DECISIONI ALGORITMICHE E TUTELA DEI DATI PERSONALI. RIFLESSIONI INTORNO AL RUOLO DEL GARANTE*

VALENTINA PAGNANELLI**

Sommario

Abstract

Moving from the results of a research on the provisions of the Italian Data Protection Authority regarding
algorithmic decisions, the paper offers some reflections on the constitutional role of the DPA in the governance of the digital society, characterized by Big Data and the development of Artificial Intelligence techniques. In the conclusions, the contribution questions the relations of the DPA with other European and national Authorities intended to regulate Artificial Intelligence and cyber security.

Suggerimento di citazione

V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante,* in *Osservatorio sulle fonti,* n. 2/2021. Disponibile in: http://www.osservatoriosullefonti.it

* Il contributo costituisce la rielaborazione della relazione tenuta al *webinar* "Autorità amministrative indipendenti e regolazione delle decisioni algoritmiche" svoltosi il 7 maggio 2021 e organizzato dal Dipartimento di Scienze Giuridiche dell'Università di Firenze, nell'ambito del Progetto PRIN 2017 *Self- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law* (SE.CO.R.E TECH).

** Dottoranda in Diritto pubblico nell'Università degli Studi di Firenze.
Contatto: valentina.pagnanelli@unifi.it

Registrazione presso il Tribunale di Firenze n. 5626 del 24 dicembre 2007
Rivista inclusa nella classe A delle Riviste scientifiche di Area 12 – Direttore Prof. Paolo Caretti
ISSN 2038-5633

Premessa. Un'indagine a partire dalla prassi

Questo contributo reca i risultati di un'indagine sull'attività di regolazione del Garante per la protezione dei dati personali in materia di decisioni algoritmiche. I documenti qui richiamati rappresentano solo un esiguo campione rispetto alla vastissima produzione dell'Autorità, che percorrendo i decenni ha spaziato tra le innumerevoli declinazioni pratiche dei trattamenti automatizzati di dati personali.

Prima di procedere all'esposizione dei risultati della ricerca è necessario fare una premessa *terminologica:* poiché i trattamenti automatizzati di dati personali sono connotati da una rilevantissima componente tecnologica, soggetta a sviluppi costanti e rapidissimi, gli attori pubblici e privati coinvolti nel contraddittorio con il Garante hanno utilizzato ed utilizzano, nel riferirsi a singole fattispecie, un lessico vario e variabile.

L'indagine svolta ha tenuto conto di questa complessità tecnologica e, a volte, terminologica[1]. Di conseguenza l'individuazione dei provvedimenti rilevanti per la ricerca è avvenuta compiendo di volta in volta un raffronto tra le modalità descrittive dei singoli trattamenti esaminati e lo schema di analisi che si può dedurre dalla normativa rilevante e dal fondamentale contributo interpretativo ed integrativo che ci è fornito dalle Linee guida del Gruppo di lavoro Articolo 29[2].

1. Quali algoritmi? L'oggetto della ricerca

Le decisioni individuali automatizzate erano già regolate nella Direttiva n. 95/46 in materia di protezione dei dati personali[3], nel Codice della privacy italiano[4] e prima ancora nella legge n. 675 del 1996[5], seppure in termini non

[1] Termini quali *algoritmo, decisione algoritmica, decisione automatizzata, profilazione, Intelligenza artificiale, cibernetica et similia* sono talvolta utilizzati in modo intercambiabile, per riferirsi a singoli trattamenti di dati, piuttosto che a software, devices, motori di ricerca, tecnologie di riconoscimento biometrico e così via. Questi termini sono stati inseriti come parole-chiave nel motore di ricerca presente nel sito istituzionale del Garante per la protezione dei dati personali per l'individuazione dei documenti rilevanti ai fini della *survey*.

[2] Sul Gruppo di lavoro Articolo 29 ved. https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_it .

[3] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.*

[4] D. lgs. n. 196 del 30 giugno 2003, *Codice in materia di protezione dei dati personali*.

[5] L'articolo 14 del Codice della privacy, già articolo 17 della legge 675/1996, stabiliva al primo comma: «*Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato*». E' interessante notare come Giovanni Buttarelli, commentando la versione più risalente della norma (l'articolo 17 della legge del 1995, rubricato «*Limiti all'utilizzabilità di dati personali*»), evidenziava come non si dovesse rinunciare ad incrementare l'uso dell'informatica a scopo decisionale: «*La legge richiede più semplicemente, che i trattamenti*

perfettamente sovrapponibili alla disciplina dettata dal Regolamento europeo in materia di protezione dei dati personali[6]. Oggi l'articolo 22 del GDPR reca la disciplina dei trattamenti di dati personali effettuati con l'utilizzo di algoritmi[7], mentre le Linee guida che il Gruppo di lavoro Articolo 29 ha pubblicato nel 2018 (WP 251 rev.01)[8] costituiscono un ottimo ausilio per meglio comprendere le differenze tra le modalità con cui i trattamenti automatizzati di dati possono avvenire, e per valutare quali di questi ricadano appunto nel campo di applicazione del GDPR.

***

L'articolo 22 del GDPR pone un divieto generale all'adozione di decisioni completamente automatizzate che producano effetti giuridici o impattino comunque in modo significativo nella sfera personale degli interessati. Al divieto segue l'enunciazione delle eccezioni che, corredate da misure appropriate per tutelare diritti, libertà e interessi legittimi degli interessati, rendono leciti i trattamenti altrimenti vietati. Si tratta delle ipotesi di conclusione o esecuzione di un contratto, consenso esplicito dell'interessato e di trattamenti previsti dal diritto dell'Unione o dello Stato membro.

Le fattispecie di trattamento delineate dalla norma sono due: il trattamento automatizzato e la profilazione. Nelle citate Linee guida del Gruppo Art. 29 questa distinzione è illustrata molto chiaramente: *"Il processo decisionale automatizzato ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare. […] Le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatizzato*

che determinano riflessi diretti sull'identità personale non comportino un'abdicazione in favore delle proprietà cognitive e "decisorie" dell'elaboratore», cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997, 341 ss..

[6] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).*

[7] Tra i commenti all'art. 22 del Regolamento europeo n. 2016/679 si vedano, ex plurimis G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, 219 ss.; L. BOLOGNINI L., E. PELINO, *Codice della disciplina privacy*, Milano, 2019, 181 ss.; G. FINOCCHIARO (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 458 ss..

[8] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679*, consultabili al link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

potrebbe diventare un processo basato sulla profilazione, a seconda delle modalità di utilizzo dei dati[9]".

La profilazione, per essere tale, deve consistere in una forma di trattamento automatizzato di dati personali e deve implicare una valutazione di aspetti personali dell'interessato al fine di analizzarlo o fare previsioni su di esso. Il Gruppo Articolo 29 precisa che una semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza con finalità statistiche e non valutative delle caratteristiche personali dei soggetti coinvolti non costituisce profilazione[10].

Inoltre, la tutela prevista dall'art. 22 riguarda esclusivamente le decisioni automatizzate che abbiano un *impatto grave* sugli individui (quelli che sono definiti *effetti significativi* nella dicitura della Direttiva 95/46), come la cancellazione di un contratto, la perdita di una prestazione sociale o sanitaria, la negazione della cittadinanza piuttosto che l'accesso al credito o all'istruzione[11].

Il divieto posto dal GDPR riguarda quindi i trattamenti che incidono significativamente sulla sfera giuridica dell'interessato. È appena il caso di ricordare che i trattamenti decisionali automatizzati, quando ammessi in base alle eccezioni previste dalla norma, debbano rispettare tutte le regole del Regolamento, *in primis* i principi previsti dall'art. 5 (liceità, trasparenza, minimizzazione, limitazione delle finalità e della conservazione, esattezza[12]).

Di fronte alla produzione alluvionale di provvedimenti che, sotto diversi profili, hanno affrontato l'uso degli algoritmi, al termine del percorso sono stati selezionati documenti da cui emerge l'attenta opera di analisi svolta dal Garante sui singoli trattamenti. Proprio l'accurato esame delle caratteristiche specifiche di ogni fattispecie ha permesso di ricondurre ciascuna di esse entro gli schemi cristallizzati nelle disposizioni normative, anche con notevole approfondimento tecnico e tecnologico oltre che giuridico.

E' bene a tal proposito evidenziare come solo raramente, nel decidere in merito a trattamenti automatizzati di dati personali, l'Autorità si riferisca alle norme specifiche che nell'ordinamento dell'Unione europea e in quello nazionale disciplinano i trattamenti decisionali automatizzati e pongono diritti / divieti; piuttosto, più frequentemente è possibile riscontrare riferimenti ai principi generali della materia[13], agli strumenti di *soft law*, quali le Linee guida e ai

[9] Ibidem, 8.

[10] Ibidem, 7.

[11] Ibidem, 23.

[12] Sui principi fondamentali del trattamento ved. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy, cit.,* 49 ss..

[13] Sul ricorso, nelle decisioni del Garante, ai tradizionali principi elaborati nell'ambito della disciplina sulla protezione dei dati personali, piuttosto che ai singoli diritti e libertà che rileverebbero nel caso concreto cfr. M.S. ESPOSITO, *L'impatto del trattamento sui diritti e le libertà delle persone fisiche: una valutazione alla luce della giurisprudenza delle autorità garanti italiana e spagnola*, in A.

provvedimenti relativi a casi esaminati in precedenza. Come vedremo, i riferimenti all'art. 22 sono rarissimi.

Moltissimi sono i provvedimenti del Garante che riguardano trattamenti automatizzati che hanno effetti significativi sugli interessati: dallo spam mirato descritto nelle Linee guida del 2013 (docweb n. 2542348[14]), alla sanzione comminata all'INPS per la mancanza di informativa e consenso nell'utilizzo del *data mining* per profilare i lavoratori assenti per malattia (docweb n. 9078812 del 29/11/2018[15]), dai ricorsi per la cancellazione / rettifica dei c.d. *snippet* elaborati dagli algoritmi dei motori di ricerca (docweb n. 3736353 del 18/12/2014[16], docweb n. 5890115 del 27/10/2016[17]), all'audizione parlamentare sulle *fake news* in cui il Presidente dell'Autorità Soro, ammonendo sulla distinzione tra libertà di espressione e amplificazione algoritmica promuove un uso della tecnica in funzione di promozione, anziché di limitazione dei diritti (Audizione del 03/03/2020[18]).

Come si vedrà meglio tra poco, i provvedimenti adottati dal Garante in merito a trattamenti effettuati nel settore privato e in ambito pubblico sono difficilmente paragonabili. Vi è da dire che i titolari del trattamento nel settore pubblico molto spesso non godono degli stessi mezzi tecnici, tecnologici e organizzativi che i titolari privati possono dispiegare per perseguire le proprie finalità. Ma ciò che più di ogni altra cosa differenzia il settore pubblico da quello privato sono le regole e i limiti specifici che sono posti dalla normativa.

Innanzitutto gli articoli 6 e 9 del Regolamento n. 2016/679 com'è noto elencano le basi giuridiche che rendono leciti i trattamenti dei dati personali comuni e di quelli appartenenti alle c.d. categorie particolari. L'articolo 6 paragrafo 1 lettere c) ed e) stabilisce che sono leciti i trattamenti svolti per

MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia. Il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, 219 ss.

[14] Garante per la protezione dei dati personali, *Linee guida in materia di attività promozionale e contrasto allo spam* - 4 luglio 2013, docweb n. 2542348, reperibili al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348

[15] Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Istituto Nazionale Previdenza Sociale (INPS)* - 29 novembre 2018, docweb n. 9078812, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9078812

[16] Garante per la protezione dei dati personali, *Provvedimento del 18 dicembre 2014*, docweb n. 3736353, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3736353

[17] Garante per la protezione dei dati personali, *Provvedimento del 27 ottobre 2016*, docweb n. 5890115, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5890115

18 Garante per la protezione dei dati personali, *Audizione informale del Presidente del Garante per la protezione dei dati personali nell'ambito dell'esame delle proposte di legge C. 1056 e abb., recanti istituzione di una Commissione parlamentare di inchiesta sulla diffusione intenzionale, seriale e massiva di informazioni false (cosiddette fake news)* – 3 marzo 2020, docweb n. 9283850 reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283850 .

adempiere un obbligo legale, o per dare esecuzione ad un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. L'articolo 9 paragrafo 2 lettera g) invece reca un'ipotesi di eccezione al divieto generale di trattamento di categorie particolari di dati, quando il trattamento è necessario per motivi di interesse pubblico rilevante, è proporzionato rispetto alla finalità perseguita, rispetta il diritto alla protezione dei dati personali e prevede misure specifiche a tutela dei diritti fondamentali degli interessati.

Diverse norme del Regolamento europeo fanno espresso rimando alla potestà normativa degli Stati membri per la specificazione del contenuto delle prescrizioni. Potestà che è stata esercitata attraverso la modifica del Codice della privacy ad opera del D. lgs. n. 101 del 2018 (*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679*).

Il Decreto n. 101, modificando sensibilmente il Codice della privacy, ha introdotto alcune specificazioni ed integrazioni riguardanti il settore pubblico[19], ad esempio, l'art. 2-*ter,* l'art. 2-*sexies* e l'art. 2-*octies* del Codice privacy novellato.

L'art. 2-*ter* individua la base giuridica per il trattamento dei dati comuni in ambito pubblico, precisando che tale base potrà essere costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. L'art. 2-*sexies* elenca le materie di interesse pubblico rilevante ai fini della applicazione dell'art. 9, par. 2, lett. g), specificando che i trattamenti di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante sono ammessi se previsti dal diritto dell'Unione o da norme di legge o, nei casi previsti dalla legge, di regolamento che debbono specificare i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. L'articolo 2-*octies* prevede che, fatto salvo quanto previsto dal D. lgs. 51/2018[20], il trattamento di dati relativi a condanne penali e a reati o connesse misure di sicurezza che non avviene sotto il controllo dell'autorità pubblica, è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

[19] Si veda per un commento F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Torino, 2021, 366 ss.

[20] Attuativo della Direttiva 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

Come anticipato, le disposizioni appena richiamate dimostrano che le autorità pubbliche e gli organismi di diritto pubblico sono sottoposti a vincoli molto più stringenti rispetto a quanto avvenga per i titolari del trattamento privati. La differenza si riflette anche nei provvedimenti del Garante, che deve utilizzare parametri diversi nel giudicare la legittimità dei trattamenti sottoposti al suo vaglio, e decidere sulla base della rispondenza del trattamento delineato a tutte le regole poste dalla normativa europea e nazionale. Come si vedrà più avanti, trattamenti apparentemente simili potranno essere giudicati coerenti con il sistema di tutela dei dati personali oppure no.

2. Il Garante e l'uso degli algoritmi nel settore privato: dalla identificazione alla analisi biometrica "anonima"

La rassegna dei provvedimenti del Garante in materia di decisioni algoritmiche non può che iniziare con un richiamo alla copiosa produzione relativa ai trattamenti automatizzati finalizzati all'identificazione di persone fisiche, per consentire alle stesse di accedere a banche o ad aree particolari dei loro luoghi di lavoro[21]. Questo tipo di esame, pur non rappresentando, a rigore, un processo decisionale automatizzato che abbia effetti rilevanti sull'interessato, quanto piuttosto un procedimento di identificazione, costituisce cionondimeno il primo passo di una lunga attività del Garante che si muove spesso sul confine tra le due tipologie di trattamento automatizzato, ove peraltro la valutazione sulla esistenza o meno di una *decisione* è tutt'altro che scontata[22].

In sede di verifica preliminare il Garante ha più volte autorizzato l'utilizzo di sistemi di identificazione basati sul trattamento di dati biometrici (come l'impronta digitale o la geometria della mano). Questo tipo di trattamenti ha ottenuto il via libera dell'Autorità ogniqualvolta il titolare avesse predisposto misure idonee, tali da garantire al contempo la risposta alle esigenze di

[21] Si vedano in proposito le *Linee guida del Garante per la protezione dei dati personali in materia di riconoscimento biometrico e firma grafometrica* del 12 novembre 2014, docweb n. 3563006, reperibili al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3563006 .

[22] Si pensi agli algoritmi utilizzati dai Social network e all'influenza che questi possono avere nel condizionare le scelte e la formazione delle opinioni degli utenti. A tale proposito l'Interim report sui Big Data pubblicato da Agcom nel 2018 ricorda come gli algoritmi siano «*determinanti nel definire le modalità di consumo informativo degli utenti, e assumono un valore significativo anche dal lato dell'offerta nell'orientare il successo di talune notizie (ed editori) rispetto ad altre e nel determinare le scelte di editori e giornalisti*». Relativamente all'influenza dei Social network sull'opinione pubblica il report conclude affermando che «*l'esposizione a messaggi informativi piuttosto che ad altri sulle piattaforme online, rispetto alla quale i big data raccolti risultano decisivi, non soltanto incide sulle percezioni degli utenti, ma è in grado di riflettersi sulla formazione delle opinioni degli stessi per poi tradursi in scelte e azioni concrete, incluse quelle determinanti per gli esiti elettorali*», cfr. Autorità per le garanzie nelle comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, 2018. Ved. anche Amnesty International: *Surveillance Giants: how the business model of Google and Facebook threatens human rights*, 2019.

sicurezza e la tutela dei dati personali. Generalmente si trattava di sistemi in cui, mediante un algoritmo, i dati biometrici venivano trasformati in una sequenza numerica e inseriti in una *smart card* in possesso del solo interessato (tra le altre decisioni, docweb n. 1306098 del 15/06/2006[23], n. 1835792 del 10/06/2011[24], n. 2710934 del 19/09/2012[25] e sulla lettura della geometria della mano n. 2354574 del 10/01/2013[26]).

In questo specifico ambito di intervento del Garante, riveste particolare interesse la verifica preliminare all'esito della quale l'Autorità ha ammesso un trattamento consistente nella analisi comportamentale *on-line* dei clienti di un servizio di *home banking*, al fine di scongiurare, o di ridurre, il rischio di frodi informatiche (docweb n. 5252271 del 09/06/2016[27]). Il trattamento si basava sulla progressiva creazione di un *profilo comportamentale* del cliente, che veniva tradotto, dopo l'analisi di successive sessioni di navigazione, in un punteggio. Tale punteggio risultava dalla applicazione di calcoli probabilistici e algoritmi di autoapprendimento a parametri quali le traiettorie effettuate con il mouse, le azioni eseguite, la velocità di digitazione sulla tastiera. Uno scostamento tra il punteggio del cliente e quello di un eventuale criminale informatico avrebbe a quel punto avviato una procedura di controllo e blocco di intrusioni indebite. L'Autorità ha ritenuto che il trattamento fosse lecito e proporzionato, e rispondente al principio di necessità. Anche in questo caso la valutazione ha riguardato il bilanciamento tra le misure di tutela adottate e le finalità di sicurezza e prevenzione delle frodi perseguite attraverso il trattamento.

La modalità appena descritta di verifica dell'identità dell'utente attraverso la profilazione dei suoi comportamenti quando esso è collegato in rete richiama la proposta fatta di recente dal Garante privacy al social network Tik-Tok, a seguito delle vicende di cronaca riguardanti le conseguenze drammatiche dell'accesso a questi canali di comunicazione da parte di bambini. L'Autorità

[23] Garante per la protezione dei dati personali, *Verifica preliminare: uso della biometria per identificazione del personale nelle banche* - 15 giugno 2006, docweb n. 1306098, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1306098

[24] Garante per la protezione dei dati personali, *Trattamento di dati biometrici ricavati dalla lettura delle impronte digitali* - Verifica preliminare - 10 giugno 2011, docweb n. 1835792, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1835792

[25] Garante per la protezione dei dati personali, *Sistema per l'accesso della clientela in modalità self service, 24 ore su 24, alle cassette di sicurezza, con trattamento di dati biometrici* - Verifica preliminare richiesta da Credito Lombardo Veneto S.p.A. - 19 settembre 2013, docweb n. 2710934, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2710934

[26] Garante per la protezione dei dati personali, *Sistema di rilevazione di dati biometrici dei lavoratori basato sulla lettura della geometria della mano* - 10 gennaio 2013, docweb n. 2354574, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2354574

[27] Garante per la protezione dei dati personali, Verifica preliminare. *Trattamento di dati personali e biometrici basato sull'analisi comportamentale dei clienti di una banca in occasione della loro navigazione nell'area privata del sito web* - 9 giugno 2016, docweb n. 5252271, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5252271

ha proposto a Tik-Tok di rafforzare i controlli sull'età effettiva degli utenti anche attraverso lo sviluppo di algoritmi di *age verification*, basati sull'analisi dell'interazione dell'utente con l'applicazione e con il device, per una verifica "predittiva" non già dell'identità dell'utente, bensì della sua età[28].

La dichiarata disponibilità del social network cinese a sviluppare algoritmi "non identificativi" conferma una tendenza degli operatori del settore privato ad adeguarsi alla normativa in materia di protezione dati e ad accogliere le indicazioni dell'Autorità garante, a cui pare corrispondere un'apertura del Garante ad un dialogo costruttivo e basato su approfondite analisi degli aspetti tecnologici dei trattamenti in esame.

Due interessanti esempi di questa tendenza risalgono al 2018.

Il primo riguarda la verifica preliminare avente ad oggetto il rilevamento di immagini in punti diversi all'interno dell'Aeroporto di Roma-Fiumicino, al fine di monitorare il tempo di permanenza dei passeggeri all'interno della struttura e la durata delle code. Questa misurazione avveniva attraverso il riconoscimento facciale e il successivo confronto del *template* rilevato in due zone diverse dell'Aeroporto[29] (docweb n. 8789277 del 15/03/2018[30]).

In questo caso il Garante ha autorizzato il trattamento dopo aver verificato che esso è basato su un *software* di riconoscimento facciale che codifica le immagini immediatamente dopo la loro acquisizione e crea un *template* biometrico non riconducibile alla persona e non associabile alla carta d'imbarco. Il Garante, dunque, all'esito dell'esame ha ritenuto che il trattamento sottoposto al suo scrutinio fosse lecito e proporzionato rispetto alle finalità perseguite, specialmente alla luce delle misure di mitigazione del rischio predisposte, quali

[28] Si vedano gli interventi del componente dell'Autorità garante Guido Scorza del 24 e 25 gennaio 2021: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9526211; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9526029

[29] Per un approfondimento sulle tecnologie di riconoscimento facciale si veda G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021. In particolare, sulla rilevanza del principio di minimizzazione nella costruzione del *template* biometrico, ved. 174: «*Le dimensioni dei modelli biometrici e la quantità dei dati contenuti, da una parte, devono essere sufficientemente ampie da rendere il template utile alle finalità di trattamento e permettere di garantire la sicurezza dei dati, evitando il rischio di sovrapposizione tra dati biometrici diversi o di sostituzione di identità, come avverrebbe nel caso di modelli troppo poco accurati; dall'altra, le dimensioni del template devono essere sufficientemente ristrette, per mantenere l'univocità della costruzione del modello e non consentire di risalire ai dati biometrici raccolti dai quali esso è stato costruito*»

[30] Garante per la protezione dei dati personali, Verifica preliminare. *Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)* - 15 marzo 2018, docweb n. 8789277, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8789277

la cancellazione automatica delle immagini appena dopo la creazione del *template*[31] e l'uso dei soli dati relativi a persone non identificabili.

Un profilo ancora differente ed ulteriormente evolutivo viene affrontato con il provvedimento relativo ai c.d. *Totem*, le colonnine pubblicitarie installate presso la Stazione Centrale di Milano, e finalizzate all'analisi dell'*audience* pubblicitaria. Queste colonnine effettuano dei trattamenti che consentono di determinare il tempo di permanenza di un volto davanti allo schermo, il sesso, l'età e l'espressione facciale dello spettatore.

All'esito dell'istruttoria su questo trattamento, il Garante ne ha ammesso la prosecuzione basandosi sulla differenza tra algoritmi di *face recognition* e algoritmi di *face detection*, poichè le immagini dei volti vengono memorizzate solo per pochi istanti, mentre l'analisi statistica che viene effettuata a partire da tali rilevazioni è anonimizzata. Il Garante ha ammesso la prosecuzione del trattamento, impartendo delle prescrizioni relative alla informativa semplificata e al monitoraggio periodico dello stato dei dispositivi.

L'Autorità ha basato la decisione anche sulla considerazione che "*l'impiego di software di elaborazione in grado di estrapolare dati di tipo statistico dalle immagini riprese in modo pressochè immediato, senza elaborazioni biometriche né registrazioni di immagini, né accessi live, valgono a far ritenere che siano previste adeguate cautele affinchè non siano messi a rischio i diritti e le libertà fondamentali, nonché la dignità e la riservatezza degli interessati*". Il Garante inoltre ha autorizzato questo trattamento in assenza di consenso, data la difficoltà oggettiva della sua acquisizione, indicando la finalità di *marketing* come requisito alternativo (cfr. docweb n. 7496252 del 26/01/2018[32]).

Dalla lettura di questa prima serie di provvedimenti emerge una evoluzione che a partire dall'autorizzazione all'utilizzo di algoritmi di riconoscimento biometrico, attraverso l'esame di modalità di trattamento dei dati biometrici sempre meno invasive della privacy, giunge al paradosso della analisi biometrica anonima, una *profilazione senza identificazione*.

Il settore privato, grazie ad evidenti investimenti nello sviluppo di tecnologie rispettose della protezione dati, e privo dei vincoli cui è invece sottoposta l'attività del settore pubblico, ha dunque trovato in alcuni casi, come quelli proposti, la via per superare il vaglio del Garante.

[31] Sulla necessità della cancellazione dei dati biometrici "grezzi" generati nel procedimento di acquisizione dell'immagine e creazione del template si veda G. MOBILIO, *Tecnologie di riconoscimento facciale,* cit., 177.

[32] Garante per la protezione dei dati personali, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria* - 21 dicembre 2017, docweb n. 7496252, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252

Nel settore pubblico invece sembrerebbe emergere una tendenza all'utilizzo sempre più consistente delle decisioni algoritmiche e della profilazione seppure nella temporanea assenza di basi giuridiche e di garanzie per gli interessati. In questo ambito l'attività del Garante pare così essere più spesso caratterizzata dal richiamo alla corretta e completa applicazione della normativa in materia di protezione dei dati personali, come si vedrà nel prossimo paragrafo.

3. Il Garante e l'uso degli algoritmi nel settore pubblico: dalla sorveglianza mirata alla "sorveglianza universale"

Come accennato poc'anzi, l'utilizzo degli algoritmi nel settore pubblico è evoluto nel tempo verso una sempre più stringente tendenza alla profilazione del cittadino/contribuente/lavoratore/utente del Servizio Sanitario Nazionale, per le più svariate finalità. Questa tendenza ad un controllo più pervasivo, da realizzarsi grazie alle potenzialità dei trattamenti automatizzati, ha costretto l'Autorità ad incrementare la sua attività di sorveglianza e consulenza e in alcuni casi ad utilizzare i suoi poteri sanzionatori.

Sul versante delle attività di contrasto alla evasione fiscale, è nota, nei suoi termini generali, la vicenda che ha riguardato il c.d. *Redditometro*. In questo caso l'utilizzo di algoritmi da parte dell'Agenzia delle Entrate era finalizzato in primo luogo a selezionare i contribuenti da sottoporre ad accertamento e rideterminazione del reddito sulla base di informazioni provenienti da diverse fonti (dati conferiti dal contribuente, comunicazioni obbligatorie di operatori telefonici ed assicurazioni, specifiche campagne di controllo), e successivamente ad attribuire al contribuente un profilo cui imputare spese presunte. Tale profilo sarebbe stato elaborato sulla base di informazioni quali la residenza in una determinata zona geografica, o l'appartenenza ad una specifica tipologia di famiglia. Relativamente ai profili che rilevano in questa dissertazione, nel parere del 21/11/2013 (docweb n. 2765110[33]) l'Autorità ha prescritto all'Agenzia delle Entrate di adottare tutte le garanzie necessarie a tutelare i contribuenti rispetto ai trattamenti automatizzati e alla loro profilazione, primariamente per quanto riguarda la qualità dei dati utilizzati nella attribuzione del profilo.

Sempre sulla qualità dei dati vertono le indicazioni fornite dall'Autorità alla Agenzia delle Entrate nel 2019 e relative ad un sistema di analisi del rischio di evasione fiscale basato sul trattamento automatizzato di dati provenienti dall'Archivio dei rapporti finanziari e di ulteriori informazioni presenti

[33] Garante per la protezione dei dati personali, *Redditometro: le garanzie dell'Autorità a seguito della verifica preliminare sul trattamento di dati personali effettuato dall'Agenzia delle entrate* - 21 novembre 2013, docweb n. 2765110, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2765110

nell'Anagrafe tributaria per l'individuazione di profili di evasione rilevanti. In questo parere compare il riferimento all'intervento umano nel trattamento decisionale automatizzato. Infatti il Garante invita l'Agenzia delle Entrate a modificare lo schema di provvedimento sottoposto al suo esame, e a richiamare espressamente le garanzie per gli interessati, tra cui la "*puntuale valutazione della coerenza complessiva della posizione di ciascun contribuente selezionato da parte di operatori qualificati appartenenti alle Direzioni provinciali, appositamente istruiti […]*" (cfr. docweb n. 9106329 del 14/03/2019[34]).

È completamente assente l'intervento umano nel trattamento delineato dalla Provincia Autonoma di Trento nell'ambito della erogazione di interventi di sostegno economico-finanziario (concessione e determinazione di contributi, sussidi, sovvenzioni ed altre forme di vantaggi economici) (cfr. docweb n. 9480921 del 15/10/2020[35]). Nella norma sottoposta al vaglio dell'Autorità è previsto infatti che "*qualora la relativa attività istruttoria si sostanzi nel mero accertamento dei requisiti e nel calcolo dell'ammontare da corrispondere in base a fattori predeterminati con legge o con delibera*" l'amministrazione possa avvalersi di "*sistemi, anche totalmente automatizzati, la cui logica algoritmica sia periodicamente verificata allo scopo di minimizzare il rischio di errori, distorsioni o discriminazioni di sorta*". La Provincia Autonoma di Trento sottolinea nella relazione illustrativa che si tratta di una attività sostanzialmente priva di discrezionalità amministrativa. Anche in questo caso però la presenza di un operatore è prevista tra le garanzie: la formula algoritmica utilizzata sarà resa pienamente conoscibile agli interessati in modo che gli stessi possano se del caso contestare la decisione e chiedere l'intervento umano.

Pur richiedendo un rafforzamento delle misure a tutela degli interessati, il Garante ha espresso in questo caso parere favorevole al trattamento decisionale completamente automatizzato predisposto dalla Provincia Autonoma di Trento, in quanto esso reca tutte le garanzie richieste dal Regolamento in presenza di decisioni algoritmiche.

[34] Garante per la protezione dei dati personali, *Parere sul provvedimento del Direttore dell'Agenzia delle entrate recante "Disposizioni di attuazione dell'articolo 11, comma 4, del DL 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214, e successive modificazioni. Analisi del rischio di evasione. Estensione all'anno 2014-2015 della sperimentazione della procedura di selezione basata sull'utilizzo delle informazioni comunicate all'Archivio dei rapporti finanziari* - 14 marzo 2019, docweb n. 9106329, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9106329

[35] Garante per la protezione dei dati personali, *Parere favorevole sullo schema di norma predisposta dalla Provincia Autonoma di Trento in materia di trattamenti che implicano decisioni integralmente automatizzate* - 15 ottobre 2020, docweb n. 9480921, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9480921

Il 5 marzo 2020 il Garante ha reso un importante parere al Consiglio di Stato (docweb n. 9304455[36] del 5 marzo 2020). A sua volta il Ministero della Salute si era rivolto ai Giudici di Palazzo Spada per chiedere un parere relativo all'utilizzo di nuove modalità di ripartizione del fondo sanitario tra le Regioni e il Consiglio di Stato ha ritenuto di coinvolgere per competenza l'Autorità garante. Il Ministero della Salute proponeva un sistema di ripartizione del FSN basato su una interconnessione tra i flussi amministrativi attivi presso il Ministero e, successivamente, un incrocio di tali flussi con le informazioni reddituali provenienti dall'Anagrafe tributaria, dai registri di mortalità, dall'ISTAT, oltre che i codici di esenzione per patologia. I profili risultanti da queste elaborazioni avrebbero consentito di procedere ad una *stratificazione* degli utenti del Servizio Sanitario Nazionale in base allo stato di salute individuale e alla situazione economica. Questa stratificazione avrebbe portato alla creazione di raggruppamenti per malattie croniche e per status sociale legato al reddito individuale.

In questo caso il Garante sottolinea la necessità di effettuare un attento bilanciamento tra interesse pubblico rilevante e tutela dei dati personali. Riconducendo esplicitamente il trattamento delineato dal Ministero della Salute alla definizione di profilazione contenuta nel GDPR, il Garante richiama la sentenza del Consiglio di Stato n. 8472 del 2019 in cui i Giudici di Palazzo Spada hanno ricordato come dal diritto sovranazionale emergano tre principi che debbono essere applicati in presenza di decisioni automatizzate. Si tratta del principio di conoscibilità, ovvero la possibilità di conoscere l'esistenza di processi automatizzati riferiti alla propria persona e di ricevere informazioni significative sulla logica utilizzata dagli algoritmi, il principio di non esclusività della decisione algoritmica e infine il principio di non discriminazione algoritmica "*secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che 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*".

[36] Garante per la protezione dei dati personali, *Parere al Consiglio di Stato sulle nuove modalità di ripartizione del fondo sanitario tra le regioni proposte dal Ministero della salute e basate sulla stratificazione della popolazione* - 5 marzo 2020, docweb n. 9304455, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9304455

Il Garante conclude rilevando che al momento non sussiste una base giuridica per interconnettere i flussi informativi sanitari del Ministero della Salute e per acquisire categorie particolari di dati da altre Amministrazioni pubbliche, e che non si rinviene una base giuridica neppure per la delineata attività di stratificazione di tutti gli utenti del SSN.

Concludiamo anche la rassegna relativa agli interventi di regolazione del Garante nel settore pubblico con due pronunce relative alle tecnologie di riconoscimento facciale.

Con provvedimento del 25 marzo 2021 (docweb n. 9575877 del 25/03/2021[37]) l'Autorità si è pronunciata sul c.d. *sistema SARI Real Time*, che ove fosse stato utilizzato, avrebbe consentito di analizzare in tempo reale i volti ripresi da telecamere installate in aree geografiche predeterminate, confrontandoli con una banca dati predefinita (*watch-list*) contenente un massimo di 10.000 volti. Il sistema, sottoposto alla valutazione dell'Autorità dal Ministero dell'Interno - Dipartimento di Pubblica Sicurezza, attraverso un algoritmo di riconoscimento facciale avrebbe individuato corrispondenze tra i volti e avrebbe di conseguenza generato un *alert* per richiamare l'attenzione degli operatori sul *match* tra il soggetto ripreso e uno dei profili contenuti nell'archivio di riferimento.

Il Garante nell'esprimere un parere su tale proposta ha chiarito che "*il sistema in argomento realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di polizia; ancorchè la valutazione d'impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno l'identificazione di una persona in luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella "watch-list*". Nell'ordinamento italiano mancano disposizioni normative specifiche che consentano tale tipo di trattamento che per le sue caratteristiche determina una forte interferenza con la vita privata delle persone interessate, pertanto il Garante esprime parere negativo rispetto al trattamento sottoposto al suo vaglio. Molto significativo appare il passaggio del provvedimento in cui l'Autorità sottolinea come con il trattamento biometrico di tutte le persone che circolano in uno spazio pubblico si determini "*una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui*". Infatti, l'impiego di

[37] Garante per la protezione dei dati personali, *Parere sul sistema Sari Real Time* - 25 marzo 2021, docweb n. 9575877, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

tecnologie di riconoscimento facciale per finalità di prevenzione e repressione dei reati dovrebbe avvenire solo ove strettamente necessario, in modo proporzionato alle finalità e con le dovute garanzie[38].

L'assenza di una specifica previsione normativa sulla raccolta dei dati biometrici è il rilievo su cui si basa anche l'ingiunzione al Comune di Como del 26/02/2020 (docweb n. 9309458[39]), con la quale il Garante si è espresso negativamente rispetto alla sperimentazione di un sistema di videosorveglianza con funzioni di riconoscimento facciale con la finalità di ausilio alla Polizia locale nella individuazione di persone oggetto di indagine o scomparse, o situazioni potenzialmente pericolose.

Il mancato rispetto del principio di proporzionalità, piuttosto che la mancanza di una base giuridica adeguata, o addirittura la compressione ingiustificata di un diritto fondamentale quale la tutela della vita privata sono le motivazioni per cui il Garante si è espresso, nei casi citati, sfavorevolmente rispetto a trattamenti di dati personali proposti da attori pubblici. Alla luce dei provvedimenti richiamati appare ancora più evidente quanto rilevino i vincoli posti ai titolari del trattamento pubblici, che frequentemente nel sottoporre al Garante la proposta di una nuova tecnologia o di un nuovo trattamento automatizzato di dati personali incontrano, prima di ogni altro, il limite della mancanza di una base giuridica adeguata.

Ne sia una riprova il fatto che la Provincia Autonoma di Trento ha ricevuto parere favorevole, pure in presenza di un trattamento decisionale completamente automatizzato. Ciò si è verificato innanzitutto in quanto il trattamento proposto dall'ente locale è previsto da una norma di legge primaria, che contiene tutte le misure a garanzia degli interessati. Non così, per esempio, nel caso della proposta del Ministero della Salute rispetto alla stratificazione degli utenti del Servizio Sanitario Nazionale in base alla situazione clinica ed economica, in quanto mancava una base giuridica per il trattamento.

Significativo appare anche il confronto tra le decisioni riguardanti i trattamenti di riconoscimento facciale su larga scala nel settore privato e in quello pubblico. Rispetto ai due casi relativi al settore privato, cioè la creazione di *template anonimi* presso l'Aeroporto di Roma-Fiumicino e la *profilazione senza*

[38] La proposta di Regolamento europeo sull'Intelligenza Artificiale presentata dalla Commissione (di cui si dirà *infra*) pone l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto tra le pratiche vietate, salvo poi porre eccezioni e condizioni che sembrerebbero attenuare di molto la portata del divieto. Cfr. *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (Legge sull'Intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final*, art. 5 par. 1 lett. d, parr. 2,3,4.

[39] Garante per la protezione dei dati personali, *Provvedimento del 26 febbraio 2020*, docweb n. 9309458, reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9309458

identificazione realizzata attraverso i Totem pubblicitari della Stazione Centrale di Milano, il *sistema SARI Real Time* non supera il vaglio del Garante. A ben vedere, i presupposti del trattamento in questo ultimo caso sono totalmente differenti rispetto ai primi due citati. Essendo un trattamento posto in essere da una autorità pubblica, l'esame ha valutato la presenza di una base giuridica specifica (necessità di una norma di legge primaria), la qualità del titolare (il Ministero dell'Interno - Dipartimento di Pubblica Sicurezza), le finalità del trattamento (prevenzione e repressione dei reati), la tipologia degli interessati (sorveglianza universale di tutti gli individui, anche non attenzionati), la tipologia del trattamento e dei dati trattati (realizzazione di *template* biometrici in tempo reale e confronto con una banca dati), concludendo per la inammissibilità del trattamento così progettato.

4. Spunti di riflessione sul ruolo *costituzionale* del Garante nella regolazione delle decisioni algoritmiche

Ci si interroga ormai da diversi anni sulle potenzialità e sui limiti dell'uso degli algoritmi in tutti i settori della società[40]. E come sappiamo ad alcune delle più evidenti problematiche costituzionali legate all'utilizzo delle decisioni algoritmiche che hanno effetti significativi sugli individui ha tentato di rispondere il Regolamento europeo n. 2016/679. I principi di conoscibilità e di comprensibilità degli algoritmi, il principio di non esclusività della decisione algoritmica, infine il principio di non discriminazione algoritmica[41] possono essere tratti dalla lettura degli articoli 13, 14 e 22 del GDPR, oltre che del Considerando 71[42].

Molti casi giurisprudenziali nazionali ed esteri hanno consentito di portare la riflessione oltre la teoria, verificando quanto gli effetti concreti di una decisione algoritmica incostituzionale, ingiusta, discriminatoria, sbagliata possano essere gravi[43].

[40] Ex plurimis, G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, II, giugno 2019, 198 ss.

[41] Imprescindibili i contributi di A. SIMONCINI-S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, I, giugno 2019, 86 ss., e A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Rivista di BioDiritto*, n. 1/2019, 63 ss.

[42] Infatti il principio di non discriminazione algoritmica, insieme con il *right to an explanation* e al divieto assoluto di decisioni algoritmiche riguardanti i minori, pur essendo presenti nel Considerando 71, non sono riprodotti nel testo del Regolamento. Cfr. A. SIMONCINI, *L'algoritmo incostituzionale*, cit., in particolare il passaggio (84) in cui a proposito della non discriminazione algoritmica si parla di un principio fondamentale *«"latente" nella trama normativa del diritto euro-nazionale»*

[43] Si pensi al celeberrimo caso *Loomis* (*State v. Loomis*, 881 N.W.2d, Wis. 2016) sull'utilizzo nei procedimenti penali di un *software* in grado di prevedere il rischio di recidiva e la pericolosità sociale dell'imputato, la cui logica di funzionamento era però protetta dai diritti di proprietà intellettuale. Nella giurisprudenza amministrativa italiana, tra le altre: Consiglio di Stato (Sez. VI) n. 2270 dell'8

Per di più, ormai non ci si chiede più se un algoritmo di Intelligenza artificiale discrimina, ma piuttosto come lo fa, ai danni di chi, in base a che cosa[44], e gli strumenti posti in mano all'interessato per *difendersi* dalle decisioni algoritmiche sbagliate non sembrano sufficienti, specialmente alla luce dei sempre nuovi meccanismi di profilazione, realizzati attraverso la creazione di *cluster*[45], in cui perdono di efficacia gli strumenti giuridici di tutela basati sul rapporto interessato / titolare del trattamento.

Sempre più si verifica una tipologia di discriminazione algoritmica che può essere definita come *profilazione passiva*, in cui ciò che viene profilato è un contesto, più che un singolo individuo. Dalla osservazione di quante più persone che si muovono all'interno dello stesso contesto, e dei loro comportamenti, sarà possibile desumere – prevedere – il comportamento di singoli individui non profilati personalmente ma ricondotti per mezzo di altre correlazioni a quel determinato *cluster*.

In particolare, come D'Acquisto spiega magistralmente[46], le nuove tipologie di profilazione basate sui Big Data sono incentrate su due presupposti: il volume dei dati e la loro varietà. Il volume interessa sino ad una certa misura, poiché le informazioni sulle abitudini passate di un soggetto servono a confermare uno stereotipo ma non aiutano a prevedere il comportamento futuro. A questo punto entra in gioco la varietà dei dati. Il modo migliore per prevedere

aprile 2019 e n. 8472 del 13 dicembre 2019. Entrambe le decisioni hanno origine dalla riorganizzazione del corpo docente sul territorio nazionale, per la realizzazione del piano straordinario di cui alla l. 107/2015, per cui il Ministero dell'Istruzione aveva deciso di servirsi di un *software* in base al quale le assegnazioni degli insegnanti erano state effettuate mediante un algoritmo di cui erano sconosciute le concrete modalità di funzionamento. Per quanto riguarda la giurisprudenza di merito, con sentenza del 24 marzo 2021 n, 14381 la Corte di Cassazione, Sez. I civ., si è pronunciata su ricorso del Garante per la protezione dei dati personali in merito alla attività di una piattaforma *web* di *rating* reputazionale, stabilendo che il consenso dell'utente al trattamento dei propri dati personali al fine della determinazione del proprio profilo reputazionale non possa dirsi validamente espresso in mancanza di trasparenza sul funzionamento dell'algoritmo di *rating*: *«E non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati».*

[44] C. NARDOCCI, *Intelligenza Artificiale e discriminazioni*, presentato al Convegno annuale dell'associazione "Gruppo di Pisa" *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, 18 e 19 giugno 2021 e pubblicato in versione provvisoria nel sito dell'Associazione Gruppo di Pisa, 12.

[45] «*Nella maggior parte dei casi, inoltre, l'obiettivo principale dell'analisi non è più il singolo e la profilazione dello stesso sulla base dei suoi comportamenti, quanto, piuttosto, la società nel suo insieme o determinate comunità sociali e gruppi di individui. I software per l'analisi dei Big Data vengono, infatti, per lo più impiegati per individuare caratteristiche comuni, preferenze o abitudini di una determinata collettività, al fine di predirne i futuri comportamenti ovvero di adottare decisioni che interessano tutta la comunità considerata*», M.S.ESPOSITO, *L'impatto del trattamento sui diritti e le libertà delle persone fisiche*, cit., 220.

[46] G. D'ACQUISTO, *Nuovi tipi di profilazione, ecco i rischi privacy: servono tutele più ampie*, in *AgendaDigitale*, 19 aprile 2019.

una condotta infatti è osservare quante più persone possibili e integrare il profilo parziale dell'una con il profilo parziale dell'altra, piuttosto che continuare ad accumulare dati su un solo soggetto.

In questi termini, la *clusterizzazione* esce completamente dalla sfera di controllo (e dalle possibilità di difesa) dell'interessato. Essere o non essere profilato all'interno di un gruppo, essere o non essere una minoranza discriminata, non dipende da fattori e scelte personali ma da calcoli, previsioni, in definitiva da algoritmi.

Di fronte a questo scenario inquietante e alla comparsa tipologie di discriminazioni algoritmiche sempre nuove, con conseguente aumento dei rischi per i diritti e le libertà delle persone fisiche, il Garante per la protezione dei dati personali potrebbe farsi custode e promotore del rispetto dei principi fondamentali nell'uso degli algoritmi, tutelando così gli interessi non solo dei singoli interessati al trattamento, ma dell'intera collettività, ed evitando che si realizzi il *medioevo digitale* ben delineato da Mantelero[47].

Solo l'*expertise* dell'Autorità di controllo infatti potrebbe garantire una comprensione elevatissima delle questioni tecniche e tecnologiche sottese all'utilizzo degli algoritmi e al contempo potrebbe assicurare il rispetto dei principi fondamentali e dei diritti delle persone fisiche destinatarie delle decisioni algoritmiche: in definitiva il Garante effettuerebbe un controllo di costituzionalità tecnico e giuridico per individuare e correggere gli algoritmi incostituzionali[48].

I poteri che il Regolamento europeo e il Codice della Privacy novellato assegnano al Garante gli consentirebbero di agire in questa direzione.

Ci si riferisce alla significativa estensione dei poteri di *soft law* attribuiti alle Autorità di controllo dal Regolamento europeo n. 2016/679. Poteri che sono stati ampliati grazie al Decreto n. 101/2018 e alla novella al Codice della privacy. Le norme che hanno introdotto tali rilevanti novità sono l'art. 2-*quater* relativo alle regole deontologiche, l'art. 2-*septies* sulle misure di garanzia per il trattamento dei dati biometrici, genetici e relativi allo stato di salute, e l'art. 2-

[47] *«[…] un tempo "il singolo, all'atto della nascita, era collocato in una determinata casta sociale, cui erano collegati diritti e doveri, - si pensi alla posizione del 'servo' nel Medioevo, di nobile, di ecclesiastico, di militare, di reniter". Solo con il tempo, con l'evolvere della società e della cultura giuridica, il singolo è uscito dalla folla indistinta e si è affrancato da uno status che lo connotava in maniera spesso permanente. Rispetto a questo scenario di evoluzione storica del rapporto fra individuo e classificazioni sociali, i nuovi modelli algoritmici creano una sorta di nuovo medioevo digitale. Riemerge il rischio di una società connotata da una segmentazione per caste, ove lo status non è però dato dalla nascita o dall'appartenenza a classificazioni sociali tradizionali (quelle su cui vigilano le norme in materia di non-discriminazione), ma da algoritmi e dai valori di coloro che li generano»,* A. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia. Il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, 302.

[48] A. SIMONCINI, *L'algoritmo incostituzionale, cit.*

quinquiesdecies che sulla base dell'art. 36 par. 5 del GDPR disciplina i provvedimenti di carattere generale relativi a trattamenti che comportano rischi elevati per l'esecuzione di compiti di interesse pubblico[49]. Ciascuna di queste norme attribuisce al Garante poteri regolatori di assoluto rilievo. Basti ricordare che il rispetto delle regole deontologiche di cui all'art. 2-*quater* è condizione essenziale per la correttezza e liceità dei trattamenti dei dati personali.

A norma dell'art. 2-*septies* par. 5 le misure di garanzia individuano «*le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati»,* cioè regolano aspetti di dettaglio dei trattamenti, di fatto creando un *sotto-apparato regolatorio*[50].

L'art. 2-*quinquiesdecies* sembra reintrodurre l'istituto delle autorizzazioni preventive, consentendo al Garante di intervenire, d'ufficio, con provvedimenti di carattere generale volti a prescrivere misure ed accorgimenti a tutela dell'interessato, anch'esse vincolanti per il titolare.

Accanto ai poteri di *soft law*, il ruolo di vigilanza e regolazione del Garante può sostanziarsi anche attraverso specifici *poteri* che il GDPR attribuisce alle Autorità di controllo, tra cui quello di ottenere dal titolare o dal responsabile del trattamento l'accesso a tutte le informazioni necessarie per l'esecuzione dei suoi compiti[51]. Una interpretazione estensiva di questa disposizione potrebbe legittimare indagini molto penetranti su ogni aspetto della tutela dei dati personali.

I compiti del Garante, infatti, comprendono la sorveglianza sull'applicazione del Regolamento e la possibilità di svolgere indagini al fine di individuare eventuali violazioni. Non a caso nell'articolato la trattazione dei reclami e le attività di indagine sono elencati sotto punti separati. Dunque il Garante potrebbe richiedere ai titolari di fornire informazioni sul trattamento dei dati personali, anche finalizzate a conoscere la logica sottesa agli algoritmi, e a comprendere come determinate pratiche di Intelligenza Artificiale possano incidere significativamente nella sfera giuridica delle persone fisiche, anche e soprattutto quando queste non possono essere qualificate come interessati, in ragione del fatto che, come descritto in precedenza, vi potrebbe essere una

[49] Ved. 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 tra Italia e Spagna*, Pisa, 2018, 79.

[50] Ibidem, 126.

[51] Art. 58 par. 1 lett. e del GDPR.

scissione tra il soggetto i cui dati vengono analizzati e il soggetto destinatario di una decisione algoritmica.

La *toolbox* del Garante, delineata nel GDPR e nel Codice novellato, è ulteriormente arricchita dallo strategico potere consultivo sulla normativa primaria previsto dall'art. 58 par. 3 lett. b del GDPR[52]. Il Garante ora può di sua iniziativa, o a richiesta, rilasciare pareri al Parlamento, al Governo o ad altri organismi ed istituzioni su questioni riguardanti la protezione dei dati personali.

Attraverso i pareri sulla normativa primaria l'Autorità può segnalare in anticipo eventuali criticità delle disposizioni, consentendo al legislatore di apportare i correttivi necessari al fine di garantire il pieno rispetto delle regole della protezione dati e quindi dei diritti e delle libertà degli interessati, anticipando il vaglio al momento della predisposizione degli atti normativi e regolamentari[53].

Vi sono questioni di assoluta delicatezza e complessità, che difficilmente possono essere affrontate a livello politico o di legislazione primaria. In questo senso il ruolo che al Garante viene assegnato dal Regolamento e dal Codice della privacy sulla elaborazione di pareri obbligatori sulla normativa primaria è decisamente strategico. La stretta collaborazione con il legislatore e con l'esecutivo appare la via più efficace per garantire che le norme prodotte rispondano ai requisiti di tutela dei dati personali, e quindi, ai principi fondamentali di cui si è detto, dal momento della progettazione. A ben vedere dunque la collaborazione tra Garante e legislatore altro non è che la forma più alta e ben riuscita di tutela dei dati personali *by design*.

[52] La Direttiva 95/46 prevedeva che le Autorità di controllo fossero consultate solamente in merito alle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali (art. 28 par. 2).

[53] F. MODAFFERI, *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e Codice novellato*, Torino, 2021, 372. Il Garante per la protezione dei dati personali ha accolto molto favorevolmente le nuove attribuzioni relative ai poteri sulla normativa primaria. Già nel Discorso per la Relazione annuale 2018 il presidente si era espresso in questi termini: «*Il parere obbligatorio del Garante sulla normativa primaria si è dimostrato, in questo primo anno di applicazione, un passaggio essenziale per delineare il miglior equilibrio possibile tra la protezione dati e gli altri diritti e interessi di rilevanza costituzionale, nel rispetto del canone di proporzionalità, valorizzato di recente dalla stessa Consulta in relazione alla trasparenza. Il dialogo tra Garante e legislatore ha spesso consentito apprezzabili miglioramenti dei testi, come nel caso del reddito di cittadinanza. Maggiori resistenze si sono invece riscontrate, ad esempio, rispetto all'introduzione generalizzata dei controlli biometrici per i dipendenti pubblici. È auspicabile che la sottovalutazione dei principi di proporzionalità e minimizzazione dei dati, riscontrata rispetto a tali provvedimenti, lasci spazio in futuro a un supplemento di riflessione, sottraendo temi così rilevanti all'enfasi della politica di parte e al conseguente rischio di norme meramente simboliche*». Anche il documento di *Obiettivi programmatici e linee di priorità dell'Autorità per l'anno 2021* contiene un riferimento alla crescente attività di redazione di pareri obbligatori sulla normativa primaria, cfr. Garante per la protezione dei dati personali, *Obiettivi programmatici e Linee di priorita' dell'Autorita' per l'anno 2021*, docweb n. 9539607, reperibili al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9539607.

Di più. I meccanismi di raccordo del Garante con le altre autorità di controllo, oltre che con il Comitato europeo per la tutela dei dati personali[54] consentiranno, se ben utilizzati, di avere un costate *double-check* e una verifica dell'aderenza della legislazione italiana all'*acquis* europeo in materia di protezione dati personali, scongiurando la possibilità di essere destinatari di procedure d'infrazione o pronunce pregiudiziali della Corte di Giustizia dell'Unione europea.

***

A fronte delle idee esplorative appena delineate sul ruolo costituzionale del Garante come custode dei diritti fondamentali, è bene prima di concludere evidenziare come lo scenario entro il quale l'Autorità si muove potrebbe essere presto occupato anche da altri attori, con ruoli che probabilmente si intersecheranno con quello del Garante.

Mi riferisco in particolare al Comitato europeo per l'Intelligenza artificiale, previsto dalla proposta di Regolamento europeo in materia di Intelligenza artificiale[55]. Il Comitato sarà presieduto dalla Commissione e costituito allo scopo di fornire alla stessa consulenza e assistenza al fine di agevolare la cooperazione tra e con le Autorità nazionali di controllo per le materie disciplinate dal Regolamento, la applicazione uniforme della normativa nel territorio dell'Unione, e per «*coordinare e contribuire agli orientamenti e all'analisi della Commissione, delle autorità nazionali di controllo e di altre autorità competenti sulle questioni emergenti nel mercato interno in relazione alle materie disciplinate dal presente regolamento*»[56].

[54] Mi riferisco ai meccanismi di coesione e coerenza di cui al Capo VII del GDPR ed in particolare alla funzione di raccordo tra le Autorità di controllo che viene attribuita al Comitato europeo per la protezione dei dati, che tra l'altro: promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le Autorità di controllo, promuove programmi comuni di formazione e scambio di personale tra le stesse, promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo (cfr. art. 70, par. 1 lett. u,v,w del GDPR.

[55] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (Legge sull'Intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, consultabile al link https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN . Per una sintesi del contenuto ved. L. TOSONI, *Intelligenza artificiale, i punti chiave del regolamento europeo*, in *AgendaDigitale*, 21 aprile 2021.

[56] Cfr. Art. 56 della Proposta.

Rileva, a parere di chi scrive, l'indicazione nella disposizione del *mercato interno* come area di intervento del Comitato. Il focus è dunque dichiaratamente quello del mercato, piuttosto che la tutela dei diritti[57].

L'articolo 59 stabilisce che ogni Stato membro possa istituire o designare autorità nazionali competenti[58] per l'applicazione del Regolamento, mentre l'art. 57 delinea la composizione del Comitato facendo un riferimento generico alle Autorità di controllo nazionali ed uno invece specifico e significativo alla presenza del Garante europeo per la protezione dei dati, in questo modo fornendo una indicazione precisa rispetto alla *intentio* del legislatore europeo[59].

Appare ad oggi un po' meno lineare il coordinamento dell'attività del Garante con quella dell'Agenzia per la cybersicurezza nazionale, istituita con decreto-legge n. 82 del 14 giugno 2021[60]. Sebbene apparentemente il settore di competenza della neonata Agenzia sia, sulla carta, chiaramente differenziato rispetto al campo di azione del Garante privacy[61], non sembra difficile prevedere circostanze in cui le Autorità si troveranno in modo differente coinvolte[62].

In occasione della presentazione della Relazione 2019 sull'attività del Garante, il discorso del Presidente Soro toccava il tema della cybersecurity in questi termini: *«[…] la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale con i suoi vari snodi*». E ancora: «*Le implicazioni, in termini di sicurezza nazionale, di alcuni data breach dimostrano anche come la stretta*

[57] Sul passaggio, con la Proposta di Regolamento sull'AI, da anni di riflessione sulla "*Trustworthy AI*" ad una «*regolamentazione di tipo industriale*» ved. A. MANTELERO, *Sulle regole AI l'Europa sceglie un approccio "industriale"*: luci ed ombre, in *AgendaDigitale*, 27 aprile 2021. L'A. riflette sulla carenza, nella Proposta di Regolamento, di un quadro organico per la valutazione dell'impatto dell'Intelligenza artificiale sui diritti e le libertà fondamentali.

[58] «*Gli Stati membri garantiscono che le autorità nazionali competenti dispongano di risorse finanziarie e umane adeguate per svolgere i loro compiti a norma del presente regolamento. In particolare, le autorità nazionali competenti dispongono di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di intelligenza artificiale, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti»,* art. 59 par. 4 della Proposta.

[59] In questa ottica appare significativo che il Garante per la protezione dei dati personali con Delibera del 27 maggio 2021, peraltro in continuità con quanto esposto nel documento di Obiettivi programmatici e linee di priorità per l'anno 2021 rispetto alla crescente rilevanza delle questioni implicanti l'utilizzo di sistemi di Intelligenza artificiale (ved. *Supra* nota 53), abbia istituito al proprio interno il *Dipartimento intelligenza artificiale.*

[60] Decreto-legge 14 giugno 2021, n. 82 *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*.

[61] Cfr. art. 7 del D.L. n. 82/2021, *Funzioni dell'Agenzia per la cybersicurezza nazionale*.

[62] A norma dell'art. 7 par. 1 lett. d del D.L. n. 82/2021 l'Agenzia diviene Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto.

dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" induca a ripensare il concetto di sovranità digitale. […] In un contesto in cui le tecnologie ICT sono divenute – sempre più chiaramente con la pandemia – la principale infrastruttura di ciascun Paese, assicurarne una regolazione sostenibile e adeguata, tale da garantire la sicurezza, indipendenza dai poteri privati, soggezione alla giurisdizione interna, diviene un obiettivo non più eludibile».

Il Decreto che istituisce l'Agenzia nazionale per la cybersecurity ha previsto che essa consulti e collabori con il Garante, nel rispetto delle sue competenze, anche in relazione agli incidenti che coinvolgono dati personali, e che i due enti possano stipulare appositi protocolli d'intenti per definire le modalità di collaborazione. Non resta che attendere per verificare quanto virtuosamente le Autorità riusciranno a coordinarsi.

Prima di chiudere questo contributo, mi pare opportuno ribadire che le sfere di competenza del Comitato per l'Intelligenza Artificiale, dell'Agenzia per la sicurezza cibernetica e del Garante privacy sono ben differenti: il Comitato nasce come supporto alla Commissione europea nello sviluppo dell'industria basata sull'Intelligenza Artificiale, l'Autorità per la cybersicurezza di occupa di sicurezza nazionale e il Garante per la protezione dei dati personali veglia sui diritti fondamentali.

A ben vedere, l'osservazione dei nuovi equilibri che si creeranno tra questi diversi attori della società algoritmica potrebbe offrire uno scorcio sugli obiettivi strategici, sul bilanciamento dei valori in gioco, in definitiva sul futuro dell'intera Unione.

L'auspicio è che con il moltiplicarsi di soggetti con poteri regolatori, di consulenza e di controllo non si ottenga, nel tentativo di meglio regolare e meglio tutelare, l'effetto contrario di aumentare e irrigidire le procedure, a scapito della efficienza del mercato unico, della sicurezza, e della tutela dei diritti.