Miriam Allena e Scilla Vernile

INTELLIGENZA ARTIFICIALE, TRATTAMENTO DI DATI PERSONALI E PUBBLICA AMMINISTRAZIONE

1. *Premessa: il ruolo delle pubbliche amministrazioni nella protezione dei dati personali*

Il tema del trattamento dei dati personali interessa le pubbliche amministrazioni sotto plurimi punti di vista. L'autorità principale in materia è senza dubbio il Garante per la protezione dei dati personali[1], istituito con l. 675/1996, che, come si evince agevolmente dal nome, svolge funzioni di vigilanza sulla corretta applicazione (ora) del Regolamento UE 2016/679 (Regolamento generale sulla protezione dei dati, d'ora in avanti indicato con l'acronimo inglese GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché della libera circolazione di tali dati, e di ogni altra legge o regolamento nazionale che contenga prescrizioni circa le modalità di trattamento dei dati personali a tutela dei diritti e delle libertà fondamentali degli individui[2].

Cap. XIV di: ASTRID, *Intelligenza artificiale e diritto: una rivoluzione?,* vol.I, Il Mulino, 2022

[1] Sulla natura di autorità amministrativa indipendente, cfr. A. Patroni Griffi, *L'indipendenza del Garante*, in «Federalismi.it», 14/2/2018.

[2] Attività di cui il Garante dà conto nella relazione che trasmette annualmente al Parlamento e al governo e che è svolta in collaborazione con le autorità aventi analoghe competenze negli altri Stati membri. Incidentalmente, si ricordi che sempre al Garante è affidato il compito di gestire i reclami presentati dai soggetti interessati rispetto al trattamento dei propri dati personali e di adottare ogni misura idonea per ingiungere ai titolari o ai responsabili di conformarsi alle prescrizioni normative. Alle funzioni di vigilanza si affiancano quelle di carattere regolatorio che la legge attribuisce al Garante, nonché tutte quelle attività di diffusione della «cultura» della protezione dei dati personali, tramite iniziative

Sebbene il Garante sia indubbiamente l'autorità protagonista nel perseguimento dell'interesse pubblico alla protezione dei dati personali, anche in virtù delle sue funzioni regolatorie[3], non può non rilevarsi che l'attività di tutela dei dati personali è condivisa con tutte le amministrazioni pubbliche.

In primo luogo, perché le amministrazioni inevitabilmente «trattano» dati personali per esercitare le loro funzioni[4], tanto che il GDPR riconosce espressamente la liceità del trattamento ove sia «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»[5], anche a prescindere dal consenso dell'interessato. Le pubbliche amministrazioni, nell'esercizio delle loro funzioni, gestiscono infatti necessariamente una grande vastità e complessità di dati personali, di cui deve essere garantita la protezione: tanto che il GDPR, all'art. 37, ha introdotto una figura apposita, ossia il responsabile della protezione dei dati personali, il quale deve essere obbligatoriamente individuato da ogni ente pubblico o congiuntamente da più enti pubblici, sulla base della loro struttura organizzativa e della loro dimensione[6].

volte ad accrescere la consapevolezza e la «sensibilità» del pubblico sull'importanza della protezione dei dati personali.

[3] A. Frosini, *Gli atti normativi del Garante per la protezione dei dati personali*, in «Giurisprudenza costituzionale», 2014, n. 4, 3678; G. Di Cosimo, *Sul ricorso alle linee guida da parte del Garante per la privacy*, in «osservatoriosullefonti.it», 1, 2016.

[4] M. Clarich, *Trasparenza e protezione dei dati personali nell'azione amministrativa*, in «Il Foro amministrativo. TAR», 2004, n. 12, 3885; G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017, pp. 21 ss.; Id., *Trattamento dei 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, p. 131.

[5] Art. 6, par. 1, lett. *e*.

[6] Cfr. le linee guida sui responsabili della protezione dei dati, adottate il 13/12/2016 ed emendate in data 5/4/2017, dal Gruppo di lavoro articolo 29 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali. Sulla figura del *Data protection officer* (DPO) negli enti pubblici, interno o esterno, cfr. F. Lorè, *Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del*

In secondo luogo, perché le amministrazioni sono altresì responsabili della ponderazione tra le esigenze di pubblicità e trasparenza dell'organizzazione e dell'azione amministrativa, valori irrinunciabili di un'amministrazione moderna, e quelle di riservatezza dei soggetti interessati[7]. Senza entrare nel merito della disciplina in materia di accesso ai documenti amministrativi, come oggi articolata ai sensi del combinato disposto del capo V della l. 241/1990 e del decreto Trasparenza (d.lgs. 33/2013, come significativamente modificato nel 2016)[8], è ben noto che, ove sia domandato di accedere a documenti e informazioni contenenti dati personali di terzi, l'amministrazione che detiene il dato è tenuta a bilanciare l'interesse all'accesso

Regolamento generale sulla protezione dei dati personali UE 2016/679, in «Rivista di diritto amministrativo», 2018 n. 7-8; G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, in «Giornale di diritto amministrativo», 2018, n. 4, p. 415. Cfr. anche TAR Puglia, Lecce, sez. III, 13/9/2019, n. 1468, sui requisiti necessari ove il responsabile per la protezione dei dati sia una persona giuridica, e TAR Friuli-Venezia Giulia, Trieste, sez. I, 18/7/2018, n. 252, sulla pubblicità necessaria per l'affidamento del servizio di protezione dei dati personali.

[7] E. D'Alterio, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'«ordine segreto»*, in «Giornale di diritto amministrativo», 2019, n. 1, p. 9.

[8] Senza pretesa di esaustività, cfr. D.U. Galetta, *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del decreto FOIA: la trasparenza de «le vite degli altri»?*, in «Federalismi.it», 2018; Id., *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in «Rivista italiana di diritto pubblico comunitario», 2016, n. 5, p. 1019; S. Vaccari, *Decisioni amministrative e interessi pubblici sensibili: le nuove regole sulla trasparenza*, in «Le Istituzioni del Federalismo», 2017, pp. 1021 ss.; E. Carloni, *Il nuovo diritto di accesso generalizzato e la persistente centralità degli obblighi di pubblicazione*, in «Diritto amministrativo», 2016, n. 4, p. 579; M. Savino, *Il FOIA italiano. La fine della trasparenza di Bertoldo*, in «Giornale di diritto amministrativo», 2016, n. 5, p. 593; A. Marchetti, *Le nuove disposizioni in tema di pubblicità e trasparenza amministrativa dopo la riforma «Madia»: anche l'Italia ha adottato il proprio Foia? Una comparazione con il modello statunitense*, in «Federalismi.it», 2017; A. Cauduro, *Il diritto di accesso a dati e documenti amministrativi come promozione della partecipazione: un'innovazione limitata*, in «Diritto amministrativo», 2017, n. 3, p. 601.

del richiedente con la privacy del soggetto cui si riferiscono i dati richiesti[9].

Nel presente contributo, dopo avere dato conto delle più recenti previsioni in tema di trattamento dei dati personali per finalità di pubblico interesse, ci si soffermerà in particolare sul compito spettante alle amministrazioni pubbliche di assicurare, nell'esercizio della loro attività autoritativa, la protezione dei dati personali intesa come garanzia di un uso corretto e non discriminatorio degli stessi, oltre che nei termini, più evidenti, del controllo della diffusione illecita o della predisposizione degli accorgimenti opportuni per evitare la perdita, la distruzione o il deterioramento di tali dati. In particolare, il tema del «trattamento» dei dati personali – definito dall'art. 4 del GDPR, par. 2, come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» – sarà affrontato tenendo conto dell'impatto del progresso tecnologico e della transizione digitale cui le amministrazioni sono chiamate[10].

L'utilizzo di banche dati dotate di una capacità inedita di raccolta e gestione di dati, l'avvento di nuove tecnologie capaci di rivoluzionare completamente la tenuta e la gestione dei dati, unite al sempre più frequente ricorso a strumenti informatici in grado di adottare decisioni sulla base dei dati

[9] F. Manganaro, *Evoluzione ed involuzione delle discipline normative sull'accesso a dati, informazioni ed atti delle pubbliche amministrazioni*, in «Diritto amministrativo», 2019, n. 1, p. 743.

[10] Si ricordi incidentalmente che circa il 27% delle risorse totali del Piano nazionale di ripresa e resilienza (PNRR) è destinato agli interventi per favorire la transizione digitale. Cfr. G. Sgueo, *Lo Stato digitale nel PNRR. La transizione digitale dei procedimenti amministrativi*, in www.irpa.eu.

acquisiti, pongono nuove sfide per le amministrazioni[11]. Pur nella consapevolezza dei vantaggi in termini di efficienza e tempestività dell'azione amministrativa, occorrerà, allora, verificare l'impatto delle nuove tecnologie e dell'intelligenza artificiale sull'attività amministrativa quando quest'ultima è chiamata ad assicurare, nel suo svolgimento, la protezione dei dati personali.

2. *Il trattamento dei dati personali per finalità di pubblico interesse*

Il d.l. 8/10/2021, n. 139, cd. decreto Capienze, nel prevedere disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni, ha dettato altresì disposizioni in tema di dati personali. In particolare, l'art. 9, intervenendo sul testo dell'art. 2-*ter* del Codice in materia di protezione dei dati personali (d.lgs. 196 del 2003), ha esteso la base giuridica del trattamento dei dati personali quando lo stesso sia effettuato da una pubblica amministrazione: dopo il comma 1 – il quale prevede che la base giuridica per il trattamento dei dati personali sia «costituita da una norma di legge, di regolamento da atti amministrativi generali» – è stato infatti aggiunto un nuovo comma 1-*bis*, a norma del quale il suddetto trattamento è anche consentito se «necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti»[12].

[11] M. Tresca, *Big data, open data e algoritmi: i dati al servizio della pubblica amministrazione*, in «Rivista trimestrale di Diritto pubblico», 2021, n. 2, p. 545.

[12] «1-*bis*. Il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del d.lgs. 30/3/2001, n. 165, ivi comprese le Autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della l. 31/12/2009, n. 196, nonché da parte di una società a controllo pubblico statale di cui all'articolo 16 del d.lgs. 19/8/2016, n. 175, con esclusione per le società pubbliche dei trattamenti correlati ad attività svolte in regime di libero mercato, è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri

Il testo, convertito con modificazioni della l. 3/12/2021, n. 205, ha suscitato un vivace dibattito in dottrina e nelle competenti sedi parlamentari[13].

Volendo riassumere in poche battute una questione complessa[14], si può dire che la conseguenza della nuova previsione è che, laddove vi sia una legge che attribuisca a una pubblica amministrazione un determinato compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ciò è sufficiente per consentire alla stessa il trattamento dei dati personali, senza che sia necessaria una ulteriore espressa previsione di legge o di regolamento che precisi per quale specifica finalità viene consentito il trattamento: è semmai il soggetto pubblico a dover indicare tale finalità in coerenza al compito svolto o al potere esercitato. In tal modo, il trattamento dei dati personali da parte delle pubbliche amministrazioni viene chiaramente differenziato rispetto al trattamento dei medesimi dati che sia effettuato dai privati: mentre quest'ultimo, essendo basato sul consenso dell'interessato, necessita di una espressa indicazione, tramite legge (o regolamento, o atto amministrativo generale), della finalità del trattamento onde prevenire ipotesi di abuso, nel caso

a essa attribuiti. La finalità del trattamento, se non espressamente prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento, è indicata dall'amministrazione, dalla società a controllo pubblico in coerenza al compito svolto o al potere esercitato, assicurando 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».

[13] Cfr. gli interventi scritti acquisiti in sede di audizione al Senato dalla Commissione permanente (Affari costituzionali) nella seduta n. 292 del 3/11/2021, riguardante la «Conversione in legge del d.l. 8/10/2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali». Sul tema cfr., per tutti, F. Francario, *Protezione dati personali e pubblica amministrazione*, in «Giustizia insieme», 1/9/2021.

[14] Si prescinderà qui dai profili di sussistenza o meno dei caratteri di effettiva necessità e urgenza che, soli, giustificano l'inserimento di una data previsione nel testo di un decreto-legge.

delle pubbliche amministrazioni tale espressa indicazione legislativa non è più ritenuta necessaria.

La nuova norma, è appena il caso di evidenziarlo, riprende testualmente l'art. 6, par. 1, lett. *e* del GDPR, ai sensi del quale il trattamento dei dati personali è lecito – tra gli altri – se «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»[15]. L'art. 6, par. 3, del GDPR prevede poi che la finalità del trattamento sia determinata dalla base giuridica costituita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento, ovvero, alternativamente, «per quanto riguarda il trattamento di cui al paragrafo 1, lett. *e*», è quella «necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento».

Il legislatore europeo ha cioè ritenuto che, quando la base giuridica del trattamento risiede nella esecuzione di

[15] L'art. 6, par. 1, del GDPR prevede sei condizioni che legittimano il trattamento dei dati personali, vale a dire: *a)* se l'interessato ha espresso il suo consenso; *b)* se il trattamento è necessario alla esecuzione di un contratto di cui l'interessato è parte; *c)* se il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento; *d)* se il trattamento è necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica; *e)* se il trattamento è 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; *f)* se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (per es., come chiarito dal Considerando n. 47, per finalità di prevenzione delle frodi o per finalità di marketing diretto). Cfr. la Relazione tecnica al disegno di legge di conversione del d.l. 8/10/2021, n. 139, ove si evidenzia, con riferimento all'art. 9 del decreto-legge che «l'intervento normativo mira ad allineare le previsioni del codice in materia di protezione di dati personali, di cui al d.lgs. 30/6/2003, n. 196 (…) al rispetto delle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27/4/2016 (…), nell'ottica di semplificare il quadro e valorizzare le attività e i compiti di interesse pubblico svolti dalle pubbliche amministrazioni o dalle società a controllo pubblico statale per finalità di pubblico interesse, oltreché nell'adozione e attuazione delle misure e riforme previste dal PNRR».

un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, una esplicitazione in sede legislativa della finalità del trattamento non sia necessaria: ciò pare confermato anche dai Considerando nn. 41 e 45 del Regolamento[16], oltre che da una lettura sistematica del medesimo art. 6 GDPR e, in particolare, da un confronto tra l'art. 6, par. 1, lett. *e* – ove la valutazione del trattamento come necessario e inevitabile è rimessa alla discrezionalità della pubblica amministrazione[17] – e l'art. 6, par. 1, lett. *c*, che viceversa autorizza il trattamento dei dati quando il titolare deve adempiere a un obbligo legale, nel qual caso è appunto la legge a valutare *ex ante* se un determinato trattamento sia necessario e inevitabile[18].

Insomma, la nuova previsione segna senza dubbio un cambio di passo rispetto al passato, nel senso che sembra attribuire maggiore fiducia alle pubbliche amministrazioni, sul presupposto che le stesse già agiscano istituzionalmente nel perseguimento di finalità di pubblico interesse dettate dalla legge e che, comunque, debbano sempre esercitare la loro discrezionalità nell'osservanza dei principi dell'azione amministrativa, *in primis* del principio di proporzionalità (il quale implica che, in presenza di più alternative per raggiungere il medesimo obiettivo, sia scelta quella meno invasiva). E ciò, si noti, sin da quando sono chiamate a valutare la stessa «necessità» del trattamento dei dati personali per l'esercizio di pubblici poteri o per lo svolgimento di un dato compito di interesse pubblico.

[16] I quali precisano, rispettivamente, che il riferimento a una base giuridica o a una misura legislativa per il trattamento di dati personali non deve essere inteso come riferito a un atto legislativo in senso proprio, purché si tratti di una «base giuridica» chiara, precisa e prevedibile da parte degli interessati, e che non occorre un atto legislativo specifico per ogni trattamento.

[17] Stesso discorso potrebbe essere fatto per l'art. 6, par. 1, lett. *f*, del GDPR, che fa riferimento al trattamento necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

[18] Non a caso, solo nelle ipotesi di cui all'art. 6, par. 1, lett. *e* ed *f*, l'art. 21 GDPR prevede la possibilità per l'interessato di opporsi «in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano».

In linea con tale impostazione, la nuova previsione riscrive anche i successivi commi 2 e 3 del medesimo articolo 2-*ter* del Codice in materia di protezione dei dati personali legittimando i soggetti pubblici a scambiarsi i dati, a comunicarli a terzi e a diffonderli a soggetti indeterminati quando ciò sia necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Viene abrogata pure la previsione che sottoponeva la comunicazione dei dati personali alla previa autorizzazione (eventualmente nella forma del silenzio-assenso) del Garante[19]. Sicché, di nuovo, la scelta è di lasciare alle pubbliche amministrazioni la valutazione e la ponderazione dei diversi interessi che vengono in gioco, incluso – si noti – il principio di trasparenza dell'azione amministrativa che, come si è accennato, deve essere sempre bilanciato con il diritto alla privacy.

A prescindere dalle ragioni immediate che possono avere indotto il legislatore a una scelta di questo tipo[20], e al netto di alcuni affinamenti forse necessari (per esempio per ripristinare un qualche ruolo del Garante), ciò che interessa qui evidenziare è che la novella legislativa appare connotata da quello stesso spirito di fondo che ha animato alcune previsioni chiave dei decreti di attuazione del PNRR: si pensi, per es., alla previsione del d.l. Semplificazioni (d.l. 16/7/2020,

[19] L'art. 3-*bis*, comma 2, secondo periodo, prevedeva infatti che la comunicazione fra titolari che effettuano trattamenti di dati personali fosse ammessa quando «comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione nelle misure da adottarsi a garanzia degli interessati».

[20] L'intervento legislativo in esame è stato criticato sull'assunto che costituirebbe una reazione affrettata ad alcuni episodi verificatisi durante il periodo pandemico, in cui una male intesa concezione della privacy ha finito talora per mettere a repentaglio l'efficienza e l'efficacia dell'azione amministrativa: si è parlato molto della sanzione comminata dal Garante dei dati personali all'INPS per avere quest'ultimo male esercitato (in violazione della disciplina sulla privacy) la funzione di controllo e vigilanza sull'erogazione del bonus COVID-19 a sostegno delle categorie di lavoratori e professionisti colpite dalle misure del *lockdown*: cfr. il provvedimento sanzionatorio del Garante n. 87 del 25/2/2021.

n. 76, convertito, con modificazioni, dalla l. 11/9/2020, n. 120) che ha limitato la responsabilità amministrativa dei dipendenti pubblici solo ai casi di dolo (con esclusione dunque della colpa grave)[21], il cui ambito di applicazione è stato poi esteso dal d.l. Semplificazioni-*bis* (d.l. 31/5/2021, n. 77, convertito, con modificazioni, dalla l. 29/7/2021, n. 108) fino al 2023[22]; oppure alla previsione, sempre contenuta nel d.l. Semplificazioni-*bis*, che ha eliminato i limiti al subappalto attribuendo alle stazioni appaltanti il compito di definire nella *lex specialis* la percentuale di lavori non subappaltabili[23].

In tutti questi casi, ciò che emerge è una rinnovata fiducia (o forse una scommessa) nel ruolo delle pubbliche amministrazioni e la consapevolezza della necessità – ove si vogliano cogliere le sfide e le opportunità del PNRR – di rivedere la tendenza a limitarne la discrezionalità, vista come fonte di abusi e di *maladministration* (tendenza che però, in ultima analisi, tradiva una sfiducia di fondo circa le capacità dell'amministrazione di operare bene)[24].

Volendo guardare allo stesso fenomeno da un altro punto di vista, la novella corregge la tendenza degli ultimi anni a intendere le norme sulla privacy in senso particolarmente limitativo quando ad essere in gioco è l'azione amministrativa: il che, a ben vedere, costituiva un non senso a fronte della possibilità viceversa consentita a soggetti privati e imprese di trattare ampiamente (e legittimamente) i dati personali dietro gli schermi del consenso (spesso prestato secondo formule standardizzate neppure lette dall'interessato) o della necessità contrattuale.

Si tratta di un primo passo certamente apprezzabile nell'attuale momento storico in cui, dopo che tanti risultati sono stati raggiunti sul piano delle garanzie del cittadino nei

[21] Si tratta dell'art. 21 del d.l. 76/2020 che prevedeva tale limitazione fino al 31/12/2021.

[22] Cfr. l'art. 51 del d.l. 77/2021.

[23] Cfr. l'art. 49, comma 2, lett. *a* del d.l. 77/2021.

[24] Su questo tema, da ultimo, F. Cintioli, *Risultato amministrativo, discrezionalità e PNRR: una proposta per il giudice*, in «La Magistratura, Rivista a cura dell'Associazione nazionale magistrati», 13/11/2021.

confronti dell'azione amministrativa, è venuto il momento – pur senza abbassare la guardia rispetto ai pubblici poteri – di volgere lo sguardo ad altri poteri, vale a dire quelli privati, rispetto ai quali un analogo sistema di garanzie è, come è noto, ancora tutto da costruire.

3. *L'impatto della tecnologia: l'interoperabilità delle banche dati tra efficienza delle pubbliche amministrazioni e tutela dei dati personali. Il ruolo della «blockchain»*

La transizione digitale che ha riguardato e riguarda l'azione amministrativa, semplificando le comunicazioni, nonché la raccolta, la catalogazione e l'elaborazione dei dati[25], è essenziale per promuovere un'amministrazione efficiente e «vicina» ai cittadini. L'ampio ricorso a strumenti informatici e telematici snellisce l'azione amministrativa e favorisce la cooperazione tra soggetti pubblici, al contempo riducendo la distanza tra amministrazioni e cittadini, semplificandone i rapporti e promuovendo una maggiore partecipazione dei secondi ai processi decisionali[26].

Già con il d.lgs. 12/2/1993, n. 39[27], recante «Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche», sono state poste le basi per la

[25] Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, cit.

[26] Emblematica in tal senso la delega contenuta nella l. 7/8/2015, n. 124, all'art. 1 sulla Carta della cittadinanza digitale, con lo scopo di «garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici»: cfr. V. Cerulli Irelli, *La tecnificazione*, in L. Ferrara e D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana*, IV: *La tecnificazione*, a cura di S. Civitarese Matteucci e L. Torchia, Firenze, 2016, p. 279.

[27] Il d.lgs. 39/1993 costituisce il primo atto normativo organico in materia, tuttavia, specifiche previsioni erano già contenute in precedenti disposizioni normative: si pensi, ad esempio, all'art. 2 del d.lgs. 3/2/1993, n. 29, confluito nell'art. 2 del d.lgs. 30/3/2001, n. 165, ai sensi del quale le amministrazioni devono favorire il collegamento delle attività degli

«costruzione» di un'informatica pubblica[28], favorita altresì dall'introduzione di disposizioni volte a disciplinare l'atto amministrativo informatico[29] che sono state raccolte nel d.lgs. 7/3/2005, n. 82, Codice dell'amministrazione digitale[30]. Al codice e alle diverse disposizioni settoriali che si riferiscono all'uso della telematica si affianca, in via generale, la previsione dell'art. 3-*bis*, l. 241/90, come modificata nel 2020, secondo la quale «per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati».

L'intento del legislatore è chiaro: favorire un efficace scambio informativo tra pubbliche amministrazioni e tra queste ultime e i privati per un'effettiva collaborazione[31]. In questo senso, le banche dati, con la loro capacità di gestire e organizzare una ingente mole di dati e di renderli facilmente accessibili, consentendo una consultazione immediata e da remoto, costituiscono uno strumento irrinunciabile per favorire la cooperazione tra amministrazioni, oltre che l'«alleggerimento» degli adempimenti burocratici gravanti sui privati, in applicazione del principio dell'*once only*[32].

uffici, adeguandosi al dovere di comunicazione interna ed esterna, e l'interconnessione mediante sistemi informatici e statistici pubblici.

[28] M. Bombardelli, *Informatica pubblica, e-government e sviluppo sostenibile*, in «Rivista italiana di Diritto pubblico comunitario», 2002, n. 5, p. 991.

[29] Sulla questione dei vizi formali dell'atto e, in particolare, sul problema della sottoscrizione, cfr. A.G. Orofino, *L'esternazione informatica degli atti amministrativi*, in Civitarese Matteucci e Torchia (a cura di), *La tecnificazione*, cit., p. 181.

[30] Si vedano, da ultimo, le misure volte a favorire l'avanzamento dell'amministrazione digitale, specialmente a seguito dell'emergenza sanitaria determinata dalla diffusione del COVID-19, introdotte nel Codice dell'amministrazione digitale dal d.l. 16/7/2020, n. 76 («decreto Semplificazioni»), convertito, con modificazioni, dalla l. 11/9/2020, n. 120, e dal d.l. 31/5/2021 («decreto Semplificazioni-*bis*»), convertito, con modificazioni, dalla l. 29/7/2021, n. 108.

[31] Anche in attuazione del principio di collaborazione sancito ormai espressamente dalla l. 241/90 all'art. 1, comma 2-*bis*.

[32] Sulla promozione del principio anche a livello europeo, per favorire la cooperazione tra Stati membri e istituzioni dell'Unione, cfr. A.

La più ampia interoperabilità tra le banche dati utilizzate dai diversi enti pubblici dovrebbe essere un obiettivo da perseguire con forza per assicurare uno scambio di informazioni rapido ed efficace[33]. Fermo restando che il trasferimento dei dati dovrebbe essere sempre strettamente funzionale all'esercizio dei «compiti» di interesse pubblico di competenza dell'amministrazione che vi accede[34].

Tuttavia, il risvolto negativo della maggiore facilità e rapidità dello scambio informativo che la tecnologia assicura consiste nella difficoltà di controllare la diffusione di tali dati e nella conseguente necessità di predisporre misure di contrasto di possibili accessi illeciti: si pensi, di recente, all'attacco hacker al portale della Regione Lazio del luglio 2021. Del resto, il rischio di tentativi di acquisizione illecita è quanto mai attuale: i dati personali rappresentano ormai delle vere e proprie risorse, dei «beni di scambio» per le loro potenzialità soprattutto commerciali[35].

D'altro canto, come subito si vedrà, le soluzioni tecnologiche pensate per superare il problema del *data breach* pongono a loro volta problemi nuovi a fronte dei quali le pubbliche amministrazioni sono chiamate a ripensare non solo le modalità di conservazione e di gestione dei dati, ma

Monica, *Lo sportello digitale unico: uno strumento che può unire cittadini e amministrazioni europee*, in «Rivista italiana di Diritto pubblico comunitario», 2019, n. 3, p. 477.

[33] A. Sandulli, *Lo «stato digitale» pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in «Rivista trimestrale di Diritto pubblico», 2021, n. 2, p. 513.

[34] Cfr. il già richiamato art. 2-*ter* del Codice in materia di protezione dei dati personali. Sul punto, cfr. G. Carullo, *Big data e pubblica amministrazione nell'era delle banche dati interconnesse*, in «Concorrenza e mercato», 2016, n. 1, p. 181.

[35] Sul cd. nuovo petrolio, cfr. E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in «Diritto pubblico», 2019, n. 2, p. 363; S. Tommasi, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in «Revista de Direito Brasileira», 2020, n. 10. Sulle possibili forme di tutela che muovono dalla «patrimonializzazione» dei dati, F. Midiri, *Proteggere i dati personali con le tutele del consumatore*, in «Giornale di diritto amministrativo», 2021, n. 5, p. 609.

addirittura il loro stesso ruolo rispetto alla conservazione e alla gestione dei dati.

Non è un segreto che l'avvento della tecnologia dei registri distribuiti, la quale consente la conservazione dei dati non più in modo centralizzato, su un solo server, ma su una pluralità di computer (cd. «nodi») che fanno parte di una rete e sono tutti tra loro sincronizzati in tempo reale (nel senso che ogni volta che viene inserito un nuovo dato in uno dei computer, tutte le altre copie del registro si aggiornano in tempo reale) è destinata a incidere profondamente sulla modalità di tenuta e di gestione dei dati, compresi quelli personali, da parte di soggetti pubblici e privati.

Senza potersi qui soffermare sui dettagli della tecnologia[36], è sufficiente ricordare che su un registro distribuito i dati sono cronologicamente aggregati in blocchi (da cui il nome *blockchain*), i quali sono collegati l'uno all'altro attraverso un sistema di cd. *hashing* (cioè, i dati di ogni blocco vengono trasformati in una stringa di caratteri alfanumerici di lunghezza fissa, pari a un *hash* e ogni *hash* è associato a uno specifico blocco), che fa sì che una modifica anche minima del contenuto dei dati di un blocco produca un *hash* completamente diverso. In specie, per formare la «catena di blocchi», l'*hash* di ogni blocco viene firmato crittograficamente e collegato all'*hash* del blocco precedente, sullo stesso è apposta una marca temporale e viene reso pubblico (attraverso la pubblicazione dell'*hash* e della marca temporale).

Il risultato è un database trasparente, condiviso e resistente alla manomissione, con diversi livelli di visibilità dei dati in esso contenuti (l'intestazione del blocco è di solito visibile da tutti, mentre il contenuto del blocco può essere criptato).

[36] Per una compiuta analisi della tecnologia *blockchain* e per la sua applicazione ai processi decisionali pubblici, specie in materia ambientale, si veda, se si vuole, M. Allena, *Blockchain Technology for Environmental Compliance: Towards a Choral Approach*, in «Environmental Law Review», 50, 2020, n. 4, pp. 1055 ss. Cfr. inoltre, almeno, M.F. Monterossi, *Blockchain (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Agg., Torino, 2021, pp. 29 ss.

Soprattutto, in tale database a essere distribuita non è solo la conservazione dei dati, ma anche il loro inserimento: la validazione dei dati – necessaria per il loro inserimento nella catena dei blocchi – è affidata a un meccanismo di consenso (il cd. *consensus protocol* che indica l'insieme delle regole che consentono ai vari nodi di raggiungere un accordo su quali blocchi aggiungere alla catena) distribuito tra i vari nodi della rete[37].

In genere, quando si parla di registri distribuiti e pubblica amministrazione vengono in rilievo le cd. *permissioned blockchain* (contrapposte alle *permissionless blockchain*) ove il registro è condiviso più che distribuito (si parla di *narrowly distributed platforms*), perché solo alcuni ben identificati partecipanti alla rete (per es., altre amministrazioni, ma anche associazioni non governative o rappresentative di vari gruppi di interessi) validano i dati e conservano l'intero database. Gli altri (i comuni cittadini) hanno accesso al database nel senso che visualizzano i dati e ne possono chiedere l'inserimento, ma non partecipano alla costruzione vera e propria del registro.

Ciò non toglie che la verifica sulla completezza, tempestività e regolarità formale dei dati sia effettuata non più solo, come è sino ad oggi avvenuto, da parte della pubblica amministrazione detentrice di tali dati ma, appunto, in modo diffuso: ciò può aiutare a ridurre i costi di verifica della correttezza formale dei dati e accrescere la fiducia nella autenticità degli stessi. D'altro canto, tale sistema può avere conseguenze importanti in termini di (maggiore) circolazione delle informazioni (che non sono più ospitate su un unico server), di abbattimento dei costi della burocrazia, di riduzione dell'intermediazione, di diffusione dei controlli, di possibilità di produrre certezze (dunque, di incidere sulla

[37] In genere, i dati sono validati dai cd. *miners*, rappresentati da alcuni nodi della rete i quali o prestano il potere computazionale delle proprie macchine per svolgere i calcoli necessari per risolvere un problema crittografico necessario per aggiungere un blocco di informazioni alla catena (cd. *proof of work*), o sono scelti come validatori dei dati sulla base di altri criteri, per es. la quantità di criptovaluta che ciascuno di essi detiene e il tempo per il quale la ha posseduta (cd. *proof of stake*).

funzione di certificazione pubblica) in modo diffuso, per citarne solo alcune.

Per quel che in questa sede maggiormente interessa, tale tecnologia pare idonea a incidere profondamente sul ruolo dei soggetti pubblici nella gestione dei dati: tale ruolo viene ridisegnato in un'ottica multipolare (il che previene rischi di «cattura» del regolatore) e di contitolarità – almeno entro certi limiti – della funzione pubblica. Tanto è vero che non si è mancato di notare come essa sia idonea a porre in crisi il sistema di regolazione dei dati di cui al GDPR (fondato ancora sul presupposto che, per es., vi sia un unico soggetto responsabile del trattamento al quale gli interessati possono rivolgersi per far valere i propri diritti alla riservatezza, o sull'idea che sia sempre possibile ottenere la cancellazione dei dati quando ciò sia richiesto dalla legge)[38].

4. *Intelligenza artificiale e decisioni amministrative*

Questione diversa, ma altrettanto rilevante, sempre strettamente correlata alla transizione digitale in atto nella pubblica amministrazione, riguarda la necessità di garantire la protezione dei dati personali in termini di corretto uso degli stessi. Il riferimento va, in particolare, ai rischi di effetti discriminatori che sono stati registrati a seguito dell'utilizzo, nell'esercizio di funzioni pubbliche, di alcuni algoritmi, specialmente di tipo predittivo, espressione di quella che comunemente viene definita «intelligenza artificiale» e che nei «dati» trova la propria linfa.

L'esercizio dell'azione amministrativa presuppone inevitabilmente il ricorso alla tecnologia, quantomeno ove la si intenda meramente in funzione servente o strumentale all'attività umana, escludendone una portata sostitutiva[39]. Sennonché, il

[38] Per tutti, cfr. M. Finck, *Blockchains and the General Data Protection Regulation*, in «European Data Protection Law Review», 2018, n. 4, pp. 17 ss.

[39] D.U. Galetta e J.G. Corvalán, *Intelligenza artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica*

ricorso a sistemi automatizzati basati su formule algoritmiche, in grado di adottare decisioni «al posto» del funzionario persona fisica[40], si fa sempre più esteso, per i vantaggi che parrebbe avere in termini di rapidità ed efficienza[41], data la capacità dello strumento informatico di acquisire, catalogare ed elaborare una vastità e complessità di dati in maniera estremamente più rapida di qualsiasi persona fisica. A ciò si aggiunga che, sebbene la scelta dei dati inseriti e dei criteri utilizzati dall'algoritmo non sia neutrale, dovrebbe esserlo il suo funzionamento, per definizione «impersonale» e idoneo a eliminare il rischio di errori umani[42].

Le considerazioni da svolgere, tuttavia, sono più complesse, specialmente ove si introduca la distinzione tra algoritmi deduttivi e algoritmi predittivi[43]. Questi ultimi, riconduci-

in atto, in «Federalismi.it», 2019, n. 3, individuano tre distinti livelli: *a*) Primo livello. Automazione completa; *b*) Secondo livello. Automazione e intervento umano ridotto; *c*) Terzo livello. Automazione più predizione.

[40] Sugli atti amministrativi automatizzati, senza pretesa di esaustività, cfr. G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intelligibilità*, Napoli, 2019; A. Masucci, *L'atto amministrativo informatico*, Napoli, 1993; Id., *Atto amministrativo informatico* (voce), in *Enciclopedia del Diritto*, Aggiornamento, I, Milano, 1997, p. 221; G. Duni, *Amministrazione digitale* (voce), in *Enciclopedia del Diritto*, Annali, I, Milano, 2007, p. 13; Id., *L'amministrazione digitale. Il diritto amministrativo nella evoluzione telematica*, Milano, 2008; A. Usai, *Le elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche*, in G. Duni (a cura di), *Dall'informatica amministrativa alla teleamministrazione*, Roma, 1992, p. 55; Id., *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in «Diritto dell'informazione e dell'informatica», 1993, n. 1, p. 163; U. Fantigrossi, *Automazione e pubblica amministrazione*, Bologna, 1993; D. Marongiu, *L'attività amministrativa automatizzata*, Bologna, 2005; A.G. Orofino e R.G. Orofino, *L'automazione amministrativa: imputazione e responsabilità*, in «Giornale di diritto amministrativo», 2005, n. 12, p. 1300.

[41] Questione diversa da quella trattata è rappresentata dall'influenza indiretta degli algoritmi sui processi decisionali, affrontata da V. Molaschi, *Algoritmi e nuove schiavitù*, in «Federalismi.it», 2021, n. 18.

[42] M.C. Cavallaro e G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in «Federalismi.it», 2019, n. 16.

[43] F. Costantino, *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in «Diritto amministrativo», 2017, n. 4, p. 799; Id.,

bili alla nozione di intelligenza artificiale, si basano su una tecnologia di *machine* (o *deep*) *learning* che consente alla «macchina» di acquisire ed elaborare dati ulteriori rispetto a quelli selezionati *ex ante* e inseriti nella formula algoritmica. In altri termini, l'algoritmo predittivo è in grado di sviluppare decisioni basate su informazioni ulteriori, acquisite direttamente dal software. Di conseguenza, le decisioni assunte non sarebbero prevedibili come sono (o, almeno, dovrebbero essere) quelle adottate tramite algoritmi deduttivi che si limitano ad elaborare i dati negli stessi inseriti.

In disparte l'eventualità che anche l'algoritmo deduttivo conduca a risultati incomprensibili – emblematico, a tal proposito, il noto caso del Piano straordinario «Buona scuola»[44] –, è evidente che gli algoritmi basati su meccani-

Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data, in «Diritto pubblico», 2019, n. 1, p. 43.

[44] La procedura di mobilità nazionale di cui alla l. 31/7/2015, n. 107, commi da 95 a 104 (cd. Buona scuola), per la copertura dei posti di potenziamento, sostegno e comuni degli istituti scolastici statali di ogni ordine e grado per l'anno scolastico 2015/2016, prevedeva, ai sensi del comma 98, un'assunzione graduale dei docenti articolata in tre distinte fasi, in modo da garantire ai docenti che non fossero stati assunti nella fase A (ossia entro il 15/9/2015, secondo le procedure ordinarie di cui all'art. 399 del d.lgs. 16/4/1994, n. 297, «TU Istruzione»), di essere assunti nelle successive fasi B e C, sempre in maniera graduale, in base alla posizione detenuta in graduatoria, tenendo conto dell'ordine di preferenza espresso tra posti di sostegno e posti comuni e tra tutte le province a livello nazionale. Sennonché, nell'ambito della fase B, nonostante la preferenza espressa, alcuni docenti sono stati assegnati in province e classe di concorso diverse da quelle indicate, mentre, nella successiva fase C, i docenti, collocati in graduatoria in posizione deteriore, sono stati assegnati nelle province oggetto di preferenza e per la classe di concorso prescelta. Sul contenzioso che ne è derivato, sia consentito rinviare a S. Vernile, *Verso la decisione amministrativa algoritmica?*, in «MediaLaws - Rivista di diritto dei media», 2020, n. 2, p. 136. Cfr. anche R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in «Diritto amministrativo», 2019, n. 4, p. 773; G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica*, in «MediaLaws - Rivista di diritto dei media», 2019, n. 3, p. 234; N. Muciaccia, *Algoritmi e procedimento decisionale: alcuni recenti arresti della giustizia amministrativa*, in «Federalismi.it», 2020, n. 10; L. Musselli, *La decisione amministrativa nell'età degli algoritmi: primi spunti*, in «MediaLaws - Rivista di diritto dei

smi di *machine learning*, ancorché più avanzati e, dunque, potenzialmente più «utili», presentano non poche criticità[45], in massima parte dovute all'imprevedibilità della decisione e alla opacità del processo decisionale[46], per la difficoltà di ricostruirne l'iter logico e, dunque, di motivare la decisione finale[47].

Il Consiglio di Stato, sez. VI, con sentenza 8/4/2019, n. 2270, ha chiarito, infatti, che l'utilizzo degli strumenti informatici e, in particolare, degli algoritmi in sede decisionale, è ammesso a condizione che siano rispettati tutti i principi che regolano l'azione amministrativa, con riguardo in particolare a quello di trasparenza, in base al quale l'algoritmo utilizzato deve essere «conoscibile» o, meglio, comprensibile, sicché si devono indicare puntualmente i parametri applicati e le modalità di funzionamento.

Analogamente, con la successiva pronuncia del 13/12/2019, n. 8472, il Supremo Consesso amministrativo, pure riconoscendo l'importanza della rivoluzione digitale per ragioni di efficienza e neutralità, almeno con riguardo alle procedure seriali e standardizzate, «implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale», ha ribadito che il ricorso a una «procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata[o], ma anzi, in linea di massima, incoraggiata[o]», a condizione, però, che

media», 2020, n. 1, p. 18; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in «Diritto pubblico», 2019, n. 1, p. 5; Cavallaro e Smorto, *Decisione pubblica e responsabilità*, cit.; M. Timo, *Algoritmo e potere amministrativo*, in «Il Diritto dell'economia», 2020, n. 1, p. 753.

[45] Vantaggi e rischi dell'intelligenza artificiale sono stati messi in luce dalla Commissione europea con la pubblicazione, in data 19/2/2020, del *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*.

[46] G. Lo Sapio, *La «black box»: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in «Federalismi.it», 2021, n. 16.

[47] F. de Leonardis, *Big data, decisioni amministrative e «povertà» di risorse della pubblica amministrazione*, in E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, p. 137.

la formula algoritmica applicata sia pienamente trasparente e conoscibile. Tanto che, secondo i giudici di Palazzo Spada, non potrebbero ostacolare la conoscibilità dell'algoritmo le eventuali ragioni di riservatezza invocate delle imprese produttrici, poiché queste «ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza».

Ancora, il Consiglio di Stato ha affermato che si ricava dal GDPR un principio di non esclusività della decisione algoritmica, in base al quale «deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica»[48]. Occorre, dunque, sempre, un controllo «umano» a valle della decisione. Controllo che, come confermato dal Consiglio di Stato, con la citata sentenza n. 8472/2019, deve essere effettuato in primo luogo dall'organo competente all'adozione del provvedimento che resta responsabile, per legge, degli effetti del provvedimento. D'altronde, non può non riconoscersi a chi potrebbe essere chiamato a rispondere degli effetti della decisione la possibilità di discostarsene o, analogamente, di accettarla[49], quand'anche basata su un meccanismo di *machine learning*[50].

[48] Ai sensi dell'art. 22 del GDPR, «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona». Cfr. S. Sassi, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in «Analisi giuridica dell'economia», 2019, n. 1, p. 109.

[49] Sulla difficoltà del controllo, anche in virtù dell'«autorevolezza» della decisione concepita dall'elaboratore informatico, cfr. A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in «BioLaw Journal - Rivista di BioDiritto», 2019, n. 1, p. 63; P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, in «Federalismi.it», 2018, n. 2; Molaschi, *Algoritmi e nuove schiavitù*, cit.

[50] A. Masucci, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Torino, 2011, p. 97, per il quale «l'elaboratore è solo un mezzo a disposizione dell'amministrazione per attuare gli obiettivi definiti dall'amministrazione, dal momento che gli elaboratori elettronici producono la decisione sulla

5. *La protezione dei dati personali nell'«amministrazione algoritmica»*

Il caso «Buona scuola», cui si è accennato nel precedente paragrafo, ha generato grande scalpore per i risultati paradossali cui è giunto l'algoritmo, seppure di tipo deduttivo (avrebbe dovuto individuare la sede di servizio cui assegnare i singoli docenti tenendo conto dei seguenti criteri di priorità: la posizione detenuta in graduatoria, la provincia oggetto di preferenza e per ciascuna provincia la tipologia di posto)[51]. La «discriminazione» lamentata dai docenti insorti avverso i provvedimenti di assegnazione, invero, è parsa piuttosto la conseguenza di una sorta di «malfunzionamento» dell'algoritmo, o comunque di una non corretta «traduzione» della regola giuridica in linguaggio tecnico, che ben avrebbe potuto essere oggetto di verifica e «soluzione» ove vi fosse stato un controllo successivo, nel rispetto del richiamato principio di non esclusività della decisione algoritmica.

Una vera e propria fattispecie di discriminazione, invece, è stata registrata in alcuni casi in cui il processo decisionale devoluto all'algoritmo era basato sulla profilazione dei soggetti interessati[52], definita dal GDPR, all'art. 4, par. 4, come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità,

base di un programma definito (o fatto proprio) dall'amministrazione competente per l'adozione dell'atto».

[51] In particolare, ai sensi dell'art. 1, comma 101, l. 13/7/2015, n. 107, «per ciascuna iscrizione in graduatoria, e secondo l'ordine di cui al comma 100, la provincia e la tipologia di posto su cui ciascun soggetto è assunto sono determinate scorrendo, nell'ordine, le province secondo le preferenze indicate e, per ciascuna provincia, la tipologia di posto secondo la preferenza indicata».

[52] Il tema, infatti, è più puntuale se è vero, come ci ricorda Molaschi, *Algoritmi e nuove schiavitù*, cit., che non tutti i processi decisionali algoritmi comportano profilazione e, al contempo, la profilazione non implica necessariamente un processo algoritmico.

il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Tra le più emblematiche vi è la vicenda statunitense nota come Compas, concernente un sistema algoritmico per la valutazione del rischio di recidiva, basato sui dati dei precedenti giudiziari e dei questionari compilati dai pregiudicati, alcuni dati statistici ed elementi ulteriori non resi noti in quanto considerati rientranti nella proprietà intellettuale della società privata sviluppatrice del software[53]. Sennonché, la valutazione offerta dall'algoritmo collocava tra i soggetti ad alto rischio i pregiudicati appartenenti a minoranze di colore in misura sproporzionatamente superiore rispetto ai pregiudicati bianchi.

I dati e soprattutto le modalità di inserimento, evidentemente, erano già in parte discriminatori, sicché la decisione adottata dall'algoritmo non ha potuto che riflettere la «qualità» dei dati utilizzati, secondo il principio noto come GIGO (*garbage in, garbage out*)[54].

Il dovere di protezione dei dati personali si traduce, allora, in primo luogo, in un onere di particolare accortezza nella individuazione e introduzione dei dati che saranno elaborati dal decisore informatico, con un'«anticipazione» della tutela della privacy (che da successiva diviene preventiva), già in sede di progettazione[55]. In linea con gli ormai diffusissimi concetti di *privacy by design*, che implica il ricorso a misure tecniche e organizzative idonee a garantire la protezione dei dati sia al momento della scelta dei mezzi da utilizzare sia al momento del trattamento, e di *privacy by default*, espressione con cui si fa riferimento alla necessità che, per impostazione predefinita, siano oggetto del trattamento esclusivamente i dati effettivamente necessari per la specifica finalità di volta in volta perseguita.

[53] Su questo e altri casi di algoritmi discriminatori, G. Giorgini Pignatiello, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle «Digital Authorities»?*, in «Federalismi.it», 2021, n. 16; Molaschi, *Algoritmi e nuove schiavitù*, cit.

[54] Simoncini, *L'algoritmo incostituzionale*, cit.

[55] L. Aulino, *Consenso al trattamento dei dati e carenza di consapevolezza: il «legal design» come un rimedio «ex ante»*, in «Diritto dell'informazione e dell'informatica», 2020, n. 2, p. 303.

D'altronde, il concetto di protezione dei dati ben ricomprende la necessità di garantirne un utilizzo corretto e, quindi, certamente non discriminatorio, come chiarito dall'art. 5 GDPR, par. 1, lett. *a*, dove si legge che i dati personali devono essere trattati in modo corretto, oltre che lecito e trasparente, nonché in maniera più chiara, ma meno vincolante, dal Considerando n. 71 del medesimo Regolamento[56], ai sensi del quale, tra l'altro, è opportuno «che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori» e che il titolare del trattamento «impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello *status* genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

In secondo luogo, ancora una volta, non si può rinunciare a un controllo a valle della decisione algoritmica, anche al fine di verificare e correggere gli eventuali inammissibili effetti discriminatori, in applicazione del principio di non esclusività della decisione algoritmica, l'unico conciliabile, come già emerso nel paragrafo precedente, almeno *de iure condito*[57], con le regole in materia di responsabilità.

[56] Così Simoncini, *L'algoritmo incostituzionale*, cit.; Giorgini Pignatiello, *Il contrasto alle discriminazioni algoritmiche*, cit.; Molaschi, *Algoritmi e nuove schiavitù*, cit.

[57] Non può non richiamarsi almeno la proposta, a livello europeo, di un Regolamento in materia di intelligenza artificiale: Commissione europea, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, 21/4/2021.