Il trattamento dei dati nelle sperimentazioni di intelligenza artificiale riguardanti le pubbliche amministrazioni*

di Simone Franca

1. *Introduzione*

L'impiego dell'intelligenza artificiale (IA) nell'attività della pubblica amministrazione[1] può essere considerato sotto due punti di osservazione.
Per un verso, la possibilità di impiegare l'IA per l'analisi di dati consente di ricavare da essi conoscenze ulteriori che vanno a vantaggio del buon andamento e dell'efficienza dell'amministrazione[2]: da un lato, si ha infatti un risparmio rispetto allo studio di dati

* Il presente scritto è stato elaborato nel contesto di una ricerca Astrid su Intelligenza artificiale e diritto, ed è stato pubblicato in ASTRID, "Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione", a cura di Filippo Donati, Alessandro Pajno, Antonio Perrucci, vol. II, Ed. il Mulino, Bologna, 2022

[1] Assume rilievo non solo l'impiego dell'IA nell'ambito dell'attività propriamente decisionale, ma anche entro l'attività preparatoria. Su tale distinzione rispetto agli impieghi dell'IA si v. B. Marchetti, *La garanzia dello* human in the loop *alla prova della decisione amministrativa algoritmica*, in *Biolaw Journal*, 2, 2021, p. 372.

[2] Cfr. in tema, anche sul tema generale delle ICTs, S. Civitarese Matteucci, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubbl.*, 2019, p. 10; S, Civitarese Matteucci, L. Torchia, *La tecnificazione dell'amministrazione*, in ID. (a cura di), *La tecnificazione*, Firenze University Press, Firenze, 2016, pp. 33 s.; D.U. Galetta, J.G. Corvalán, *Intelligenza artificiale per un'amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 2019, p. 10; I. Martín Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Ist. Fed.*, 3, 2019, pp., 643 ss.; A. Masucci, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Dir. pubbl.*, 2020, 3, pp. 944 ss. Sull'ascendenza teorica della fiducia verso le nuove

che altrimenti richiederebbe molto più tempo e l'impiego di maggiori risorse economiche e umane, specie rispetto a trattamenti routinari; dall'altro lato, si ottengono informazioni sempre più complete per supportare le decisioni del soggetto pubblico.
Per altro verso, l'operare degli algoritmi di autoapprendimento pone a rischio coloro i cui dati sono trattati. Sono infatti noti i casi di decisioni basate su algoritmi di *machine learning* che hanno portato ad esiti poco soddisfacenti rispetto alle posizioni giuridiche degli individui, a causa di *bias* che si traducono in discriminazioni[3].
La sussistenza di queste due prospettive è ben espressa dalla recente Proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale (Proposta reg. IA)[4], che nasce dall'esigenza di avvalersi dei benefici socio-economici dell'IA, senza trascurare i «*nuovi rischi o conseguenze negative per le persone fisiche o la società*»[5].
Occorre poi considerare che la riflessione sull'impiego dell'IA (invero, non solo da parte della p.a.) presuppone, a monte, la considerazione del regime dei dati personali che vengono utilizzati come nutrimento degli algoritmi. In effetti, le tecnologie di IA, pur se già conosciute da tempo, hanno assunto una maggiore diffusione in tempi recenti proprio in ragione della maggiore disponibilità di dati (in particolare, *big data*) da utilizzare per il *training* degli algoritmi[6].
È quindi necessario prendere in considerazione le garanzie previste dal GDPR. Oltre alle regole che riguardano ogni trattamento di dati e che assicurano un maggiore controllo di questi ultimi (gli obblighi informativi di cui agli art. 12 ss. GDPR e i diritti degli interessati disciplinati dagli artt. 15 ss. GDPR), che si inseriscono nel solco dei principi relativi al trattamento dei dati (art. 5 GDPR), vi sono regole specifiche per i

tecnologie si v. A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, in AA. VV., *Scritti per Franco Gaetano Scoca*, vol. 1, Napoli, 2020, p. 680.
[3] Per quanto riguarda il problema dei *bias* si v. L.A. Fridell, *Producing Bias-Free Policing. A Science-Based Approach*, Springer, 2017, passim; T. Numerico, *Social network e algoritmi di machine learning: problemi cognitivi e propagazione dei pregiudizi*, in *Sistemi Intelligenti*, 2019, 3, pp. 469 ss.; D. Di Cagno, A. Galliera, *Non provarci ancora Sam! Effetti di contesto e metodi di contenimento del bias della "quasi vincita". I risultati di un esperimento*, *ivi*, 2021, 1, pp. 29 ss.; L. PARONA, "Government by algorithm": *un contributo allo studio del ricorso all'intelligenza artificiale nell'esercizio di funzioni amministrative*, in *Giorn. dir. amm.*, 1, 2021, p. 17.
[4] COM(2021) 206 final del 21 aprile 2021. Sulla portata di tale proposta cfr. C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *Biolaw Jornal*, 2021, 3, pp. 415 ss.; G. Marchianò, *Proposta di regolamento della Commissione Europea del 21 aprile 2021 sull'Intelligenza Artificiale con particolare riferimento alle IA ad alto rischio*, in *AmbienteDiritto.it*, 2, 2021. Utili indicazioni, anche in prospettiva comparata, si rinvengono in B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *Dir. pubbl. comp. Eur.*
[5] Proposta reg. IA, p. 1.
[6] Cfr., per tutti, G. Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. It.*, 7, 2019, p. 1671.

trattamenti tramite IA, come l'art. 22 GDPR, che disciplina il regime delle decisioni automatizzate.

Se però si guarda al GDPR, alla luce della richiamata dialettica tra efficienza dell'azione amministrativa e garanzie dei cittadini, è possibile riscontrare come, per un verso, esso pone una serie di adempimenti in capo alle amministrazioni che possono apparire come una complicazione[7] (si pensi all'obbligo di informativa per ogni trattamento o alla sottoscrizione di atti consensuali per il trattamento di dati da parte di più soggetti)[8]; per altro verso, esso sembra non offrire un quadro di garanzie sufficiente nei confronti dei cittadini (si pensi al fatto che la sfera applicativa dell'art. 22 GDPR presenta eccezioni piuttosto ampie)[9].

Su un piano più generale, è stato riscontrato che le garanzie del GDPR sono fondate su trattamenti "monodimensionali" – *i.e.* trattamenti posti in essere da un solo titolare –, lasciando così scoperte le problematicità date da catene di trattamenti, quali quelle che si basano, generalmente, sulla cd. *big data analytics*, dove è frequente che siano titolari "terzi" a trattare queste enormi quantità di dati[10]. I problemi che si pongono sono numerosi: l'individuazione delle condizioni di liceità per il trattamento di dati accumulati in ragione di altre basi giuridiche; il tenore degli obblighi informativi ex artt. 12, 13 e 14 del GDPR, che devono illustrare anche le modalità di trattamento; l'adozione delle necessarie misure tecniche e organizzative.

---

[7] Si tratta di un tema che, ad esempio, si è posto in materia di ricerca scientifica (in tema, cfr. *ex multis* E.S. Dove, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *The Journal of Law, Medicine & Ethics*, 4, 46, 2018 pp. 1013 ss.; J. Rumbold, B. Pierscionek, *A critique of the regulation of data science in healthcare research in the European Union*, in *BMC Medical* Ethic, 18, 2017, p. 1.

[8] Per un quadro più ampio in tema, sia consentito rinviare a S. Franca, *La semplificazione delle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, in *Dir. pubb.*, 2, 2021, pp.

[9] Sulla portata dell'art. 22 GDPR cfr., in part., C. Casonato, B. Marchetti, *op. cit.*, pp. 428 ss.; A. Masucci, *op. cit.*, pp. 953 ss.; P. Guarda, *"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation*, in *BioLaw Journal*, 2019, pp. 368 ss.; A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 28.; ID., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, 1, spec. pp. 79 ss.; ID., *Profili costituzionali della amministrazione algoritmica*, in *Riv. Trim. Dir. Pubbl.*, 4, 2019, pp. 1171 ss.

[10] I termini "monodimensionale" e "catena di trattamenti" sono impiegati in F. Pizzetti, *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in A. Mantelero, D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, Pisa University Press, 2018, pp. 84 ss. In senso analogo rispetto all'insufficienza del modello individualistico del GDPR a fronte del proliferare dei *Big data* cfr. G. Finocchiaro, *Intelligenza artificiale*, cit., pp. 1676-1677.

Peraltro, con l'impiego di algoritmi particolarmente sofisticati, come quelli di *machine learning* (ML) o *deep learning* (DL)[11], vi è il rischio che eventuali criticità relative alla base di dati di partenza, così come delle successive iniezioni di dati, assuma una portata esponenziale, giacché una iniziale violazione coinvolge a cascata tutti i trattamenti successivi.

Diventa dunque necessario porsi almeno due domande: la prima concerne il modo in cui i principi del GDPR si adattano al caso dell'IA, per valutare come il GDPR si pone nella dialettica tra efficienza e garanzia del cittadino; la seconda relativa allo spazio che eventualmente hanno le amministrazioni per garantire la tutela dei dati personali nei casi di impiego dell'IA.

In tale prospettiva, a parere di chi scrive, è importante adottare un approccio empirico, muovendo da specifiche sperimentazioni[12] svolte dalla pubblica amministrazione, così da evidenziare le criticità che possono sorgere sul piano della tutela dei dati personali, in ordine alla raccolta dei dati e alle modalità del loro trattamento.

In questa prospettiva, si è scelto di considerare tre fattispecie specifiche, che riguardano l'uso di algoritmi per finalità distinte e cioè: 1) per semplificare il filtro alla segnalazione degli esposti; 2) per l'analisi del *sentiment* attraverso l'utilizzo di dati rivenienti nei *social network*; 3) per predire il dissesto finanziario dei Comuni.

Come è evidente, si tratta di sperimentazioni molto variegate, che vedono la pubblica amministrazione talvolta come attore principale, talaltra come *partner* di ricerca o vero e proprio oggetto della ricerca. Le amministrazioni selezionate sono sia amministrazioni statali (nella specie, autorità indipendenti), sia enti autonomi (nella specie, comuni). Bisogna poi considerare che le sperimentazioni possono essere in fase molto avanzata o, al contrario, in fase preliminare. Infine, gli algoritmi impiegati, come si avrà modo di

[11] Sulla distinzione tra tali due algoritmi cfr., per tutti, G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intelligibilità*, Editoriale scientifica, 2019, pp. 5-10; B. Marchetti, *op cit.*, p. 378; P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, in *Federalismi.it*, 2, 2018, p. 191; U. Pagallo, W. Barfield, *Advanced introduction to Law and Artificial Intelligence*, Elgar Publishing, Cheltenham-Northampton, 2021, pp. 14 ss.

[12] Il metodo delle sperimentazioni o *sandboxes* è peraltro incentivato fortemente dalla Proposta reg. IA, che ne offre una specifica disciplina agli art. 53 ss. e ne specifica i vantaggi in termini di sicurezza (Considerando n. 71) e per garantire l'innovazione dell'IA (Considerando n. 72). In tema cfr. C. Casonato, B. Marchetti, *op. cit.*, p. 419. Per un inquadramento delle sperimentazioni di IA, più in generale, entro la cd. *risk regulation*, cfr. A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law*, 1, 1-2, 2020, p. 66

osservare, sono molto differenti fra loro, ma, nella prospettiva della loro messa a regime, si collocano nell'ambito dell'attività preparatoria della pubblica amministrazione[13].
Il contributo sarà suddiviso in tre parti. Nella prima si tenterà di offrire una analisi delle singole sperimentazioni prese in considerazione, al fine di isolare i flussi di dati personali con riferimento alle categorie degli stessi, alla loro fonte e alle modalità di trattamento algoritmico. Nella seconda si cercherà di far emergere eventuali criticità sul piano della protezione e gestione dei dati nella prospettiva (spesso non molto lontana) della messa a regime delle sperimentazioni. Infine, dall'analisi svolta, si tenterà di trarre alcuni spunti sul ruolo delle amministrazioni rispetto all'attuazione della disciplina in tema di protezione dei dati nell'impiego dell'IA.

2. *Le fattispecie: a) Le procedure di segnalazione degli esposti*

Nell'ambito dell'attività delle autorità amministrative indipendenti un primo impiego di trattamenti automatizzati concerne la gestione degli esposti privatistici relativi a ipotetiche violazioni da cui le medesime autorità, come Banca d'Italia e CONSOB, avviano l'istruttoria per l'eventuale accertamento e l'adozione dei conseguenti provvedimenti.
Scorrendo i *report* relativi alla gestione degli esposti rivolti ad alcune delle menzionate autorità emerge subito come nel corso del tempo la segnalazione di violazioni da parte dei privati abbia assunto sempre maggiore portata[14]. L'impiego di algoritmi non è motivato dalla sola esigenza di accelerare i tempi delle procedure, dovendosi altresì tenere conto che tramite l'analisi algoritmica e, dunque, automatizzata di eventuali ricorrenze è possibile rilevare la sussistenza di problemi a carattere sistemico.
Tenendo conto di ciò, si è dunque reso necessario ipotizzare soluzioni organizzative in grado di filtrare la mole di esposti inoltrati alle suddette autorità in modo da agevolare l'attività dei funzionari coinvolti nella verifica degli stessi.
Sul piano pratico emerge che tanto Banca d'Italia quanto CONSOB intendono muoversi nell'implementazione di tali tipologie di trattamenti automatizzati.
Per quanto attiene alla prima autorità, è in corso di realizzazione il progetto EspTech. Si tratta di un progetto che prevede l'implementazione di algoritmi *machine learning* al fine di filtrare e classificare gli esposti che quotidianamente sono inviati all'autorità. Gli

[13] Cfr. *supra* nt. 1. Sulle ricadute positive dell'impiego di algortmi ML rispetto all'esercizio dei poteri tecnico-discrezionali da parte delle autorità pubbliche, cfr. L. Parona, *Poteri tecnico-discrezionali e* machine learning: *verso nuovi paradigmi dell'azione amministrativa*
[14] Ad esempio, dalla Relazione sugli esposti dei clienti delle banche e delle finanziarie - anno 2020 si evince un aumento percentuale del numero di esposti presentati rispetto al 2019 pari al 36%.

esposti che vengono inviati provengono da diverse tipologie di soggetti e cioè: consumatori, società o altre categorie non specificate. I loro dati personali che vengono trattati consistono essenzialmente nei dati anagrafici, nei dati contenuti nel documento di identità e in tutte le informazioni ad essi relative eventualmente ricavabili dalle argomentazioni riversate negli esposti. L'algoritmo opera secondo cinque fasi: i) la fase ETL, che consiste nell'estrazione, pulitura del dato e nel suo inserimento all'interno di un *database*; ii) la fase di *preprocessing,* che mira a ricondurre ciascun lemma alla sua radice; iii) la fase di *feature extraction,* in cui i dati iniziali vengono lavorati per ridurne la dimensionalità con diverse tecniche (es. *semantic embedding*, consistente nella individuazione di parole aventi la stessa radice semantica); iv) la fase di *clustering*, consistente nel raggruppamento di elementi omogenei in un insieme di dati. v) la fase finale, di traduzione del lavoro operato in una interfaccia dedicata all'utente (Web UI)[15]. Per quanto attiene alla CONSOB, l'analogo procedimento di verifica degli esposti si svolge come segue[16].

Esso si avvale del *machine learning,* al fine di filtrare gli esposti analogamente a quanto già visto per Banca d'Italia. In questo caso, gli esposti provengono da soggetti come risparmiatori, associazioni e comitati a tutela dei risparmiatori e operatori di mercato. I dati recati negli esposti sono sostanzialmente i medesimi di quelli sopra richiamati.

Il procedimento di *machine learning* si compone di quattro funzionalità: i) la *keywords analysis* (funzionalità che esamina un set di parole ricorrenti, anche grazie alla previa individuazione di parole già precaricate nel sistema); ii) la *topic analysis* (attraverso la funzione di *text mining*, utilizza il linguaggio naturale per trasformare il testo libero di documenti in dati strutturati e normalizzati: questa è la funzione più autenticamente di intelligenza artificiale); iii) la funzionalità della mappa semantica (collega *keywords* e *topic*, permettendo così di operare collegamenti che consentono lo svolgimento di analisi di tipo aggregato che permettono di fare ricerche in base a elementi che presentano analogie); iv) la funzionalità denominata "analisi dello scrivente" (funzione più di analisi e ricerca, di estrazione dati per successive analisi e valutazioni, in quanto consente di acquisire informazioni di contesto sulle caratteristiche dell'autore dell'esposto al fine di classificarlo per "categoria di appartenenza".

[15] Informazioni su tale processo possono essere tratte dalle tavole del documento A. Maggi, *Machine Learning a supporto dell'azione di Vigilanza: l'esperienza di EspTech sugli esposti privatistici*, 2021, pubblicato in https://www.cipa.it/attivita/workshop/2021/index.html. In tema cfr. anche E. Chiti, B. Marchetti, N. Rangone, *L'uso dell'intelligenza artificiale nelle attività della Banca d'Italia*, in *Biolaw journal*, 2021, n. 4, pp. 229-244.

[16] Cfr. E. Chiti, B. Marchetti, N. Rangone, *L'uso dell'intelligenza artificiale nell'attività di Consob, Agcom e Arera*, in *Biolaw Journal – Rivista di BioDiritto 2021, n. 4, pp. 211-227*, 2021

3. *Segue: b) Le procedure di analisi del* sentiment

Un altro interessante filone sperimentale attiene alle cd. analisi del *sentiment*. Si tratta di analisi che svolgono un ruolo preliminare rispetto all'indirizzo dell'attività delle autorità pubbliche.

In questo caso, le esperienze che si ritiene opportuno prendere in considerazione sono quelle di Banca d'Italia e AGCOM.

Per quanto concerne Banca d'Italia, la sperimentazione svolta in relazione all'analisi del *sentiment* prevede l'impiego di algoritmi di *machine learning*. I dati vengono raccolti, in questo caso, dal *social network* Twitter: si tratta dunque di dati pubblici, in particolare *tweet* relativi ad opinioni degli utenti sull'inflazione, ma anche di dati raggruppati nel cd. *noise*, ovvero dati ulteriori come pubblicità, *tweet* di *e-commerce* e anche *tweet* che parlano di inflazione in contesti diversi da quelli dell'aumento dei prezzi[17]. È dunque evidente che le categorie di soggetti coinvolti sono difficilmente individuabili.

Per quanto riguarda la procedura di analisi essa è stata realizzata come segue. Anzitutto, sono state selezionate alcune parole chiave rilevanti per identificare i *tweet* relativi ai prezzi di beni e servizi (attuali e previsti) in Italia per costruire il *dataset* iniziale (tra il 1° giugno 2013 e il 31 dicembre 2019). Sono stati così isolati circa 11,1 milioni di *tweet*. Per ridurre il *noise* si è adottata una procedura trifasica: 1) una di filtro, implementando un'analisi per argomenti sul testo dei messaggi attraverso la *Latent Dirichlet Allocation* (LDA), un algoritmo di *machine learning* non supervisionato [18] che stima statisticamente gli argomenti (collezioni probabilistiche di parole) di un insieme di documenti, consentendo di selezionare i *tweet* relativi agli sviluppi dell'inflazione; 2) una di applicazione, sui dati filtrati, di un dizionario di bi-grammi e tri-grammi etichettati manualmente per assegnare ciascun *tweet* a delle fasce, ciascuna delle quali denota aspettative di inflazione crescente o decrescente; 3) infine, una di aggregazione dei conteggi giornalieri grezzi dei *tweet* che rappresentano aspettative di inflazione crescente o decrescente in indicatori direzionali, che aumentano (o diminuiscono) con le aspettative di inflazione crescente (o decrescente)[19].

Per quanto concerne la sperimentazione attualmente in corso da parte di AGCOM, essa viene condotta per lo più in sinergia con istituzioni di ricerca. Le sperimentazioni

[17] Cfr. C. Angelico, J. Marcucci, M. Miccoli, F. Quarta, *Can we measure inflation expectations using Twitter?*, Working papers di Banca d'Italia, 2021, p. 11

[18] Si tratta dunque di un algoritmo che attinge a dati non preventivamente classificati. Sulla nozione di *machine learning* supervisionato e non cfr., *ex multis*, G. AVANZINI, *op. cit.*, pp. 7 ss.; P. Otranto, *op. cit.*, p. 191. Approfondimenti in T. JO, *Machine Learning Foundations. Supervised, Unsupervised, and Advanced Learning*, Springer, Cham, 2021.

[19] Cfr. C. Angelico, J. Marcucci, M. Miccoli, F. Quarta, *op. cit.*, pp. 6 ss.

condotte riguardano l'*hate speech* nell'ambito del progetto IMSyPP - Innovative Monitoring Systems and Prevention Policies of Online Hate Speech[20].
Anche se i trattamenti sono svolti per la preminente finalità di ricerca degli enti coinvolti, non bisogna trascurare che l'AGCOM intende «*includere il rilevamento automatizzato e il monitoraggio dell'hate speech on line in un quadro regolatorio in cui l'Intelligenza Artificiale non sostituisce la valutazione umana nel perseguimento dei crimini di odio ma è limitata alla prevenzione e al monitoraggio*»[21].
Nell'ambito di tale sperimentazione[22], si è svolta una ricerca tramite *keywords* (es. corona-virus, covid, etc.) di video, anche avvalendosi dei video correlati in base all'algoritmo di Youtube.
Sono stati così raccolti i video in linea con le *keywords* e, successivamente, i commenti relativi a questi video. I soggetti interessati, anche in questo caso, sono molti, ma la loro riconoscibilità è più complessa per quanto riguarda i commenti.
È stata poi assegnata un'etichetta binaria a ciascun canale YouTube per distinguere tra due categorie: discutibile e affidabile[23]. L'elenco dei canali YouTube etichettati come discutibili è stato fornito dall'AGCOM.
A questo punto l'intervento consiste nella creazione di due *set* di dati, un *tranining set* per allenare l'algoritmo di *deep learning* a riconoscere gli *hate speech* e un *evaluation set* per testare il medesimo algoritmo. Per entrambi i set è stato adottato un sistema di annotazione basato su quattro categorie e gestito tramite annotazione manuale da otto annotatori[24]. A questo punto, l'algoritmo allenato viene utilizzato su un *dataset* di più di un milione di *tweet*.

4. *Segue: c) La predizione dei dissesti finanziari dei Comuni*

Un'ulteriore sperimentazione che mette conto analizzare concerne la configurazione di algoritmi utili a predire il dissesto dei Comuni. Giova premettere che si tratta di impieghi

[20] Per maggiori informazioni sul progetto, cfr. il link http://imsypp.ijs.si.
[21] Così si è pronunciato il Presidente dell'Autorità per le Garanzie nelle Comunicazioni, Angelo Marcello Cardani (cfr. il comunicato stampa del 31 gennaio 2017 avente ad oggetto "Intelligenza artificiale e intervento umano contro hate speech", p. 1, disponibile su *www.agcom.it*.
[22] I dati che seguono sono stati desunti dal testo M. Cinelli, A. Pelicon, I. Mozeti, W. Quattrociocchi, P. Kralj Novak, F. Zollo, *Online Hate: Behavioural Dynamics and Relationship with Misinformation*, disponibile in *arxiv.org*, cui si rinvia per maggiori informazioni.
[23] Cfr. *Op. ult. cit*. Un canale YouTube discutibile è un canale che produce contenuti non verificati e falsi o direttamente associato a una testata giornalistica che non ha superato molteplici controlli dei fatti eseguiti da agenzie di *fact checking* indipendenti.
[24] M. Neves, J. Ševa, *An extensive review of tools for manual annotation of document*s, in *Briefings in Bioinformatics*, 22, 1, 2021, pp. 146-163.

di algoritmi *machine learning* che nella letteratura specialistica sono già piuttosto diffusi e mirano, sulla base dei dati delle amministrazioni, a prevenire ipotesi di dissesto[25].
Per quanto riguarda i dati utilizzati, questi sono ottenuti dall'incrocio tra dati del Ministero dell'Interno nel periodo 1989-2016 e 26 indicatori finanziari forniti dall'Istat per il periodo 2009-2016. Il periodo di riferimento, dunque, è quello che va dal 2009 al 2016. Sono stati poi raccolti nel database i dati istituzionali del Ministero dell'Interno italiano riguardanti i politici locali, che contengono informazioni relative all'età, al sesso, all'orientamento politico, al livello di istruzione del sindaco, all'età media e alle quote di genere dei consiglieri, nonché altre variabili che tengano conto, ad esempio, della distinzione Nord/Sud.
Anche in questo caso si creano due *dataset* di dati storici, il primo per il training dell'algoritmo e il secondo per testarne le capacità, dividendo tra di essi in modo casuale i Comuni in *default* e quelli non in situazione di *default*.
L'algoritmo di *machine learning* così allenato viene impiegato per poter predire, in base ai dati forniti, che rischio vi sia che un dato Comune possa finire in una situazione di *default*.

5. *La raccolta dei dati fra liceità, correttezza del trattamento e limitazione delle finalità del trattamento*

Sulla scorta della rappresentazione di tali fattispecie, un primo gruppo di riflessioni può riguardare la raccolta dei dati nell'ambito delle sperimentazioni.
Potrebbe sembrare che, le pubbliche amministrazioni abbiano sostanzialmente carta bianca rispetto alla raccolta massiva di dati per scopo di analisi, anche mediante la cd. pesca a strascico, senza limitazioni a specifiche finalità[26].
In realtà, vi sono una serie di regole che l'amministrazione deve attuare, dal punto di vista della tutela dei dati personali, in primo luogo, per conformarsi al principio di liceità, letto congiuntamente a quello di correttezza del trattamento, e al principio di limitazione delle finalità del trattamento.
Alla luce di tali principi, infatti, il titolare deve assicurarsi che ciascun trattamento di dati da lui posto in essere sia conforme alle norme ad esso applicabili (liceità), nella

[25] Maggiori informazioni su questa sperimentazione si rinvengono in N. Antulov-Fantulin, R. Lagravinese, G. Resce, *Predicting bankruptcy of local government: A machine learning approach*, in *Journal of Economic Behavior and Organization*, 183, 2021, pp. 681-699.
[26] Sulle problematicità della pesca a strascico cfr. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in ID. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 60.

prospettiva di assicurare un un rapporto leale tra titolare e interessato (correttezza), avendo cura di raccogliere i dati per finalità determinate, esplicite e legittime (limitazione delle finalità)[27].

Il portato dei richiamati principi si traduce nell'individuazione di una base giuridica del trattamento e di limitare il trattamento a ciò che è giustificato in base ad essa. L'operazione richiede al titolare di scegliere una delle basi giuridiche indicate agli artt. 6 ss. GDPR e nelle norme rilevanti del d.lgs. 30 giugno 2003, n. 196 (d'ora in avanti, codice privacy) – su cui si tornerà *infra* –, in ragione degli elementi caratterizzanti il trattamento (ad esempio, le categorie di dati trattati, le finalità che si intendono perseguire, etc.).

Questa impostazione vale rispetto agli usi primari dei dati, ovvero quegli usi per cui i dati sono stati originalmente raccolti[28]. Va però detto che il principio di limitazione della finalità del trattamento trova una parziale deroga nel caso di usi secondari, cioè usi ulteriori di dati già raccolti, che siano compatibili con l'uso primario[29].

In questo caso, di regola[30], il titolare del trattamento dovrà svolgere una valutazione di compatibilità tra le finalità primaria e secondaria, ai sensi dell'art. 6, par.4 GDPR[31]. Solo nel caso in cui la finalità secondaria sia di «*archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*» si presume che non vi sia incompatibilità, qualora siano adottate le misure tecniche e organizzative conformi al principio di minimizzazione dei dati[32]. In assenza della compatibilità, al titolare non resterà che rintracciare un'ulteriore base giuridica che giustifichi il nuovo trattamento.

Cercando di applicare tali considerazioni ai casi di sperimentazione esposti, giova premettere che essi paiono integrare ipotesi di usi secondari. Nel primo caso, la finalità

---

[27] Sulla portata di tali principi e sul loro raccordo si veda da ultimo G. Malgieri, sub *art. 5*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, pp. 180 ss.

[28] Sulla nozione di usi primari cfr. F. Modafferi, *Il regime particolare dei trattamenti di dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli, Torino, 2021, p. 401 e cfr. il considerando n. 50 del GDPR.

[29] Cfr. art. 5, par. 1, lett. b) GDPR.

[30] Tale regola non vale "[l]*addove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1*" (art. 6, par. 4 GDPR).

[31] Ai sensi di tale disposizione, la valutazione deve considerare a) qualsiasi nesso tra finalità primarie e secondarie; b)

b) il contesto relativo alla raccolta dei dati; c) la natura dei dati personali; d) le possibili conseguenze dell'ulteriore trattamento, e) l'esistenza di garanzie adeguate.

[32] Cfr. il combinato disposto dell'art. 5, par. 1, lett. b) e dell'art. 89 GDPR

dell'uso primario corrisponde allo svolgimento dell'attività di vigilanza, mentre l'uso secondario consiste nell'approntamento di un miglioramento all'efficienza della vigilanza; nel secondo caso, l'uso primario è quello operato dai *social network* e consiste nella diffusione di opinioni degli utenti, mentre il secondario coincide con gli scopi di *policy* delle autorità; nel terzo caso, l'uso primario è quello di archiviazione del Ministero[33], mentre l'uso secondario consiste nella predizione dei dissesti.

Ciò premesso, per sperimentazioni di questo tenore, parrebbe che la compatibilità tra uso primario e secondario possa essere presunta, nella misura in cui i vari trattamenti sono riconducibili a trattamenti per finalità di ricerca scientifica[34] e purché siano adottate le misure tecniche e organizzative adeguate. Inoltre, nel caso di recepimento della Proposta reg. IA, potrebbe ritenersi che le norme relative alle sperimentazioni (artt. 53 ss.) possano costituire una idonea base giuridica per il trattamento[35] o consentire di superare altrimenti il vaglio di compatibilità richiesto dall'art. 6, par. 4 GDPR[36].

Nel caso invece della messa a regime di tali sistemi di analisi algoritmica, tramite il loro impiego nell'ordinaria attività amministrativa, è possibile che si debba svolgere una riflessione differente.

In questi casi, salva l'eventuale dimostrazione della compatibilità delle finalità del trattamento algoritmico con quelle del trattamento originario o il sussistere di casi eccezionali[37], la base giuridica ideale potrebbe essere determinata dall'art. 2-ter per dati

[33] Qui uso primario è inteso in senso relativo, rispetto al nuovo trattamento.

[34] La finalità di ricerca scientifica, infatti, va intesa alla luce del considerando n. 159 del GDPR come comprensiva, ad esempio, di "sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata". Bisogna però ricordare che ogni interpretazione non può spingersi sino a consentire trattamenti i cui scopi siano del tutto imprevisti o imprevedibili (P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Editoriale scientifica, Napoli, 2021, p. 207).

[35] Si tratterebbe di norme che possono valere ad attuare l'art. 2-ter, co. 1 o 2-sexies, co. 1 del codice privacy, su cui si v. *infra*.

[36] In linea con la previsione richiamata *supra sub* nt. 30.

[37] Per esempio, nel caso di dati particolari (es. opinioni politiche) tratti da profili pubblici sui *social network* potrebbe ritenersi che la base giuridica sia rappresentata dall'art. 9, par. 2, lett. *e)* GDPR, dunque, dal fatto che i dati sono stati resi manifestamente pubblici dagli interessati, tramite il *social network*. Per avvalersi di tale base giuridica, tuttavia, occorre tener conto delle indicazioni dello *European Data Protection Board* (EDPB). Secondo l'EDPB, la nozione di "dati resi manifestamente pubblici" va considerata con particolare attenzione rispetto ai *social media*, dovendosi dare una interpretazione restrittiva di tale eccezione e dovendosi previamente verificare che la pubblicazione sia frutto di una scelta libera e autonoma (sul punto, cfr. EDPB, *Guidelines on the targeting of social media users*, n. 8/2020, p. 4.p. 33, nt. 93; EDPB, *Statement on the use of personal data in the course of political campaigns*, n. 2/2019, p. 2, nt. 1.). In particolare, l'EDPB ha fatto presente che occorre considerare una serie di elementi nel trattamento dei dati da parte del singolo social per verificare che il trattamento sia lecito, precisando altresì che anche per tali trattamenti devono essere rispettati i principi generali previsti dall'art. 5 GDPR (cfr. EDPB, cit., n. 8/2020 pp. 29 ss.). Per un inquadramento generale delle altre basi giuridiche si vedano, *ex multis*, M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati*

personali comuni e dall'art. 2-sexies per dati particolari[38]. Si tratta delle norme che disciplinano, rispettivamente, i trattamenti di dati comuni per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri e i trattamenti di dati particolari necessari per motivi di interesse pubblico rilevante. La disciplina previgente, salvo alcune eccezioni[39], prevedeva che in entrambi casi simili trattamenti fossero leciti in presenza di una norma di legge o, nei casi previsti dalla legge, di regolamento che li disciplinasse[40].

Tuttavia, con la modifica del codice privacy ad opera dell'art. 9 del d.l. 8 ottobre 2021, n. 139, il legislatore è intervenuto sul codice privacy, apportando alcune modifiche: nella specie, è stato modificato il citato art. 2-ter, con l'introduzione di un comma 1-bis, il quale funge da "norma di legge" ai sensi del comma 1 e, si ritiene (pur con alcune

personali nel diritto europeo, Torino, Giappichelli, 2019, pp. 219 ss.; D. POLETTI, sub *art. 6,* in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *op. cit.,* pp. 191 ss.

[38] Va poi rilevato come, rispetto a tali sperimentazioni, non assumano rilievo le basi giuridiche che giustificano le eccezioni al divieto di ricorso a decisioni completamente automatizzate ex art. 22 GDPR: tali sperimentazioni, infatti, non sono riconducibili a trattamenti completamente automatizzati, dato che l'*output* generato dall'gli algoritmi ML sono è sempre oggetto di controllo prima di essere recepiti all'interno di una decisione e, in ogni caso, vi è sempre l'apporto umano rispetto alla portata del trattamento automatizzato. L'utilizzo di un algoritmo non supervisionato (come nel caso dell'analisi del *sentiment* da parte di Banca d'Italia) non sposta i termini della questione, giacché non inerisce alla garanzia dell'intervento umano rispetto alla decisione algoritmica (su tale garanzia cfr., in part., B. Marchetti, *op cit.*, pp. 377 ss.).Sulla limitazione dell'art. 22 GDPR alle decisioni completamente automatizzate e non supervisionate si veda G. Avanzini, *op. cit.*, p. 112 di cui si condividono gli ulteriori rilievi relativi all'inapplicabilità del consenso con riferimento alle pubbliche amministrazioni: il consenso non costituisce idonea base giuridica per trattamenti operati dalle p.a. per lo squilibrio che generalmente si ha tra amministrazione e interessati (cfr. Considerando n. 43 del GDPR e WP29, *Linee guida in materia di consenso,* del 10 aprile 2018). A ciò si aggiunga che, con riferimento alla *big data analytics,* vi sono perplessità rispetto al fatto che il consenso sia effettivo: in tema, cfr. le considerazioni di M. Falcone, Big Data *e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Riv. trim. dir. pubbl.*, 3, 2017, p. 615; S. D'Ancona, *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 *Riv. it. dir. pubbl. com.*, 2018, 3, pp. 600 ss.

[39] Nel caso dell'art. 2-ter, co. 2, infatti, era prevista la possibilità di svolgere una comunicazione e diffusione di dati previa comunicazione al Garante e trascorsi 45 giorni in assenza di una sua contraria determinazione. Nel caso dell'art. 2-sexies, co. 2, inoltre, si individuano tutt'ora alcuni specifici trattamenti come trattamenti di interesse pubblico rilevante.

[40] Sulle versioni previgenti dei due articoli in parola cfr., in part., F. Cardarelli, sub art. 2-ter, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *op. cit.*, pp. 1011 ss. e F. CORTESE, sub *art.2-sexies,* ivi, pp. 1043 ss.; G. Carullo, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato,* in *Riv. it. dir. pubbl. com.*, 2020, 1, 136 ss.; S. D'Ancona, *op. cit.*, pp. 612 ss.

perplessità) [41] , anche ai sensi dell'art. 2-sexies, co. 1, consentendo che le amministrazioni[42] possano sempre trattare dati «*se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri*» ad esse attribuiti. In tal caso, la finalità del trattamento può essere indicata dall'amministrazione, purché assicuri una «*adeguata pubblicità all'identità del titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano*».

In questo modo, non solo sarebbero giustificati i trattamenti algoritmici di dati già trattati dal medesimo titolare "pubblico", ma sarebbe possibile anche la comunicazione di dati tra soggetti pubblici, in armonia all'art. 2-ter, co. 2, posta anche la possibilità di comunicarli a soggetti che li trattano per altre finalità ai sensi dell'art. 2-ter, co. 3[43].

Evidentemente, tali regole di favore non fanno venir meno la necessità di rispettare le ulteriori regole relative al trattamento, in particolare in applicazione del principio di trasparenza, come ribadisce lo stesso art. 2-ter, co. 1-bis.

Le considerazioni sin qui svolte vanno poi necessariamente integrate in ragione dell'entrata in vigore il 15 dicembre 2021 del d.lgs. 8 novembre 2021, n. 200, di attuazione della direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico. In base a tale apparato normativo, infatti, si favorisce fortemente il riuso di dati pubblici, nella specie degli *open data*, ma senza pregiudicare il principio di limitazione delle finalità del trattamento: al di fuori dell'ipotesi di anonimizzazione (su cui si tornerà *infra*) una conciliazione tra *open data by design* e *privacy by design* appare piuttosto complessa[44].

---

[41] Sul punto cfr. F. Francario, *Disposizioni "urgenti" in materia di protezione dei dati personali. Brevi note sul trattamento dati per finalità di pubblico interesse,* in *Giustizia insieme*, 26 ottobre 2021, par. 6, che pare comunque propendere per l'applicazione anche all'art. 2-sexies codice privacy.

[42] Più precisamente, l'art. 2-ter, co. 1 bis parla «*di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le Autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196*» e anche di «*una società a controllo pubblico statale di cui all'articolo 16 del decreto legislativo 19 agosto 2016, n. 175, con esclusione per le società pubbliche dei trattamenti correlati ad attività svolte in regime di libero mercato*».

[43] Va comunque dato conto del fatto che questi due commi si prestano a interpretazioni di diverso tenore. Sul punto si rinvia alle considerazioni di F. CARDARELLI, *op. cit.*, pp. 1022 ss.; E. PELINO, sub *art. 2-ter*, in L. Bolognini, E. Pelino (a cura di), *Codice della disciplina privacy*, Giuffrè, Milano, 2019, pp.100-101; F. Pizzetti, *La Parte I del Codice novellato,* in ID. (a cura di), *Protezione dei dati*, cit., pp. 94-96.

[44] Sul punto cfr. Considerando n. 52 della dir. 2019/1024/UE. Per ulteriori considerazioni sulla portata della direttiva, cfr. S. Gobbato, *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli*

Ad ogni modo, sulla base delle riflessioni sin qui svolte, è chiaro che spetta al soggetto pubblico il dovere di considerare attentamente i profili di attuazione delle norme in parola e, più in generale, di progettare il trattamento che intende porre in essere, riflettendo già *ex ante* sulle basi giuridiche più adeguate, sulla compatibilità di usi secondari e sui loro eventuali limiti.

6. *Le modalità del trattamento: a) La "spiegabilità" del trattamento fra trasparenza e* accountability

Nell'ambito dei trattamenti di dati di tipo algoritmico un punto fondamentale è dato poi dalle modalità attraverso cui questi sono operati. Si è visto negli esempi esposti *supra* come si abbia una vera e propria procedimentalizzazione del trattamento, che si scompone in diverse fasi che mirano all'addestramento dell'algoritmo e alla sua messa in opera. Rispetto alla protezione dei dati entro queste fasi è imprescindibile tener conto in particolare dei principi che mirano alla spiegabilità del trattamento (trasparenza e, in certa misura, *accountability*), di tutta quella congerie di principi che intervengono da più punti di vista sulla sicurezza del trattamento (integrità, riservatezza, *privacy by design* e *by default*) e sulla qualità dei dati (minimizzazione, esattezza e limitazione della conservazione).

Quanto al profilo della spiegabilità, assumono rilievo due profili: quello della trasparenza nei confronti degli interessati in ordine ai vari aspetti del trattamento e quello, fortemente connesso al primo [45], della comprensione della portata del trattamento, in modo da mettere in atto e rendicontare le misure adeguate, per assicurare l'*accountability* dell'intera architettura del trattamento da questi realizzata[46]. In termini pratici, ciò significa che il titolare del trattamento dovrà fornire un'informativa

open data della PA: nuove opportunità per le imprese, in *Media Laws*, 2, 2020, pp. 247 ss. Più in generale sugli *open data*, cfr. F. Costantino, *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in *Dir. Amm.*, 2017, pp. 808 ss.; D.-U. Galetta, *Open Government, Open Data e azione amministrativa*, in *Ist. Fed.*, 3, 2019, pp. 663 ss.; G. Carullo, "Open Data" *e partecipazione democratica*, in *Ist. Fed.*, 3, 2019, pp. 685 ss.

[45] Sulla relazione tra trasparenza e *accountability* cfr. da ultimo, G. Malgieri, *op. cit.*, pp. 182 ss., spec. p. 190. Con specifico riferimento alla portata di tali principi rispetto all'amministrazione, cfr., per tutti, C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, n. 22, 2018, 2 ss.

[46] Sui plurimi significati dell'*accountability* cfr WP29, parere n. 3/2010 sul principio di responsabilità e in dottrina, *ex multis*, G. Finocchiaro, *Il principio di accountability*, in *Giur. It.*, 12, 2019, p. 2779.

all'interessato prima di svolgere il trattamento e, al tempo stesso, rendicontare tutte le misure prese nel corso del trattamento.

La "spiegabilità" in questo senso intesa diventa particolarmente difficile da gestire laddove si tratti di trattamenti algoritmici. Basti, a tale riguardo, richiamare l'immagine della *black box*: l'algoritmo, infatti, rappresenta una scatola nera, almeno in certa misura, anche per chi lo ha progettato[47]. Vi è poi un ulteriore limite, peraltro evidenziato anche dalla disciplina del GDPR[48], dato dai diritti di proprietà intellettuale, in particolare quelli legati al segreto commerciale che il produttore dell'algoritmo ha su di esso: questi impediscono, quanto meno, che chi impiega l'algoritmo possa rivelare tutte le informazioni riguardanti il suo funzionamento[49].

Tenendo conto di queste problematicità e riferendosi ai casi analizzati, va osservato che essi riguardavano l'impiego di algoritmi ML e DL inseriti nell'ambito di un articolato processo di *big data analytics*.

Si è potuto apprezzare come i trattamenti analizzati, peraltro, prevedano molte sottofasi e, dunque, la loro comprensione non sia particolarmente agevole.

Ora, soffermandoci sul piano della trasparenza, è chiaro che, per assicurarla, occorre bilanciare la completezza delle informazioni fornite e la loro comprensibilità, tenendo conto che il punto di riferimento del principio di trasparenza è dato dalla strumentalità rispetto all'autodeterminazione informativa dell'interessato[50]. Dunque, l'onere che incomberebbe sulle amministrazioni che intendono fare uso di algoritmi nei propri trattamenti non implica una *full disclosure*, ma la fornitura di una informazione sufficiente a garantire l'autodeterminazione informativa e la possibilità di tutelarsi[51]. A

[47] Sul problema della *blackbox* si vedano, fra i molti - oltre al celebre F. Pasquale, *The Black Box Society: The Secret Algorithms that control Money and Information*, Harvard Univ. Press, 2016 - G. LO SAPIO, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione,* in *Federalismi.it*, 16, 2021, pp. 117 ss.; B. Ponti, L*a mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi*, in *Dir. Inf.*, 2019, pp. 389 ss., spec. pp. 392 ss.; M. Martini, *Blackbox Algorithmus - Grundfragen einer Regulierung Künstlicher Intelligenz*, Springer, Berlin, 2019.

[48] Cfr. Considerando 63 GDPR.

[49] Sul fatto che gli algoritmi ricadano entro lo spetto applicativo della normativa europea in tema di segreti commerciali, cfr. M. Maggiolino, *EU Trade Secrets Law and Algorithmic Transparency*, in *Bocconi Legal Studies Research Paper*, 2019, pp. 5 ss. Sul rischio che le norme in materia di diritti di proprietà intellettuale possano vanificare l'accesso alle informazioni cfr. G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2, 2019 p. 224.

[50] Sia consentito rinviare a S. Franca, *L'informativa trasparente nel trattamento dei dati personali da parte della pubblica amministrazione*, in *Nuove aut.*, 2020, spec. p. 245.

[51] Cercando di trarre un esempio dalla fattispecie relativa alla segnalazione degli esposti, non è necessario che l'interessato sia reso edotto anche dei profili specifici dei singoli trattamenti, ma semplicemente le informazioni sufficienti per tutelarsi. La prospettiva difesa nel testo sembra in linea con la Proposta reg. IA (p. 13).

questo riguardo è necessario tenere conto delle discipline relative al diritto di accesso, delle norme in materia di proprietà intellettuale e del modo di acquisizione dell'algoritmo da parte della p.a.[52], in modo che si abbia un accesso graduale alle informazioni. Le informazioni ex art. 12 ss. GDPR dovrebbero essere più sintetiche e garantire la comprensione della portata del trattamento, potendo poi essere arricchite in presenza dei requisiti per esperire il rimedio dell'accesso [53] . In ogni caso, l'amministrazione dovrebbe essere depositaria del quadro completo di informazioni relative all'algoritmo, non solo per garantire un effettivo accesso alla tutela da parte dei cittadini, ma anche per verificare se vi sia un problema di *bias*, in virtù del principio di *accountability*[54].

In questa prospettiva, si circoscrive fortemente il problema della *blackbox*[55].

Si tratta di una prospettiva che pare ben tracciata nella Proposta reg. IA, nella misura in cui sono previsti specifici contenuti relativi agli obblighi informativi per i sistemi di IA ad alto rischio (art. 13) e per determinati sistemi di IA (art. 52), che vedono partecipi diversi soggetti della filiera di trattamento del dato, sino al ruolo delle autorità pubbliche di vigilanza (Capo 3).

Tuttavia, anche questo doppio livello della spiegabilità richiede una particolare attenzione da parte del titolare nel calibrare il trattamento in modo da mantenere un duplice livello di informazioni, quelle fornite all'interessato e quelle mantenute dal titolare, in modo che si riesca a garantire tanto la trasparenza del trattamento, quanto l'*accountability* del suo titolare.

---

[52] Sui differenti regimi in relazione al fatto che l'algoritmo sia acquisito su commissione dalla p.a. ovvero se sia utilizzato in base a contratti ad effetti obbligatori cfr. G. Resta, *op cit.*, pp. 224 ss.

[53] Cfr. G. Resta, *op. cit.*, p. 224, il quale richiama anche l'impostazione di TAR Lazio, 14 febbraio 2017, n. 3769, nel ritenere inopponibile al privato l'argomento basato sulla proprietà intellettuale. Occorre però considerare che il segreto commerciale viene fatto salvo anche nella proposta di regolamento in materia di IA: cfr. Proposta reg. IA, p. 13 e art. 70, peraltro in linea con l'art. R. 311-3-1-2 del Code des relations entre le public et l'administration. Cfr. in tema G. Avanzini, *op. cit*., p. 125; A. Bibal, M. Lognoul, A. de Streel, B. Frénay, *Legal requirements on explainability in machine learning*, in *Artificial Intelligence & Law*, 28, 2, 2020, pp. 154-155.

[54] Rimanendo agli esempi visti prima, in particolare a quello delle *fake news*, il titolare deve essere in grado di verificare che vi sia un problema di *bias* nell'operatività dell'algoritmo e così intervenire a garanzia dei diritti degli interessati e della legalità del trattamento.

[55] T. Wischmeyer, *Artificial Intelligence and Transparency: Opening the Black Box*, in T. Wischmeyer, T. Rademecher (a cura di), *Regulating artificial intelligence*, Cham, 2020, p. 78. Analogamente, cfr. la proposta di un diritto alla conoscenza della logica di fondo dell'algoritmo C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Biolaw journal*, special issue, 2, 2019, 723; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw Journal*, 1, 2019, 76. Sul rilievo degli obblighi informativi in questo senso, sia consentito il rinvio a S. Franca, *La regolazione dell'intelligenza artificiale in Germania: stato dell'arte e prospettive future*, in *Riv. reg. mercati*, 1, 2020, pp. 64-65.

7. *Segue: b) la sicurezza del trattamento*

Un ulteriore profilo da valutare attiene al tema della sicurezza del trattamento. Come è stato osservato, la sicurezza assume plurimi significati, potendo la sua violazione tradursi in perdita di confidenzialità, di integrità o di disponibilità[56]. Il punto è affrontato dal GDPR, ove si dispone che i dati debbano essere «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*», con ciò illustrando i principi di riservatezza e integrità del trattamento[57]. Tali principi si legano poi a doppio filo ai principi di *privacy by design* e *by default*, ossia all'idea per cui la tutela del dato debba avvenire sin dal momento della progettazione (*by design*) e per impostazione predefinita (*by default*).

A fini ricostruttivi, si possono isolare due momenti rilevanti nella determinazione delle misure: la prima, relativa all'individuazione dei rischi relativi al trattamento; la seconda, concernente l'individuazione delle specifiche misure atte a mitigare i rischi[58].

Per quanto riguarda la prima, uno strumento fondamentale è costituito dalla valutazione d'impatto (d'ora in avanti, DPIA). Ai sensi dell'art. 35, par. 1 GDPR, essa è resa obbligatoria nei casi in cui un trattamento possa presentare un «*rischio elevato per i diritti e le libertà delle persone fisiche*».

Dunque, per la generalità dei trattamenti, la valutazione di impatto costituisce un adempimento eventuale, a carattere eccezionale. Vi è però da dire che nel caso dell'IA parrebbe darsi la necessità di una generalizzazione dell'impiego della DPIA. Ciò non tanto perché qualsiasi trattamento tramite algoritmi comporti un rischio elevato per diritti e libertà, ma perché tale valutazione consente di aderire al *risk-based approach*, ponendo dunque al centro l'individuazione e la gestione del rischio[59]. Si consente così di svolgere una mappatura del trattamento che si rivela utile per plurime le ragioni: per la ricerca delle opportune basi giuridiche; per assicurare la trasparenza; per evidenziare

[56] Su tali diversi significati si v. G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, Torino, 2017, pp. 191 ss.

[57] Sulla portata di tali principi, cfr. M. Dell'Utri, *op. cit.*, pp. 218-219; G. MALGIERI, *op. cit.*, pp. 188-189.

[58] In questo senso pare muoversi anche il libro bianco dell'Agid denominato "L'intelligenza artificiale al servizio del cittadino" del 21 marzo 2018 (p. 56).

[59] Su tale impostazione in materia di protezione dei dati personali cfr., *ex multis*, M.S. Esposito, *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Dir. inform.*, n. 4, 2019, pp. 1071 ss.; A. Mantelero, *La gestione del rischio*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lg. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, pp. 473 ss.; R. TORINO, *La valutazione di impatto*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *op. cit.*, pp. 856 ss.

i rischi che necessitano di essere temperati con opportune misure tecniche organizzative[60]. Né un simile utilizzo si rivelerebbe contrastante con quanto previsto dal GDPR, ma anzi concorrerebbe a rafforzare l'*accountability* del titolare[61]. Il vantaggio ricollegabile all'impiego della DPIA consiste poi nel permettere al titolare di verificare dove si coagulano le maggiori criticità legate al trattamento e, dunque, dove poter intervenire con le misure tecniche e organizzative. Nel suo adattamento all'IA, evidentemente, occorre tener conto che non tutti i rischi sono prevedibili, sicché la valutazione di impatto non può limitarsi ad una previsione *ex ante*, ma andrebbe rafforzata con sistemi di valutazione e monitoraggio anche *ex post*[62]. Ad ogni modo, la meritevolezza dell'approccio fondato sul rischio pare attestata anche nella Proposta di regolamento in tema in di IA, che distingue tra diverse categorie di rischio e individua diverse modalità di gestione del rischio[63].

Per quanto attiene invece alle misure che si possono adottare è necessaria una riflessione preliminare sull'anonimizzazione.

A livello generale, giova ricordare che il trattamento di dati anonimi consente a chi lo svolge di uscire dalla sfera applicativa del GDPR. L'obiettivo del trattamento di dati anonimi appare particolarmente utile per i trattamenti in ambito pubblico, giacché consente di ottenere il materiale necessario ad arricchire l'istruttoria procedimentale, senza però dover incaricarsi di adempiere alle regole del GDPR per tutta la filiera del trattamento. Si tratta poi di una soluzione per contemperare le esigenze di apertura dei dati e, al tempo stesso, di tutela i dati personali che lo stesso legislatore europeo ha suggerito[64].

Non bisogna nascondere, tuttavia, che si tratta di un obiettivo difficilmente raggiungibile, anche tenendo conto del fatto che l'identificabilità di un interessato assume rilievo anche qualora vi sia la sola possibilità giuridica di realizzazione[65], dovendosi peraltro tener conto del contesto di riferimento, anche dal punto di vista

[60] Sul rilievo dell'attività di mappatura dei trattamenti sia permesso rinviare a S. FRANCA, *La semplificazione*, cit, pp. 635 ss.

[61] Come rilevato in G. Finocchiaro, *Il principio*, cit., p. 2779 (che richiama quanto stabilito nel parere n. 3/2010 del WP29) l'*accountability* si basa anche su un livello "volontario", ossia su un sistema di responsabilità che trascende le norme minime in tema di protezione dei dati.

[62] In relazione alle valutazioni ex post cfr. G. Orsoni, E. D'Orlando, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Ist. Fed.*, 3, 2019, pp. 615-616; P. OTRANTO, *op. cit.*, p. 203.

[63] Per un quadro ricostruttivo completo, cfr. C. Casonato, B. Marchetti, *op. cit.*, pp. 421 ss.

[64] Ci si riferisce al già richiamato Considerando n. 52 della dir. 2019/1024/UE.

[65] Sul punto è fondamentale il caso Breyer (C- 582/14 del 19 ottobre 2016), su cui si vedano i rilievi di C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Giappichelli, Torino, 2020, p. 28.

tecnologico[66]. Qui emerge con particolare nettezza la problematicità data dall'impiego dell'IA che si avvale di *big data*, considerato che tanto maggiore è la quantità di dati a disposizione, tanto più probabile è il rischio di una eventuale re-identificazione[67].Tenendo conto di tale *caveat*, l'anonimizzazione potrebbe comunque rappresentare una semplificazione.

Bisogna anche considerare, al di là della praticabilità dell'anonimizzazione, che a volte potrebbe essere la stessa amministrazione a preferire non rendere anonimi i propri dati[68]. Si pensi alla possibilità di profilare gli *haters*, così da ricavare un nesso tra il livello di istruzione e la perpetrazione di atteggiamenti di *hating online*. O si pensi, ancora, all'analisi del dato relativo alla collocazione a livello geografico o in uno specifico settore merceologico per quanto riguarda la segnalazione degli esposti. Si tratta evidentemente di un *trade-off*, in cui ad una maggiore acquisizione di dati da parte della p.a. si accompagna una necessaria configurazione delle opportune misure di sicurezza, tenendo conto che la conformità alle regole in materia di protezione dei dati rappresenta comunque un costo per le amministrazioni. Da questo punto di vista, l'anonimizzazione non rappresenta una scelta obbligata, essendo possibile il ricorso a misure come la pseudonimizzazione, l'archiviazione protetta, etc.[69]

Tra queste misure, particolare attenzione merita un'ulteriore possibilità, quella del *federated machine learning*. Si tratta di sistemi di esecuzione remota degli algoritmi di *machine learning* che facilitano la *governance* del dato. Essi, infatti, consentono di evitare i trasferimenti di dati verso i s*erver* utilizzati per l'addestramento dell'algoritmo, attraverso l'utilizzo di dispositivi decentralizzati per svolgere l'addestramento, senza

[66] Sul punto cfr. WP20, Parere 5/2014 sulle tecniche di anonimizzazione, adottato il 10 aprile 2014. Si vedano pure G. Finocchiaro, *Intelligenza artificiale*, cit., p. 1674; A. Nervi, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *op. cit.*, p. 176;

[67] Si pensi alla combinazione di più *dataset* per l'allenamento dell'algoritmo: è evidente, infatti, che un *dataset* totalmente anonimizzato, una volta combinato con un ulteriore *dataset*, potrebbe permettere l'identificabilità dei soggetti cui i dati si riferiscono. Ancora, lo sviluppo di nuove tecnologie algoritmiche può far sì che un dato inizialmente ritenuto anonimo possa poi divenire nuovamente identificabile. Sui problemi legati ad una effettiva anonimizzazione cfr. le considerazioni di P. Guarda, *Il regime*, cit., p. 210; C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità,* in *Jus civile*, 2, 2020, pp. 386 ss.

[68] Cfr. F. Modafferi, *op. cit.*, pp. 404-405, in cui si rileva come spesso l'analisi dei *big data*, quando mira a studiare caratteristiche e comportamenti degli individui, non può prescindere da elementi che li rendono identificabili.

[69] La pseudonimizzazione rappresenta una vera e propria misura di sicurezza che non fa perdere al dato la sua natura personale. Tramite l'assegnazione di codici di pseudonomizzazione si rende più difficile l'identificazione del soggetto interessato, ma essa rimane sempre possibile. Sulla distinzione tra pseudonimizzazione e anonimizzazione si v.
v. G. D'Acquisto, M. Naldi, *op. cit.*, pp. 41-169.

scambiare i dati. Si tratta di una soluzione che non risolve di per sé il problema della protezione dei dati[70], ma che senz'altro può essere esplorata, nella prospettiva di ridurre i rischi riconducibili all'incameramento di ingenti quantità di dati in un unico *server*[71].
In ogni caso, al di là delle riflessioni che possono essere svolte per ciascuna delle misure illustrate, è chiaro che la scelta in ordine alle singole misure non può che rimanere in capo al titolare del trattamento, nelle specie alle amministrazioni. Dunque, l'apertura del GDPR a soluzioni eterogenee si accompagna alla necessaria responsabilizzazione delle amministrazioni stesse, senza che nessuna scelta sia preclusa.

8. *Segue: c) la qualità dei dati*

Quando ci si riferisce al concetto di qualità dei dati si fa riferimento a un concetto che rileva da più punti di vista, non solo quello della protezione dei dati, e che è definibile come «*l'insieme delle caratteristiche di un'entità, idonee a soddisfare le esigenze esplicite ed implicite*»[72]. Ciò significa che la qualità dei dati rappresenta, in certa misura, un concetto funzionale rispetto al potenziale utilizzo che del dato si può fare. Il GDPR restituisce pienamente l'attenzione alla qualità in questo senso intesa e lo fa attraverso diversi principi: esattezza, minimizzazzione e limitazione della conservazione[73]. Dalla triangolazione tra questi principi si evince che il titolare debba garantire l'adeguatezza, la pertinenza e la limitazione del trattamento a quanto necessario per raggiungere la finalità del medesimo, adottando «*tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*» e conservando i dati trattati entro un termine che non vada oltre il raggiungimento della finalità del trattamento.
L'assetto normativo riguardante la qualità del dato solleva però alcune problematicità rispetto a trattamenti operati dall'IA.
In primo luogo, se l'intelligenza artificiale si nutre di dati è chiaro che la qualità di questo nutrimento è rilevante, in base al principio *garbage in, garbage out*: la bassa

[70] Sul punto cfr. G.A. Kaissis, M.R. Makowski, D. Rückert, R.F. Braren, *Secure, privacy-preserving and federated machine learning in medical imaging*, in *Nature Machine Intelligence*, 2, 2020, p. 308.
[71] Da questo punto di vista, assumono rilievo anche le norme della proposta di regolamento IA relative agli ambienti di sperimentazione citate *supra* alla nt. 12.
[72] Cfr. quanto stabilito nello standard. ISO 8402, Quality Management and Quality Assurance Vocabulary, richiamato pure in E. Carloni, *Qualità dei dati,* big data *e amministrazione pubblica*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino, Rubbettino, 2021, p. 118.
[73] In linea con questa prospettiva della qualità del dato nel GDPR cfr. E. Carloni, *op. cit.*, p 127; G. Finocchiaro, *Intelligenza artificiale*, cit., p. 1674.

qualità del dato porta inevitabilmente a risultati di elaborazione di bassa qualità[74]. Va detto che la bassa qualità di un *dataset* può dipendere anche dal fatto che esso non contiene una base sufficientemente omogenea di dati: si pensi al caso degli algoritmi predittivi delle situazioni di dissesto, ove il numero dei Comuni in *default* è molto limitato, comparato a quello degli altri Comuni[75].

In secondo luogo, nel caso della *data analytics* strumentale a trattamenti algoritmici il fatto che si attinga ad enormi quantità di dati implica che il problema possa assumere una portata esponenziale. Si pensi al caso della segnalazione degli esposti: se l'algoritmo riconoscesse come ammissibili esposti che contengono alcune parole chiave, ma si rivelassero totalmente sconclusionati, evidentemente, non si genererebbe l'accrescimento di efficienza auspicata dall'impiego dell'algoritmo stesso.

In terzo luogo, è necessario coordinare l'esigenza relativa alla qualità del dato con l'esercizio dei diritti dell'interessato: pur se questi ultimi non sono considerabili come diritti *ad nutum*[76], devono poter essere esercitati in ogni momento del trattamento e anche tempestivamente[77]. Questo presuppone, evidentemente, che tanto il titolare, quanto l'interessato siano in grado di comprendere la portata del trattamento che investe il secondo. Sussistendo tale presupposto occorre anche progettare il trattamento algoritmico in modo che sia possibile non solo interrompere il funzionamento dell'algoritmo e rimuovere alcuni dei dati utilizzati, in caso di istanze di cancellazione, rettifica e limitazione del trattamento. Non è un caso che la proposta di regolamento in materia di IA rilevi la necessità di costruire *set* di dati per l'addestramento degli algoritmi «*sufficientemente pertinenti, rappresentativi e privi di errori, nonché completi alla luce della finalità prevista del sistema*» e anche basati su «*proprietà statistiche appropriate*»[78].

Rimangono dunque numerose soluzioni aperte ai titolari, ma, ancora una volta, il fatto che una scelta sia operata è essenziale per delineare un regime del dato valevole sino al momento della cancellazione o anonimizzazione o, eventualmente, di un successivo riutilizzo.

Anche in questo caso, tuttavia, si può ricavare che il GDPR non ponga regole stringenti in una direzione o in un'altra, lasciando sempre al titolare la possibilità di muoversi entro un perimetro che rimane, ad ogni modo, particolarmente ampio.

---

[74] In tema, cfr. G. FINOCCHIARO, *Intelligenza artificiale*, cit., p. 1674; G. Resta, *op. cit.*, p. 208.
[75] Cfr. N. Antulov-Fantulin, R. Lagravinese, G. Resce, *op. cit.*, p. 683.
[76] G. Finocchiaro, *Intelligenza*, cit., p. 1675, con specifico riferimento al diritto all'oblio.
[77] Cfr. considerando n. 59 del GDPR, la risposta alle istanze presentate dagli interessati deve pervenire «*senza ingiustificato ritardo e al più tardi entro un mese*»
[78] Cfr. Considerando n. 44 della Proposta reg. IA. Con riferimento ai sistemi di IA ad alto rischio, cfr. l'art. 10 della Proposta reg. IA.

9. *Conclusioni*

Le esperienze di sperimentazione dell'intelligenza artificiale nell'ambito di attività che vedono protagonista la pubblica amministrazione, rappresentano un utile punto di vista per mettere a fuoco la duplice valenza delle stesse, come risorsa utile per l'efficientamento dell'amministrazione, da un lato, e come possibile fonte di criticità sul piano della tutela dei dati del cittadino, dall'altro lato. Nella prospettiva di una sempre maggiore diffusione di queste sperimentazioni e, in particolare, della loro messa a regime è necessario svolgere le analisi necessarie affinché le tecnologie impiegate si rivelino GDPR *compliant*.

In questa prospettiva, guardando alla concreta architettura delle singole sperimentazioni e alle regole del GDPR ad esse applicabili pare emergere una visione meno manichea, non solo delle sperimentazioni stesse, ma anche delle regole in materia di protezione dei dati. Queste ultime, in effetti, purché non concepite in modo estremamente rigido, paiono strutturate in modo sufficientemente aperto a gestire le principali problematicità dei trattamenti di dati implicati dalla messa in regime di simili soluzioni sperimentali. Senza dubbio, nell'auspicata approvazione della Proposta reg. IA, come si è avuto modo già di verificare incidentalmente nel corso della trattazione[79], si porrà la possibilità di delineare un quadro di garanzie più solido e pur sempre in linea con il GDPR[80].

Allo stato, vi è comunque un ampio spazio per ciascuna pubblica amministrazione che funge da titolare del trattamento per poter adottare soluzioni di tipo differente.

Tuttavia, si è potuto apprezzare come le singole questioni isolate siano fortemente collegate l'una all'altra (si pensi a come la scelta della base giuridica influisca sulla trasparenza del trattamento o a come quest'ultima sia necessaria per individuare i rischi del trattamento e garantire l'esercizio dei diritti strumentale alla qualità dei dati), ma, soprattutto, la scelta di una soluzione che concerne uno specifico profilo ha ricadute anche sugli altri elementi del trattamento: ne è un esempio evidente la scelta della anonimizzazione.

Peraltro, si è visto che le misure utili alla protezione dei dati dipendono fortemente anche dagli obiettivi delle singole sperimentazioni, pur considerando che, anche quando può rivelarsi più efficiente svolgere analisi dalla portata più ampia, non si può trascurare

[79] Ulteriori considerazioni sul raffronto tra GDPR e Proposta reg. IA, ad esempio rispetto alla previsione della garanzia dell'apporto umano e alle carenze dell'art. 22 GDPR, si rinvengono in C. Casonato, B. Marchetti, *op. cit.*, pp. 428 ss.

[80] Giova ricordare che la proposta si pone in chiara continuità con la disciplina in tema di protezione dei dati (cfr. Proposta reg. IA, p. 4).

il disposto del principio di minimizzazione, che impedisce di raccogliere più dati di quanti siano necessari.

In questa prospettiva, si rende dunque necessario adottare una prospettiva autenticamente *by design*, per la progettazione dell'intero trattamento – e già nella fase di sperimentazione –, in modo che la visione congiunta delle esigenze di efficientamento e di protezione dei dati possa agevolare la messa in opera di trattamenti innovativi basati su algoritmi. Non si intende con ciò sminuire la rilevanza di ulteriori regole, anche di natura etica – pur se la loro adozione può sempre comportare una parziale entropia all'interno del sistema[81] - così come non si intende trascurare le debolezze proprie della regolazione del GDPR[82]. Si vuole invece ribadire che il GDPR offre un cospicuo margine di flessibilità, laddove non lo si concepisca come un sistema chiuso di norme, ma come la fonte di un metodo di gestione dei trattamenti di dati[83]. Spetta, dunque, alle autorità pubbliche, individuate come titolari del trattamento, il compito di utilizzare e sviluppare questo metodo di gestione, in modo da adattarlo alle proprie esigenze[84], rimanendo sempre *accountable*.

Da questo angolo visuale, nelle more dell'approvazione della Proposta reg. IA, pare esservi comunque la possibilità di garantire il proliferare di sperimentazioni che contemperino le esigenze di sicurezza e innovazione della p.a., anche nella prospettiva di una loro messa a regime.

[81] Sul problema della regolazione etica in tema di IA cfr. E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della regolazione dei mercati*, 1, 2020, 29 ss.

[82] Cfr. *supra* par. 1.

[83] Cfr. sul punto, in part., F. Pizzetti, *GDPR, Codice novellato e Garante nell'epoca dei Big Data e della Intelligenza Artificiale*, in ID. (a cura di), *Protezione dei dati personali*, cit., pp. 233 ss., spec. p. 287.

[84] In questo senso, appare necessario superare la visione della protezione dei dati come mero fattore complicante, inserendolo *by design* e *by default* nello svolgimento dell'ordinaria attività amministrativa, in una logica che dia conto della complessità che si instaura tra regole dell'azione amministrativa e regole del trattamento. Su tali profili, sia consentito il rinvio a S. Franca, *La semplificazione*, cit., *passim*.