo ma di assurgere a modello legislativo per le legislazioni mondiali[78].

Anche da un punto di vista contenutistico, si possono scorgere analogie tra i due strumenti. Tra queste similitudini, *in primis*, si può evidenziare la *centralità dei diritti fondamentali*: entrambi i regolamenti, nell'abito del rispettivo primo considerando, fanno espresso riferimento alla necessità di garanzia di tali diritti, menzionando la Carta dei diritti fondamentali dell'Unione europea.

Ciò era pure stato evidenziato dalla dottrina intervenuta prima dell'adozione del testo definitivo dell'*AI Act* la quale, avvalendosi di una «tassonomia usuale nell'ambito degli studi di comparative law and regulation»[79], ha evidenziato che il Regolamento sulle intelligenze artificiali è costruito su «un modello regolatorio non incentrato sulla logica della ballot-box democracy, né su quella della rule by law, bensì rispondente al paradigma dei diritti fondamentali»[80].

Nel dettaglio: (i) considerando 1 GDPR: «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»; (ii) considerando 1 Regolamento IA: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione».

Inoltre, in entrambi i regolamenti, la trasparenza assume una valenza significativa in quanto strumento essenziale al fine di tutelare i diritti fondamentali delle persone: il GDPR impone diversi obblighi di trasparenza sui processi di raccolta e trattamento dei dati e l'*AI Act*, allo stesso tempo, richiede che i sistemi di intelligenza artificiale, soprattutto se ad alto rischio, garantiscano la trasparenza e la spiegabilità del risultato. Quindi, "sul piano valoriale" i due Regolamenti muovono da presupposti molto simili. Da notare che in

77. Tra i tanti esempi di legislazione straniera che si sono ispirati al modello GDPR, si può citare la legge vigente in California, USA, il c.d. *Consumer Privacy Act* (CCPA) che è la più garantista legge sulla privacy negli Stati Uniti a livello dei singoli Stati (si noti che negli USA non esiste una legge federale generale in materiale). Per approfondire si veda: Barett 2019, p. 24.

78. Si è visto come un modello alternativo regolatorio, più *soft*, possa essere quello statunitense.

79. Bignami 2018.

80. Resta 2022, p. 323 il quale evidenzia la profonda rilevanza della tutela dei diritti fondamentali nell'economia della regolazione IA europea: «(i)l cardine della proposta sembra infatti risiedere nella definizione di un modello regolatorio finalizzato alla gestione ottimale dei rischi insiti nell'utilizzo dei dispositivi IA con l'obiettivo primario di tutela dei diritti fondamentali e di salvaguardia del processo democratico. Formule di spiccato valore retorico come quella della "human-centric" o "trustworthy-AI" riflettono plasticamente l'idea che le applicazioni di IA possono incidere sul sistema di protezione della dignità umana e dei diritti fondamentali, sicché un puro modello di self-regulation risulta inappropriato. È soltanto attraverso un approccio di hard law che può realizzarsi un accettabile bilanciamento tra la tutela della persona e altri interessi concorrenti, come quello della sperimentazione innovativa e della crescita economica».

entrambi i Regolamenti, nonostante la menzionata centralità della tutela dei diritti, si registra una sensibilità al tema del necessario bilanciamento tra tale tutela e altri interessi legati allo sviluppo economico: nel caso del GDPR, l'interesse con il quale controbilanciare la tutela dei diritti è la libera circolazione dei dati, nel caso dell'*AI Act*, è la garanzia di non arrestare lo sviluppo tecnologico. Ancora, GDPR e *AI Act* condividono una spiccata tendenza alla extraterritorialità. Sul punto, è sufficiente porre a confronto l'art. 3 del GDPR e l'art. 2 del Regolamento IA: essi si applicano non solo ai soggetti che sono stabiliti nell'Unione ma anche a soggetti che siano "collegati" al mercato europeo.

Inoltre, i due strumenti aderiscono al modello del *risk based approach*[81]: più è alto il rischio di violazione dei diritti fondamentali, più gravosi sono gli obblighi imposti agli utilizzatori. Si tratta, dunque, di schemi regolatori a «geometria variabile, dove i doveri di condotta e gli itinerari di enforcement vengono modulati in funzione dei diversi livelli di rischio prevedibilmente connessi a una determinata tipologia di attività»[82]. In questo senso, il Regolamento IA riprende ed enfatizza tale metodo di regolazione basato sul rischio che è proprio anche del GDPR, come emerge dall'analisi degli artt. 25 e 35 di quest'ultimo, ove si prevedono degli obblighi per i provider di mappatura del rischio e di adottare sistemi idonei a neutralizzarlo.

Tuttavia, iniziando ad addentrarci nell'analisi degli *elementi di dissonanza* tra i due regolamenti, la declinazione del modello del *risk based approach* è differente: nel GDPR la valutazione del rischio è decentralizzata, effettuata dai soggetti direttamente coinvolti e fondata sul principio di accountability, nell'ambito dell'*AI Act* è il legislatore eurounitario che tenta di creare una categorizzazione astratta dei livelli di rischio.

In aggiunta, a monte, si può riflettere, in termini generali, sulla difficoltà che l'applicazione congiunta dei due Regolamenti comporterà: i sistemi IA necessitano di enormi quantità di dati per funzionare e, in gran parte, si tratta di dati personali; per converso, il GDPR si fonda sul principio della limitazione delle finalità del trattamento[83], che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime e il relativo riuso non sia possibile se non negli stringenti limiti individuati dalla normativa. Garantire che i dati personali immessi (moli molto significative di dati) siano trattati in modo conforme alla finalità per i quali originariamente sono stati acquisiti è estremamente complesso, se non, materialmente, impossibile. La tensione tra il principio di finalità e i sistemi di intelligenza artificiale si è registrata anche nella fase di addestramento delle stesse. Per esempio, nel noto caso *Clearview AI*[84], il Garante per la protezione dei dati personali ha sanzionato la suddetta società per aver raccolto dati al fine di addestrare un algoritmo, in aperta violazione del principio di finalità.

Sempre muovendo dal rilievo in base al quale le intelligenze artificiali sono alimentate da big data, diventa complesso garantire un altro caposaldo del GDPR la minimizzazione dei dati: difatti, anonimizzare il dato personale oltre che costituire un'operazione complessa può incidere sulla precisione dell'analisi compiuta dalla macchina.

Alla luce di quanto rilevato, pertanto, soprattutto per le IA più evolute, come quelle che si basano sul machine learning «si è determinata una inevitabile tensione con i principi cardine della normativa sul trattamento dei dati, e segnatamente con i

81. Floridi 2021.

82. Resta 2022, p. 339.

83. In dottrina cfr. Mühlhof–Ruschemeier 2024 e Trozzi 2024 i quali hanno analizzato le tensioni tra il meccanismo di funzionamento delle intelligenze artificiali e il principio di limitazione delle finalità. Sul tema, può essere anche utile richiamare la giurisprudenza relativa alle incompatibilità tra il GDPR ed i c.d. usi secondari, facendo riferimento, in particolare, al caso Digi (CGUE, sentenza del 20 ottobre 2022, *Digi Távközlési és Szolgáltató Kft. contro Nemzeti*, C-77/21).

84. Cfr. Garante per la protezione dei dati personali, Registro dei provvedimenti n. 50 del 10 febbraio 2022. Un altro esempio, sul punto, è recente caso di ChatGPT, gestita da Open AI, nell'ambito del quale il Garante ha richiesto, dopo un'approfondita istruttoria, una serie di adeguamenti, anche per garantire il rispetto del principio di finalità (cfr. Garante per la protezione dei dati personali, Registro dei provvedimenti n. 755 del 2 novembre 2024).

principi di finalità e minimizzazione»[85]; pertanto, alla luce di ciò, le scelte regolatorie in tale settore sono sottoposte ad un compromesso necessario tra le esigenze di sviluppo tecnologico e l'esigenza di tutela degli individui. Talvolta, nel bilanciamento, prevale la tutela della privacy, altre volte, prevale l'esigenza nell'avanzare tecnologico, con tutti i benefici che ne conseguono (tra cui, la tutela di altri diritti, diversi dalla privacy).

Un esempio di prevalenza dello sviluppo tecnologico rispetto alla tutela del dato personale, si ritrova all'art. 10, par. 5, del Regolamento IA, con riferimento alla normativa sui dati particolari. Infatti, l'art. 10, introduce una eccezione al divieto di raccolta e trattamento dei dati particolari di cui all'art. 9 GDPR, quando ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche[86].

In chiusura, è necessario valutare una delle più evidenti sovrapposizioni tra GDPR e Regolamento IA, valutando il rapporto tra l'art. 22 GDPR e l'*AI Act*: difatti, l'art. 22 GDPR contiene una disciplina relativa ad una delle ipotesi di forme di trattamento dei dati personali tramite intelligenze artificiali, occupandosi del trattamento nell'ambito di processi decisionali automatizzati[87].

L'art. 22, par. 1, del GDPR vieta i trattamenti dei dati personali nell'ambito di processi decisionali automatizzati, compresa la profilazione, che producano effetti giuridici o che incidano significativamente sulla persona[88]. Tuttavia, non si tratta di un divieto generale, in quanto, al secondo paragrafo, ammette tali processi decisionali automatizzati in tre diverse ipotesi: quando il trattamento sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; quando il trattamento sia autorizzato dal diritto interno o eurounitario, purché si garantiscano adeguate misure a tutela dei diritti dell'interessato; oppure nell'ipotesi in cui il trattamento si basi sul consenso esplicito dell'interessato.

Al contrario, il Regolamento IA non contiene alcun divieto generale relativamente alle forme di intelligenza artificiale che implichino processi decisionali automatizzati ma, al contempo, alcuni dei processi decisionali automatizzati sono *tout court* vietati in quanto considerati a rischio inaccettabile (si pensi al caso dello *scoring* sociale).

Come evidenziato in dottrina[89], sicché alcuni processi decisionali automatizzati sono, in teoria, ammissibili per il GDPR e vietati *tout court* per il Regolamento IA, contrariamente a quanto si potrebbe credere, la disciplina del GDPR non è

85. Resta 2022, p. 335.

86. Il Regolamento richiede, tuttavia, che siano soddisfatte una serie di condizioni, che devono sussistere in modo congiunto, tra le quali, per esempio, il fatto che le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi.

87. In dottrina, *ex multis*, si veda Bolognini–Pelino 2024.

88. Moltissime sono state le pronunce della giurisprudenza amministrativa in tema di processi decisionali automatizzati nell'ambito delle quali si è ammesso l'uso di tali tecnologie, con espresso richiamo anche all'art. 22 GDPR, a condizione che si garantiscano i principi del procedimento, in primis la trasparenza, in virtù della particolare efficienza che le stesse comportano, in attuazione dell'art. 97 Cost. A titolo meramente esemplificativo, la giurisprudenza si è occupata di assegnazione o trasferimenti, mediante tali tecnologie, degli insegnanti, ammettendone l'uso. Si veda, *ex multis*, la pronuncia del Consiglio di Stato, sentenza n. 8472 del 2019, ove il massimo consesso della giustizia amministrativa ha evidenziato che: «(a)nche il caso in esame, relativo ad una procedura di assegnazione di sedi in base a criteri oggettivi, l'utilizzo di una procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata: essa comporta infatti numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata». In senso conforme, può richiamarsi la pronuncia del Consiglio di Stato n. 2270 del 2019.

89. Sul tema si veda Falletta–Marsano 2024, p. 128.

sempre più limitativa o stringente rispetto a quanto disposto nell'*AI Act*.

In ultimo, in sintesi, è opportuna una breve comparazione dell'impianto sanzionatorio dei due Regolamenti[90]. Invero, il Regolamento IA e il GDPR, sotto questo profilo, condividono una impostazione molto simile sia per i meccanismi di quantificazione della sanzione amministrativa, che per la discrezionalità riconosciuta alle Autorità di vigilanza chiamate ad applicare le sanzioni.

Sotto il primo profilo, in entrambi i casi la determinazione della sanzione è effettuata mediante una percentuale del fatturato[91] del soggetto destinatario della sanzione. La percentuale è determinata in ragione della gravità della violazione. Inoltre, entrambi i sistemi riconoscono una significativa discrezionalità alle autorità di vigilanza[92]. In particolare, il Regolamento IA (cfr. art. 99, par. 7)[93], similmente al sistema GDPR (cfr. art. 83, par. 2) prevede che l'autorità di vigilanza, sia ai fini dell'*an* che del *quantum* della sanzione amministrativa, tiene conto di tutte le circostanze del caso concreto; per esempio, sono circostanze rilevanti: la natura, la gravità e la durata della violazione; il numero di persone interessate e il livello del danno da esse subito.

4.1. Ancora sul rapporto GDPR e Regolamento IA. La DPIA *versus* la FRIA: la duplicazione di adempimenti per le amministrazioni

Spostando maggiormente l'attenzione sul principale oggetto dell'indagine, ossia l'impatto sui soggetti pubblici della sommatoria tra i due Regolamenti, una particolare area di interferenza si rintraccia nell'ambito delle valutazioni d'impatto sui

90. *Ivi*, p. 129.

91. La percentuale sarà più o meno alta a seconda della gravità della violazione attuata. Cfr. art. 99 del Regolamento IA che prevede che la «non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35.000.000 EUR o, se l'autore del reato è un'impresa, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. La non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15.000.000 EUR o, se l'autore del reato è un'impresa, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente».

92. L'Autorità di vigilanza in materia di IA, come si vedrà nel prosieguo, nell'ambito dell'ultimo paragrafo, non coincide con l'Autorità in materia di privacy, il Garante per la protezione dei dati personali.

93. Art. 99, par. 7, *AI Act* prevede che: «(n)el decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e, se del caso, si tiene in considerazione quanto segue: a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA, nonché, ove opportuno, il numero di persone interessate e il livello del danno da esse subito; b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione; c) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento; d) le dimensioni, il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione; e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione; f) il grado di cooperazione con le autorità nazionali competenti al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) il grado di responsabilità dell'operatore tenendo conto delle misure tecniche e organizzative attuate; h) il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore; il carattere doloso o colposo della violazione; j) l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate». Cfr. considerando 168 Regolamento IA laddove prevede che nel valutare «l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up».

diritti fondamentali. Come detto, il Regolamento IA[94] impone al soggetto pubblico o al privato che fornisca servizi pubblici[95] di effettuare tale valutazione di impatto sui diritti fondamentali (c.d. FRIA) quando ci si avvalga di sistemi di IA classificati come ad alto rischio. Allo stesso tempo, l'art. 35 GDPR[96] prevede che quando il trattamento di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, soprattutto allorquando il rischio sia connesso all'uso di nuovo tecnologia, è obbligatorio effettuare la valutazione di impatto dei diritti fondamentali (in inglese *Data Protection Impact Assessment*, in breve DPIA).

Per comprendere se un trattamento di dati personali presenti, nel concreto, un rischio elevato, il titolare del trattamento deve considerare non solo il GDPR ma anche le Linee guida del Gruppo 29[97] nonché i provvedimenti delle Autorità di controllo nazionali.

Tra i trattamenti, che necessitano della DPIA, individuati dal Gruppo 29 vi sono: (i) trattamenti valutativi o di *scoring*, compresa la profilazione; (ii) decisioni automatizzate che producono significativi effetti giuridici (es.: assunzioni, concessione di prestiti, stipula di assicurazioni); (iii) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es.: riconoscimento facciale etc.).

È evidente, dunque, che vi sia un'area di applicazione congiunta degli obblighi di effettuare la DPIA e la FRIA allorquando la pubblica amministrazione si avvalga di intelligenze artificiali ad alto rischio, le quali, *ex se*, rientrano facilmente in una delle categorie di trattamento individuate dal Gruppo 29 e, in particolare, nella più generale ipotesi di «utilizzi innovativi o applicazione di nuove soluzione tecnologiche o organizzative».

In questi casi, l'amministrazione dovrà effettuare, congiuntamente, le due valutazioni, sia la DPIA che la FRIA (come ha evidenziato la dottrina «in particolare, tali sistemi ad alto rischio saranno valutati prima di essere messi sul mercato e durante tutto il loro ciclo di vita (trattasi di una valutazione d'impatto sui diritti fondamentali che si affiancherà alla valutazione di impatto privacy – DPIA – prevista dal GDPR»[98]).

5. Osservazioni conclusive: le problematiche sottese all'applicazione congiunta dei due regolamenti. Il rischio di eccesso di regolazione della tecnologia per il settore pubblico

Come si è anticipato, l'intelligenza artificiale si "nutre" di dati personali e, dunque, le relative discipline sono e devono essere studiate in stretta correlazione.

Non sorprende, pertanto, che il Regolamento sulle intelligenze artificiali e il GDPR dovranno, per forza di cose, trovare applicazione "in modo congiunto". La complementarità tra le discipline

94. Cfr. art. 27: «Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti: a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo».

95. Nonché per operatori che erogano servizi bancari e assicurativi per alcuni sistemi.

96. Cfr. art. 35 GDPR.

97. Cfr. Article 29 Data Protection Working Party 2017.

98. El Sabi 2023, p. 789.

emerge immediatamente dalla lettura dello stesso Regolamento IA, che contiene massicci richiami – sia diretti che indiretti – al GDPR, nonché dalla relazione esplicativa di accompagnamento predisposta dalla Commissione europea, laddove si esplicita che l'applicazione del primo non può pregiudicare l'applicazione del secondo.

Le due discipline sono, per molti versi, simili: la centralità dei diritti fondamentali; la tendenza all'extraterritorialità nonché, *last but not least*, l'approccio regolatorio basato sul rischio.

Tuttavia, dalla comparazione tra le due fonti, emergono molteplici profili di divergenza, tra cui: (i) il difficile rapporto tra alcuni principi fondamentali in materia di GDPR (limitazione delle finalità e minimizzazione dei dati) e (ii) il meccanismo di funzionamento delle intelligenze artificiali che necessitano, per funzionare bene, di grandi quantità di dati.

Ancora, si è evidenziata una distanza per quanto concerne le modalità di qualificazione dei rischi: il GDPR decentralizza la valutazione del rischio sotteso al trattamento, delegando la stessa ai soggetti direttamente coinvolti in base al principio di accountability, l'*AI Act* introduce una valutazione generale e a monte, creando una categorizzazione astratta delle intelligenze artificiali a seconda dei livelli di rischio.

Orbene, alla luce di ciò, un primo problema che si pone è quello di comprendere quale sia il criterio ermeneutico per risolvere i contrasti tra le due fonti. Difatti, non si potrà ricorrere al criterio di specialità, affermando una prevalenza dell'*AI Act* in quanto *lex specialis* rispetto al GDPR, *lex generali*. Ciò perché, innanzitutto, si dubita fortemente sia configurabile, effettivamente, un rapporto di specialità in senso tecnico tra il Regolamento IA e il GDPR. In aggiunta a ciò, il criterio della specialità è inservibile anche in considerazione del fatto che il GDPR tutela un diritto umano fondamentale previsto da una fonte primaria dell'Unione europea[99] e, quindi, ammettere la prevalenza per specialità dell'*AI Act* si porrebbe in contraddizione con il criterio gerarchico.

Oltre al rischio di antinomia tra le norme delle due fonti, la coesistenza delle stesse solleva un'ulteriore problematicità: il tema della duplicazione degli oneri. Difatti, non si può negare che il Regolamento IA contribuisca ad aumentare gli obblighi, in capo agli operatori, e tali obblighi, di sovente, non sostituiscono ma si aggiungono a quelli già contenuti nel GDPR, con conseguente rischio di eccesso regolatorio[100].

Il rischio di eccesso regolatorio di tali materie coinvolge soprattutto l'azione pubblica[101] (si veda l'esempio, trattato al paragrafo che precede, della FRIA, prevista nell'ambito IA, e della DPIA, imposta dal GDPR).

Il crescere degli obblighi ha un impatto ancor più gravoso sul settore pubblico in quanto nel predetto ambito la disciplina delle attività è già *ex se* penetrante e massiccia: le regole sulle IA e privacy devono confrontarsi con ulteriori, certamente non ancillari, norme e principi, tra cui, *in primis*, i principi del procedimento amministrativo, come legalità e trasparenza.

Il quadro regolatorio appare, dunque, per le pubbliche amministrazioni abbastanza saturo e poco coordinato. La tecnologia dovrebbe velocizzare e migliorare la qualità dell'attività amministrativa, *ex* art. 97 Cost., come più volte ricordato dal Consiglio di Stato[102], e, il costante "dubbio giuridico", spesso alimentato dalla ipertrofia normativa, certamente non aiuta ad accelerare il procedimento.

Tutto ciò potrebbe condurre l'amministrazione ad evitare l'utilizzo delle tecnologie più avanzate alla luce della confusione di non essere totalmente *compliant*, evitando così, in radice, di correre il rischio di rispondere per eventuali danni; il timore è "giustificabile" se si considera che le violazioni in materia, oltre ad essere sanzionate dalle Autorità di

99. Cfr. Falletta–Marsano 2024, p. 127.

100. *Ibidem*: «considerati gli ampi margini di potenziale sovrapposizione, l'attuazione delle due discipline, potrebbe portare ad un eccesso di regolamentazione».

101. Probabilmente, il fatto di prevedere questo obbligo, la FRIA, soltanto in capo ai *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), si basa su una presunzione di un rischio specifico in termini di impatto sui diritti fondamentali sotteso alla qualifica.

102. Cfr. nota 88.

vigilanza, possono rientrare nell'ambito di ipotesi di responsabilità amministrativa.

Peraltro, con l'avvento del Regolamento IA, si raddoppiano anche i rischi sanzionatori per le amministrazioni. Come si è visto, sul piano dell'impianto sanzionatorio, il Regolamento IA e il GDPR condividono una impostazione molto simile in quanto la sanzione è determinata mediante una percentuale del fatturato[103] del soggetto destinatario della sanzione. Inoltre, entrambi i sistemi riconoscono una grande discrezionalità alle autorità di vigilanza[104].

Sul punto, è bene rilevare che in Italia, le designate autorità di vigilanza in materia di intelligenza artificiale non coincidono con l'Autorità che si occupa della privacy, il Garante per la protezione dei dati personali. L'Italia ha, infatti, deciso di non attribuire al Garante anche tali competenze, designando, invece, l'AgID (Agenzia per l'Italia Digitale) e l'Agenzia per la Cybersicurezza Nazionale. Tale scelta, sebbene sia comprensibile per certi versi, non volendosi concentrare probabilmente troppe competenze in seno ad un medesimo organo, aumenta il grado di complessità generale sia a valle, sotto il citato profilo sanzionatorio, sia a monte, in quanto enfatizza il rischio di disarmonia – sotto il profilo applicativo – dei due regolamenti[105].

Quindi, anche sotto tale profilo, l'amministrazione che utilizza intelligenze artificiali e nel farlo, nella quasi totalità dei casi, tratta dei dati personali, dovrà confrontarsi non solo con due normative complementari ma anche con più Autorità di vigilanza e con le relative Linee Guida emesse ed *emettende*, con raddoppio dei rischi sanzionatori[106].

103. La percentuale sarà più o meno alta a seconda della gravità della violazione attuata. Cfr art. 99 *AI Act* e 83 e ss. GDPR.

104. Si legge, nel considerando 168 Regolamento IA, che nel valutare «l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up».

105. Si veda la Segnalazione del Garante per la protezione dei dati personali al Parlamento del 25 marzo 2024, ove si evidenziano le ragioni per cui il Garante sarebbe stata l'Autorità di vigilanza più adatta anche ai fini dell'applicazione del Regolamento IA. Nella segnalazione viene evidenziato che: «in ragione della stretta interrelazione tra i.a. e protezione dati, della competenza già acquisita in materia dalle Autorità di protezione dati sul processo decisionale automatizzato (art. 22 del Regolamento UE 2016/679) e delle caratteristiche d'indipendenza che ne connotano lo statuto, sarebbe utile ragionare sulla soluzione proposta dal Comitato europeo per la protezione dati e dal Garante europeo. Con il parere congiunto n. 5 del 2021, essi hanno infatti suggerito l'individuazione, nelle Autorità di protezione dati, delle autorità di controllo per l'i.a. Va, infatti, preliminarmente considerato che il Regolamento obbliga espressamente alla designazione delle Autorità di protezione dati quali autorità competenti rispetto all'applicazione di alcune sue disposizioni. Ai sensi dell'art. 74, p. 8, infatti, "per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, 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, 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". Inoltre, rispetto all'identificazione biometrica nell'ambito di attività di contrasto si prevede un vaglio autorizzatorio da parte di autorità giudiziarie o amministrative indipendenti (art. 5, p. 3) tenute a verificare l'osservanza, tra l'altro, dei vincoli imposti dalla disciplina di protezione dati. Ciò implica, dunque, l'opportunità dell'attribuzione al Garante anche di tale funzione, in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza. Le Autorità di protezione dati sono, dunque, le uniche autorità effettivamente destinatarie di una riserva di competenza sancita dal Regolamento (cfr., appunto, art. 74, p. 8 oltre alle varie clausole di salvaguardia in favore della protezione dati previste) e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori delicati come quello delle attività di contrasto (art. 5, p. 3). Per tale ragione, sarebbe opportuno attribuire al Garante le funzioni di cui all'art. 70 del Regolamento, ferme restando ovviamente le competenze del Governo in ordine alla generale promozione e regolazione secondaria della materia».

106. Peraltro, muovendo dall'esperienza in tema di DPIA e considerata la sua potenziale sovrapposizione con la FRIA, si consideri che sono molteplici le sanzioni ricevute, negli ultimi anni, da enti pubblici: si può citare

Tuttavia, a mitigare la sommatoria del rischio sanzionatorio concorre l'art. 99, par. 7, lett. c) del Regolamento IA che riconosce, ai fini della determinazione della sanzione, la circostanza della previa comminazione di altra sanzione amministrativa da diversa autorità, più precisamente «se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento».

Riferimenti bibliografici

M. Allena, S. Vernile (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, in Pajno A., Donati F., Perrucci A. (a cura di), "Intelligenza artificiale e diritto: una rivoluzione?", vol. 1, il Mulino, 2022

Article 29 Data Protection Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 2017

C. Barett (2019), *Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?*, in "The Sci Tech Lawyer, Chicago", vol. 15, 2019, n. 3

S. Barocas, A.D. Selbst (2016), *Big Data's Disparate Impact*, in "California Law Review", vol. 104, 2016, n. 3

M. Betzu (2021), *I poteri privati nella società digitale: oligopoli e antitrust,* in "Diritto pubblico", 2021, n. 3

F. Bignami (2018), *Introduction. A New Field: Comparative Law and Regulation*, in "GWU Legal Studies working papers", 2018, n. 49

L. Bolognini, E. Pelino (2024), *Codice della disciplina privacy*, Giuffrè, 2024

S. Calzolaio (2023), *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in "Rivista italiana di informatica e diritto", 2023, n. 2

E. Carloni (2020), *I principi della legalità algoritmica. le decisioni automatizzate di fronte al giudice amministrativo*, in "Diritto amministrativo", 2020, n. 2

R. Cantone, E. Carloni (2018), *Corruzione e anticorruzione. Dieci lezioni*, Feltrinelli, 2018

F. Cardarelli (2021), *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro, R. D'Orazio, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

G. Carullo (2024), *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in "CERIDAP", 2024, n. 3

G. Carullo (2020), *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2020, n. 1-2

G. Carullo (2017), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2017

G. Cerrina Feroni (2023), *IA nei processi decisionali della PA, il faro è la Costituzione*, in "Agenda Digitale", 29 maggio 2023

il caso dell'azienda ospedaliera di Perugia, che è stata destinataria del provvedimento sanzionatorio n. 134 del 7 aprile del 2022 del Garante della Protezione dei dati personali per violazione *ex* art. 35 del GDPR.

G. Corasaniti (2022), *Regolazione, autoregolazione, sovraregolazione della rete: dal "far" web al "fair" web*, in "Gli atti digitali di «Gli Stati Generali del Diritto di Internet»", Luiss 1, 2, 3 dicembre 2022

S. D'Ancona (2018), *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in "Rivista Italiana di Diritto Pubblico Comunitario", 2018, n. 3-4

L. D'Avack (2023), *Intelligenza artificiale e diritto: problematiche etiche e giuridiche*, in "Diritto di famiglia e delle persone", 2023, n. 4

S. Davies (2016), *The Data Protection Regulation: A Triumph of Pragmatism over Principle*, in "European Data Protection Law Review", vol. 2, 2016, n. 3

G. De Gregorio, F. Paolucci, O. Pollicino (2021), *L'intelligenza artificiale made in UE è davvero "umano-centrica"? I conflitti della proposta*, in "Agenda Digitale", 22 luglio 2021

S. El Sabi (2023), *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in "Il Diritto dell'informazione e dell'informatica", vol. 39, 2023, n. 4-5

A. Esposito (2023), *Le prime regole degli USA sull'IA: l'impatto dell'Executive Order di Biden*, in "Agenda digitale", 31 ottobre 2023

P. Falletta, A. Marsano (2024), *Intelligenza artificiale e protezione dei dati personali: il rapporto tra il Regolamento sull'intelligenza artificiale e il GDPR*, in "Rivista italiana di informatica e diritto", 2024, n. 1

C.F. Ferrari, G. Morbidelli (2023), *Codice dei contratti pubblici, commentato articolo per articolo*, La Tribuna, 2023

L. Floridi (2021), *The European Legislation on AI: Brief Analysis of its Philosophical Approach*, in "Philosophy & Technology", vol. 34, 2021

S. Franca (2023), *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Università degli Studi di Trento, 2023

F. Francario (2021), *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse*, in "Giustiziainsieme.it", 2021

C.G. Granmar (2021), *Global applicability of the GDPR in context*, in "International Data Privacy Law", vol. 11, 2021, n. 3

A. Iannuzzi (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", vol. 54, 2021, n. 209

R. Martinez (2019), *Artificial intelligence: Distinguishing between types & definitions*, in "Nevada Law Journal", vol. 19, 2019, n. 3

R. Medaglia, J.R. Gil-Garcia, T.A. Pardo (2023), *Artificial Intelligence in Government: Taking Stock and Moving Forward*, in "Social Science Computer Review", vol. 41, 2023, n. 1

R. Mühlhoff, H. Ruschemeier (2024), *Updating Purpose Limitation for AI: A normative approach from law and philosophy*, 2024

R. Niro (2021), *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive*, in "Osservatorio sulle fonti", 2021, n. 3

T. Odelberg (2024), *Understanding the Future of Artificial Intelligence Governance: Comparing the EU AI Act and U.S. Executive Order on Safe AI,* in "Ford School of Public Policy", 2024

D. Pager, H. Sheperd (2008), *The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets*, in "Annual Review of Sociology", vol. 34, 2008

A. Police (2024), *Principi e azione amministrativa*, in F.G. Scoca (a cura di), "Diritto Amministrativo", Giuffrè, 2014

O. Pollicino (2023), *Washington effect o Bruxelles effect? Regolamentazioni dell'IA a confronto*, in "formiche", 31 ottobre 2023

O. Pollicino (2019), *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "federalismi.it", 2019, n. 19

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

J.A. Powell (2008), *Structural Racism: Building upon the Insights of John Calmore*, in "North Carolina Law Review", vol. 86, 2008, n. 3

A. Puckzo (2024), *An Ambiguous Relationship between Public Administration and AI*, in P. Yao Lartey (ed.), "Recent Advances in Public Sector Management", IntechOpen, 2024

G. Resta (2022), *Cosa c'è di 'europeo' nella proposta di Regolamento UE sull'intelligenza artificiale?*, in "Il Diritto dell'Informazione e dell'Informatica", 2022, n. 2

A. Simoncini, S. Suweis (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1

D. Solove, P.M. Schwarts (2022), *ALI Data Privacy: Overview and Black Letter Text*, in "UCLA Law Review," vol. 68, 2022, n. 5

L. Torchia (2024), *Poteri pubblici e poteri privati nel mondo digitale*, in "Il Mulino", 2024, n. 1

S. Trozzi (2024), *Il principio della finalità del trattamento dei dati personali alla prova dei recenti sviluppi in tema di intelligenza artificiale: il caso ChatGPT e la neuroprivacy*, in "federalismi.it", 2024, n. 1

P. Wang (2019), *On Defining Artificial Intelligence*, in "Journal of artificial general intelligence", vol. 10, 2019, n. 2