Journal of Ethics and Legal Technologies – Volume 4(2) – November 2022

L'uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello.

Claudio Sarra

Università di Padova.
Dipartimento di Diritto Privato e critica del diritto

Abstract: With the advent of mobile network connection tools, the use of digital platforms for carrying out ordinary tasks, as well as the development of social networks, almost the entirety of people life - located in geographical areas not affected by the digital divide - are projected in the datafied environment of the Internet. This *datafication* now concerns more and more the very physical and behavioral features of people, especially those belonging to the younger generations who, on the one hand, have total confidence with digital recording tools and, on the other, appear less sensitive to the confidentiality of their exposures. As a consequence, this makes biometric data – once hard to obtain without the subject's collaboration or an act of coercion upon him - widely available for collection and processing. This large availability makes it possible to easily use those data for many kinds of applications, far beyond unique identification which has already been a thoroughly scrutinized purpose even from the legal and ethical point of view. This paper deals with the use of biometrics in recruitment and tries to clarify the general European normative framework especially with reference to particularly strict national labour legislations and in the light of the recent European Proposal for a Regulation on AI.

Keywords: Biometrics, biometric data, GDPR, European Proposal on AI, recruitment, labour law.

1. Introduzione

La "biometria" è stata definita come l'insieme delle tecniche di identificazione o di 'misurazione' dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche o comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche[1].

Finora, in quella che è stata chiamata "biometria di prima generazione" [2], l'uso di dati biometrici è stato principalmente considerato con riferimento a due tipologie di procedure: a) l'*identificazione biometrica,* nella quale il modello (*template*) individuale è comparato con altri salvati in vari *databases* per verificare se vi è incluso (il che sostanzia una comparazione "uno a molti"); b) la *verifica di identità,* nella quale il modello individuale viene invece comparato con un altro previamente generato e conservato in un database (il che sostanzia una comparazione "uno a uno")[3].

Oggigiorno, con l'avvento della c.d. società *data-driven*[4]*,* le misurazioni biometriche sono rese estremamente agevoli dall'esponenziale aumento della diffusione di immagini e video nel Web, specialmente nei *social networks,* ciò che rende facilmente disponibile un'immensa quantità di materiale da processare. Sebbene non sempre utilizzabile per l'identificazione univoca, queste informazioni biometriche possono essere impiegate per una varietà di scopi differenti, creando le condizioni per una biometria "di seconda generazione" che è resa possibile, oltre che dalla ampliata disponibilità di materiale, anche dallo sviluppo tecnologico di strumenti più sofisticati[5]. Così, aldilà dei tradizionali approcci focalizzati sul problema di stabilire univocamente l'identità di un soggetto, nuovi utilizzi di dati biometrici si rendono facilmente possibili, quali, ad esempio, lo sviluppo e lo sfruttamento della c.d. biometria "soft". Si tratta dell'applicazione di tecniche biometriche a dati ricavati da tratti fisici e comportamentali dell'essere umano che, da soli, non consentirebbero l'identificazione univoca[6], ma ben utilizzabili per altri differenti fini.

Inoltre, l'aggregazione di grandi quantità di dati, inclusi quelli biometrici, assieme all'impiego di tecniche di *data mining* può essere usata per generare il modello di un desiderato ideal-tipo di soggetto quale referente statistico per includere o escludere certi individui a seconda del grado di corrispondenza.

[1] Cfr. Comitato Nazionale di Bioetica, 2010, p. 3.
[2] North-Samardzic, 2020, p. 435.
[3] Jain, Ross, Nandakumar, 2011, p. 10; Comitato Nazionale di Bioetica, 2020, p. 6; cfr. anche Garante per la Protezione dei Dati Personali, *Provvedimento generale prescrittivo in tema di biometria* – del 12 novembre 2014, nonché l'Allegato A del medesimo.
[4] Sarra, 2019.
[5] North-Samardzic, 2020, p. 437.
[6] Per uno sguardo complessivo sulla "soft biometrics" si veda ora Hassan, Isquierdo, Piatrik, 2021.

In queste applicazioni, il problema non è tanto stabilire l'identità di una certa persona ma, piuttosto, di trovare strumenti più affidabili per estrarre utili corrispondenze per altri scopi.

Nel caso del reclutamento al lavoro, per esempio, il profilo di un lavoratore ideale (per una specifica posizione) è elaborato quale referente per pre-selezionare i candidati o per classificare le loro richieste in vista di un'ulteriore fase di selezione, sia essa automatizzata o basata su decisione umane.

Vi sono alcune problematiche molto note circa le pratiche biometriche che sono assai più sensibili quando è in gioco il problema di stabilire univocamente l'identità personale. Questioni tipiche sono, per esempio, la legittimità dell'estrazione e dell'uso dei dati biometrici, la loro affidabilità nel tempo (alcune caratteristiche fisiche cambiano), l'universalità del tratto fisico o comportamentale considerato, l'abilità di individuare una deviazione naturale dal modello antropologico, anatomico o fisiologico standard di riferimento, o la volontaria alterazione dei tratti fisici o comportamentali; la resilienza del sistema con riferimento all'alterazione o eliminazione di dati rilevanti nel caso di processamento illegale, ed altre ancora[7].

Nel caso di applicazioni riferite al mondo del lavoro, vi sono spesso altre restrizioni e cautele da considerare. Leggi speciali sono talvolta particolarmente restrittive circa il processamento dei dati personali dei lavoratori o dei candidati ad un posto di lavoro e, cosa più importante, esse possono richiedere la necessità di una giustificazione assai rigorosa della relazione tra l'uso di un tratto biometrico, o un insieme di tratti biometrici, e le competenze e le abilità richieste per quel tipo di impiego.

Nell'ordinamento giuridico europeo, i livelli normativi da coordinarsi per chiarificare gli aspetti giuridici dell'uso dei dati biometrici per il reclutamento sono principalmente il Regolamento Europeo sulla Protezione dei Dati Personali e le leggi nazionali in materia[8]. Ma la recente "Proposta per un Regolamento Europeo sull'Intelligenza Artificiale" (Aprile 2021) introduce alcune nuove questioni rilevanti.

In particolare, essa stabilisce una deroga alla proibizione generale di usare dati "sensibili" (inclusi quelli biometrici) per finalità di monitorare e correggere i *bias* nei sistemi di Intelligenza Artificiale ad alto rischio (art. 10, §5)[9].

[7] In Smith, Miller, 2021, si offre una discussione sintetica complessiva sugli aspetti giuridici ed etici della biometria.

[8] Si veda inoltre il *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101,* del 5 giugno 2019 del Garante per la Protezione dei Dati Personali e che, con riferimento specifico ai dati biometrici, si applica fino al provvedimento contenente ulteriori misure di garanzia previsto all'art. 2-*septies* del D. Lgs 30 giugno 2003, n. 196.

[9] Il concetto di *bias* nell'ambito di procedure algoritmiche di decisione è, in verità, alquanto complesso è sta suscitando una discussione molto ricca in letteratura. Da un lato può dirsi

L'ampiezza delle possibili interpretazioni di questa deroga può suscitare dei dubbi in merito alla tenuta della protezione restrittiva fornita dal GDPR e dalle leggi nazionali, un punto questo che appare meritevole di approfondimento.

In questo lavoro, pertanto, darò inizialmente un quadro generale di riferimento sulla biometria (§ 2), poi, discuterò delle relazioni tra il GDPR e le leggi nazionali in merito all'uso di dati biometrici per il reclutamento, utilizzando l'esempio Italiano (§ 3), quindi mi concentrerò sulla Proposta di Regolamento Europeo sull'Intelligenza Artificiale, in particolare sulla possibilità di utilizzare la deroga di cui all'art. 10, § 5 per aggirare le restrizioni presenti nel *framework* generale (§ 4), infine, proverò a suggerire un coordinamento interpretativo tra queste fonti, offrendo alcune osservazioni conclusive (§ 5-6).

Per ragioni di brevità, nel parlare dei sistemi di reclutamento al lavoro presupporrò quale scenario di riferimento quello di procedure ibride nelle quali gli strumenti di IA sono usati per supportare la decisione umana. Non prenderò in considerazione, quindi, l'ipotesi di reclutamenti basati interamente su sistemi automatizzati senza alcun intervento umano[10].

2. Biometria: quanto di te è abbastanza?

Stabilire univocamente l'identità di una persona significa organizzare una serie di strumenti e di tecniche affidabili per discernere quel determinato soggetto rispetto ad altri in quanto titolare di determinati diritti, facoltà, obblighi o prerogative.

---

senz'altro che "algorithms inevitably make biased decisions. An algorithm's design and functionality reflects the values of its designer and intended uses, […] Development is not a neutral, linear path; there is no objectively correct choice at any given stage of development, but many possible choices''. Dall'altro la deviazione ripetuta da uno standard preferibile per ragioni etico-sociali, costituisce una caratteristica difettiva del sistema che richiede intervento. Il fatto è che vi sono numerose modalità per correggere tale comportamento (es. escludere certe variabili dal sistema, introdurre *bias* di bilanciamento, ecc.) i cui effetti potrebbero produrre a loro volta situazioni indesiderate. Questo punto è importante per comprendere che, come si vedrà, la deroga all'uso di dati biometrici di cui alla Proposta di Regolamento sull'IA può portare, se interpretata in modo troppo benevolo, a legittimare modalità di utilizzo di tali dati molto ampie. Per una discussione sullo stato delle questioni in merito al concetto di *bias* cfr. Tsamados, Aggarwal *et al.,* 2021; Mittelstadt, Allo *et al.,* 2016.

[10] Tale scenario, infatti, richiederebbe una discussione assai più lunga sul tema del c.d. *algorithmic decision-making* e della complessa disciplina di cui all'art. 22 GDPR che non è possibile svolgere qui. Il lettore interessato può consultare almeno: Sarra, 2020; Sarra, 2020a; Almada, 2019; ART29WP, 2018; Bygrave, 2020; Brkan, 2019; Mendoza, Bygrave, 2017; Roig, 2018, con la bibliografia ivi citata. A tale proposito, con riferimento specifico al diritto di contestazione delle decisioni automatizzate di cui al §3 dell'art. 22, un interessante lavoro di coordinamento operativo delle proposte dottrinali sul tema della contestabilità *by design* delle decisioni automatizzate si trova oggi in Alfrink, Keller, Kortuem G. *et al.*, 2022.

In questo contesto, pertanto, il concetto di identità personale non va confuso con una sorta di "essenza" metafisica della persona umana ma ha invece a che fare con la possibilità pratica di arrangiare le molte manifestazioni fenomeniche di taluno in uno specifico schema idoneo a distinguerlo – sperabilmente – da tutti gli altri soggetti di un determinato contesto[11].

Le misurazioni biometriche usate per stabilire l'identità personale si affidano alla possibilità di trarre vantaggio da manifestazioni fisiche e comportamentali peculiari e codificate in maniera oggettiva al fine di rendere i processi identificatori più veloci, affidabili e, possibilmente, automatici.

In quanto pertinenti alla stessa corporeità, i tratti fisici e comportamentali sono assai più strettamente correlati ad un soggetto rispetto ad altre caratteristiche che a questo possano essere attribuite con lo scopo di stabilire se una certa pretesa provenga effettivamente da lui in quanto soggetto titolato, quali ad esempio, la disponibilità di un certo codice, una *password*, un numero identificativo, un oggetto specifico (come una chiave fisica, ad esempio) e così via. In questi casi, la caratteristica identificante è "separabile" dal soggetto: può essere rubata, falsificata, perduta. Con una certa enfasi è stato detto che la biometria cambia il focus dell'identificazione da "qualcosa che si ha" a "qualcosa che si è" [12].

In generale, i dati biometrici devono corrispondere ad alcuni requisiti per potersi usare al fine di stabilire l'identità univoca di una persona.

Tali requisiti minimali sono:

- *universalità:* la caratteristica in questione dovrebbe essere posseduta da ciascuna persona;
- *misurabilità:* la caratteristica deve essere quantitativamente misurata;
- *distintività:* la caratteristica dovrebbe essere diversa da persona a persona;
- *permanenza:* la caratteristica dovrebbe essere relativamente invariante nel tempo[13];
- *accettabilità:* l'utilizzo di tale caratteristica biometrica dovrebbe essere accettato come mezzo di identificazione dalla società di riferimento in qualche grado[14].

Nessuno di questi requisiti dovrebbe essere preso in considerazione in maniera assoluta: ci possono essere variazioni nel caso specifico, o a causa di alterazioni fisiche (per es. impronte digitali rovinate dal lavoro manuale; un

[11] Da questo punto di vista si distingue tra il concetto di "identità" per riferirsi al problema metafisico e quello di "identificazione" per indicare la questione pragmatica di "*how* – or *in virtue of what – one may be recognized or recognize*", cfr. Mordini, Tsovaras, Ashton, 2012, at p. 2 (corsivo nel testo).

[12] Fairhurst, 2018, cap. 1, § 2 (versione elettronica).

[13] Jain, Ross, Prabhakar, 2004, p. 4.

[14] Smith, Miller, 2021, p. 3.

pattern dell'iride difettivo per una malattia dell'occhio, modificazioni dovute all'invecchiamento), o a causa di una difettiva raccolta del campione. Infatti, la specifica acquisizione del campione da compararsi con quello salvato – di solito raccolto in condizioni ottimizzate – può produrre immagini alterate, rendendosi difficile il perfetto accoppiamento (per es. nel caso delle impronte digitali, a causa di un'inadeguata pressione sul sensore, o un posizionamento incorretto delle dita, difetti di illuminazione, movimento troppo veloce ecc.)[15].

Inoltre, il sistema in quanto tale dovrebbe garantire un certo livello di performance in termini di accuratezza e velocità come pure di resistenza alla manomissione[16].

Date tutte queste questioni, le procedure di accoppiamento del campione conservato e di quello raccolto al momento della identificazione includono delle decisioni circa la soglia di somiglianza che deve essere stabilita al fine di salvaguardare la funzionalità nonostante tutte le imperfezioni del caso[17].

Questa soglia può essere fissata più in alto o più in basso con la conseguenza di dover accettare livelli più alti o, rispettivamente, più bassi di erroneo rigetto (FRR, *False Rejection Rate*) o, inversamente, più bassi o più alti livelli di erronea accettazione (FAR, *False Acceptance Rate*)[18].

Di conseguenza, anche nel caso di biometria usata per l'identificazione univoca, si ha propriamente a che fare con inferenze di tipo probabilistico più o meno prone all'errore.

Per migliorare l'accuratezza, può essere usata la c.d. "*multibiometrics*", vale a dire l'uso di sistemi complessi basati su molteplici moduli classificatori o sistemi multimodali di classificazione (per es. che usino sia le impronte digitali che il riconoscimento dell'iride) [19].

In un'era meno tecnologicamente avanzata di quella odierna, l'estrazione biometrica e l'identificazione si risolvevano in procedure piuttosto invasive, difficili, lunghe e prone all'errore umano. Tali procedure, richiedendo la misurazione di tratti corporei, necessitavano della collaborazione consapevole del soggetto o la sua sottoposizione ad atti coercitivi.

Sicché una tale situazione impediva di pensare ad un uso massiccio di tecniche biometriche limitandole a quegli ambiti considerati di maggior valore sociale nei quali è essenziale la massima precisione nei processi identificatori

[15] Per una visione generale delle problematiche tecniche relative alle tipologie di tecniche biometriche più largamente in uso, oltre alla letteratura già citata si veda Das, 2019.
[16] Jain, Ross, Prabhakar, 2004, p. 4.
[17] Malik, Girdhar, 2014.
[18] Fairhust, 2018, cap. 2, §4.
[19] Ross, Jain (2004); Ross, Jain (2006).

(per es. finalità di polizia giudiziaria, o identificazione per motivi di ordine pubblico o di necessità pubblica).

Ma nell'attuale condizione tecnologica, con il diffondersi della presenza di strumenti di datificazione anche nelle situazioni più ordinarie, la possibilità di estrarre dati tratti da caratteristiche fisiche o comportamentali è così ampliata che i "dati biometrici" appaiono essere oggi molto facilmente disponibili. Informazioni sui tratti fisici, sui movimenti, sul colore della pelle, l'altezza, su caratteristiche instabili come la lunghezza e il colore dei capelli, della barba, il vestiario sono tutte immediatamente disponibili in video registrazioni o immagini caricate sul web dagli stessi utenti o da dispositivi sempre più presenti di vigilanza pubblica e possono pertanto essere estratte rapidamente, in maniera non invasiva e, volendo, senza nemmeno che il soggetto ne sia consapevole.

Anche se spesso inidonei per una "perfetta" identificazione univoca, tali dati possono tuttavia essere usati al di fuori di questa tipologia di procedure oppure, anche in quei casi, per integrarle e migliorare l'accuratezza statistica dei sistemi di identificazione. Questo è il caso della cosiddetta *soft biometrics* che oggigiorno appare in grande sviluppo[20].

Nel caso di quella che è stata chiamata la biometria di "seconda generazione", nuovi strumenti e tecniche biometriche danno accesso a una vasta varietà di tratti fisici e comportamentali quali i movimenti oculari, i *pattern* di digitazione o movimento del cursore, caratteristiche dell'andatura, il comportamento online ecc. Grazie a tale materiale, l'accoppiamento statistico può giovarsi di fonti biometriche molto varie che sono collegate in qualche modo a specifici tratti della personalità e possono dimostrarsi rilevanti specialmente quando si tratti di selezionare un *tipo* di soggetto.

3. L'uso di dati biometrici per il reclutamento al lavoro nel diritto Europeo

Oggigiorno le società di reclutamento al lavoro utilizzano strumenti di *big data analytics* per organizzare procedure di selezione che coinvolgono grandi quantità di candidati specialmente per posizioni ordinarie[21].

Le questioni relative alla protezione dei dati in tali situazioni sono assai delicate perché, da un lato, una certa conoscenza della persona è necessaria per valutare il livello di eleggibilità del candidato. Ma, dall'altro, tecniche di *data*

[20] Hassa, Isquierdo, Piatrik 2021. Per applicazioni nell'ambito della c.d. *Internet of* Things, cfr. Tomičić, Grd, Bača, 2018; invece, per situazioni che richiedono autenticazioni continue (p. es. sessioni online) cfr. Garg, Arora, Singh, Saraswat, 2018.

[21] Cfr. Fraij, Várallyai, 2021, per un esame complessivo della letteratura sull'uso dell'Intelligenza Artificiale nel *recruiting*.

mining e di profilazione applicate a grandi quantità di dati possono rivelare molto più di quanto sia necessario, potendo, inoltre, dare accesso a informazioni altamente sensibili la cui conoscenza può condurre a decisioni inique.

Per tali ragioni, le cornici regolatorie spesso adottano un approccio restrittivo al processamento dei dati e tale è il caso, appunto, della legislazione italiana come subito si vedrà.

Fino a poco tempo fa, il reclutamento avveniva principalmente sulla base delle informazioni acquisite dal *curriculum vitae,* colloqui di lavoro e test attitudinali, in altre parole, si trattava di procedure fortemente *human-centric* nelle quali l'esperienza e la conoscenza del settore erano essenziali per la selezione della forza lavoro.

Ma organizzare grandi quantità di richieste in tale maniera appare assai dispendioso in termini di tempo e soprattutto soggetto a idiosincrasie tipiche quali il pregiudizio o la decisione arbitraria con potenziali effetti discriminatori o iniqui[22].

Pertanto, l'utilizzo di tecniche di profilazione basate su ampi *databases* come pure l'ampliamento della tipologia di dati da includere nella elaborazione statistica sono viste come modalità di ottimizzazione dei processi, sebbene, come è noto, gli strumenti di decisione algoritmica debbano essere progettati e "allenati" accuratamente per evitare il rischio di avviare pratiche discriminatorie perfino peggiori, data l'ampiezza della scala di impiego[23].

Recentemente, i *social networks* sono divenuti nuove potenti fonti di informazioni sulle persone da assumersi: tanto *posts* e commenti quanto immagini, video e altre rappresentazioni personali sono così utilizzati sempre di più quali strumenti utili per valutare le persone nell'ambito dell'impiego[24].

Inoltre, la familiarità con cui le giovani generazioni maneggiano videocamere e le tecniche di registrazione video, accompagnata da una scarsa preoccupazione per la resa pubblica di sé e della propria immagine[25], hanno suggerito l'idea di arricchire le richieste di lavoro con delle video presentazioni[26]. Talvolta ai candidati è richiesto di registrare i loro video seguendo specifiche istruzioni (ad esempio rispondendo a domande prestabilite) cosicché ogni futura elaborazione possa trarre vantaggio da comportamenti organizzati secondo certe regolarità[27].

[22] Per quanto importante, la nozione di *fairness* non è affatto chiara. La letteratura più recente sul tema ha mostrato la presenza nel dibattito di numerose definizioni non facilmente riconducibili ad unità coerente, per una panoramica si vedano: Mittlestadt, Allo, Taddeo, Watcher, Floridi 2016, pp. 8-9; Tsamados, Aggarwal *et al.* 2021, p. 7.

[23] Geetha, Bhanu Sree 2018; Nawaz 2019.

[24] Ollington, Gibb, Harcourt (2013.

[25] Bryce, Klang (2009.

[26] Rasipuram, Pooja Rao, Jayagopi 2016.

[27] Cojan, Verzea, Vilcu 2017.

Data la qualità raggiunta ormai da questi strumenti ordinari, un tale materiale apre le porte alla possibilità di usare la biometria per acquisire una più profonda conoscenza del soggetto: ad esempio è possibile utilizzare sistemi biometrici basati sull'Intelligenza Artificiale per quantificare e valutare i comportamenti verbali, paraverbali (ad esempio la velocità del parlato e la qualità della voce) e non-verbali (sorrisi, attenzione visuale) degli intervistati[28].

Al fine di rendere effettive le predizioni sulla idoneità di un candidato a prodursi in buone performance lavorative in un certo contesto, sono disponibili diversi modelli, sebbene il più usato sia il c.d. "Modello a Cinque Fattori" (dall'inglese *FFM, Five-Factors Model*), altrimenti detto, modello "Big Five", nel quale il nucleo di fattori da valutarsi sono:

- *Openness:* la misura del grado in cui un individuo si presenta immaginativo e creativo;
- *Consciousness:* la misura del grado in cui un individuo è organizzato, riflessivo e scrupoloso;
- *Extraversion:* la misura in cui un individuo è energico, assertivo e loquace;
- *Agreeableness:* il grado in cui un individuo è empatico, gentile, e affettuoso;
- *Neuroticism:* la misura della tensione, l'incostanza e l'ansia che un individuo possa manifestare[29].

La recente letteratura sul punto ha mostrato che le *Reti Neurali Convoluzionali* possono essere usate per riconoscere i cinque tratti fondamentali di una persona attraverso l'esame delle espressioni facciali estratte da video *clips,* tali modelli sembrano presentare capacità predittive superiori a quelle di un selettore umano[30].

Data l'importanza che i sistemi di reclutamento basati sull'Intelligenza Artificiale stanno assumendo è fondamentale, perciò, fare il punto sullo stato dell'ordinamento Europeo in materia.

Il GDPR – come è noto - traccia il quadro generale ma per quanto riguarda le norme giuslavoristiche l'idea del legislatore Europeo è stata quella di lasciare più spazio ai diritti nazionali. L'art. 88, infatti, stabilisce che gli stati membri possano utilizzare propri strumenti normativi (legislativi e concertativi) per fornire regole "più precise per assicurare la protezione dei diritti e delle libertà" con riferimento al processamento dei dati dei lavoratori nel contesto di lavoro e in particolare con riferimento al reclutamento […]". Inoltre, il § 2 del medesimo articolo richiede che tali regole includano idonee e specifiche misure di garanzia della dignità umana dell'interessato, del suo

[28] Hickman *et al.*, 2021.
[29] Sueng, Hung, Lin, 2019.
[30] *Ibidem.*

legittimo interesse e dei diritti fondamentali con particolare riguardo alla trasparenza dei processi, al trasferimento dei dati in un gruppo di società controllate o di imprese impegnate unitariamente in una attività economica come pure dei sistemi di controllo nel luogo di lavoro[31].

In tale contesto, quindi, il diritto del lavoro nazionale fungerà da *Lex specialis* con riferimento sia al reclutamento che al rapporto di lavoro.

Oltre all'art. 88, vi sono altre disposizioni del Regolamento Europeo direttamente rilevanti per la protezione dei dati dei lavoratori. Per esempio, lo stesso n. 4 dell'art. 4, nel definire la "profilazione" considera anche le sue applicazioni per analizzare o prevedere (tra le altre cose) anche le performance al lavoro.

Quanto ai dati biometrici, la definizione di questi ultimi si trova nel n. 14 dell'art. 4 GDPR ai sensi della quale essi sono "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

È importante notare che la recente proposta della Commissione per un Regolamento Europeo sull'Intelligenza Artificiale – d'ora in poi "Proposta sull'IA" – appare totalmente in linea con il GDPR per quanto riguarda la nozione di dato biometrico (cfr. Proposta sull'IA, art. 3, n. 33).

Come si può vedere, la stessa nozione giuridica di dato biometrico si compone di tre elementi:

- deve risultare da uno specifico processo tecnologico;
- deve riguardare caratteristiche fisiche o comportamentali di una persona naturale;
- deve confermare o consentire la identificazione univoca di quella persona.

L'art. 9 GDPR, proibisce, dal canto suo, il processamento di dati genetici e biometrici in quanto "intesi ad identificare in modo univoco la persona naturale", includendoli così nel novero dei dati che richiedono particolare protezione assieme a quelli "che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale [...] dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

La proibizione di cui all'art. 9, §1, può essere derogata nei casi indicati al §2 che sono numerosi e complessi.

Prima facie, appaiono rilevanti per il tema del reclutamento le ipotesi sub lett. b) e h)[32]. Anche quelle sub lett. a) potrebbero rilevare nella misura in cui

[31] Art. 88, § 2.

[32] Art. 9, §2, lett. b), GDPR: "il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto

le leggi nazionali siano in linea con il Regolamento nel consentire al libero consenso del lavoratore superare il divieto di cui al primo paragrafo (ciò che non è nel caso italiano).

Entrambi gli articoli (art. 4, n. 14 e 9) trattano esclusivamente di quella che abbiamo chiamato biometria "di prima generazione", vale a dire quella che si serve di dati derivanti da caratteristiche fisiche o comportamentali di una persona con lo scopo di stabilire o verificare univocamente la sua identità.

Sembra, dunque, che *non ogni datificazione di caratteristiche fisiche o comportamentali* si traduca in dati biometrici nel senso specifico di cui al GDPR ma solo quelli che "ne consentono o confermano l'identificazione univoca"[33].

Tale disposizione dovrebbe interpretarsi in un senso *oggettivo* vale a dire avuto riguardo alla tipologia di tratto datificato e allo stato della tecnologia disponibile, per cui, ad esempio, se le impronte digitali, correttamente rilevate, sono *oggettivamente* idonee a stabilire l'identità di una persona, non così può dirsi del taglio di capelli o dell'andatura in sé e per sé considerati.

Inoltre, allorché si sia di fronte a dati biometrici in senso pieno, il *data controller* incontrerà limiti specifici di utilizzo solo quando ricorrano altresì le condizioni di cui all'art. 9 e, nello specifico, che tali dati siano in effetti usati con lo scopo di stabilire l'identità univoca del soggetto. In questa ipotesi, ci si troverà di fronte al divieto generale, potendosi "solo" verificare la possibilità di giovarsi delle deroghe di cui al §2.

Aver ristretto la rilevanza dei dati biometrici a quelli usati dalla biometria "di prima generazione" porta alle seguenti conseguenze:

a. quei dati che devono considerarsi biometrici secondo la definizione di cui all'art. 4, n. 14, ma che *non siano usati* con lo scopo di identificare univocamente la persona cui si riferiscono, sfuggono dalla proibizione di cui all'art. 9 e sono soggetti, pertanto, alle regole generali di liceità del trattamento stabilite dal GDPR;
b. in teoria, il dato fisico o comportamentale che oggettivamente non sia idoneo a consentire o confermare l'identità della persona cui appartenga non è considerato "biometrico" nel senso di cui al GDPR (e, per quanto detto sopra, anche ai sensi della Proposta sull'IA), sicché, nuovamente essi possono essere trattati secondo le regole generali.

---

del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato". La lett. h) dispone che "il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3".

[33] Questo punto è accuratamente e specificatamente discusso in Kindt, 2018.

Questo scenario apparentemente chiaro si complica con l'avvento della *soft biometrics* almeno nelle ipotesi in cui essa, come si è accennato, sia usata nei contesti di identificazione con lo scopo di migliorare l'accuratezza delle procedure statistiche basate sulla biometria *hard.* Qui, in effetti, anche i dati "soft", in un certo senso, contribuiscono all'identificazione, dunque, nel lessico del GDPR, "consentono o confermano" tale possibilità.

Di principio, quindi, tali dati devono considerarsi "biometrici" solo quando effettivamente usati a tale scopo e nella misura in cui, oggettivamente, sono idonei a portare un miglioramento delle procedure di identificazione.

In questo caso, naturalmente, non solo essi rientrerebbero nella nozione di "dato biometrico" ex art. 4, n 14, ma il loro uso specifico per finalità di identificazione si troverebbe anche a dover fare i conti con la proibizione di principio di cui all'art. 9 e, dandosi il caso, con la disciplina in deroga di cui allo stesso articolo.

Al contrario, quando usati per scopi differenti, i dati "soft", pur essendo frutto della datificazione di tratti fisici o comportamentali sarebbero da escludersi sia dalla nozione di cui all'art. 4, n. 14, che, di conseguenza, anche dalla disciplina specifica di cui all'art. 9.

Per quanto riguarda la legislazione sul lavoro, tuttavia, come detto, devono prendersi in considerazione anche le legislazioni nazionali quali sono richiamate sia dall'art. 88 che dall'art. 9, §2, lett. b), sicché la legittimità dell'uso di dati biometrici al fine del reclutamento dovrà essere valutata anche alla luce di queste fonti.

Ora, cosa accade se tali normative (sia legislative che concertative) risultino più restrittive della disciplina generale appena vista?

Prendiamo in considerazione il diritto italiano sul punto, giacché ci presenta esattamente questa ipotesi.

4. Il trattamento dei dati nell'ambito delle procedure di *recruiting* secondo il diritto nazionale.

Giunti a questo punto, è opportuno ricapitolare brevemente i tre elementi fondamentali che sono stati stabiliti dalla discussione precedente in merito al quadro europeo generale sul tema dei dati biometrici:

- se essi non sono oggettivamente idonei a consentire o confermare l'identità univoca di una persona fisica (art. 4, num. 14; ad esempio perché esprimenti una caratteristica priva di elementi di stabilità minimamente sufficienti, ad es. la lunghezza della barba) o anche se lo sono ma non sono usate con tale intendimento (art. 9, §1), il loro processamento non richiede alcuna particolare condizione di legittimità ulteriore rispetto a quelle richieste per il trattamento di dati ordinari. Di conseguenza, e questo è un elemento interessante, non

ogni misurazione fisica o comportamentale offre dati "biometrici" nel senso specifico e tecnico di cui alle definizioni normative. D'altro canto, tali misurazioni possono diventare dati "biometrici" in tale senso se e nella misura in cui "consentono o confermano" l'identificazione univoca;

- al contrario, se i dati sono considerati "biometrici" e sono usati con l'intendimento di procedere all'identificazione univoca della persona fisica, il *data controller* dovrà fare i conti con la disciplina di cui all'art. 9, la quale proibisce tale uso, salvo ricorrano le ipotesi di deroga ivi indicate.

Inoltre, nel caso del diritto giuslavoristico, incluso quello che disciplina la fase di reclutamento, le leggi nazionali possono introdurre una disciplina più specifica per una protezione ulteriore dei diritti del lavoratore.

Ora, sebbene il reclutamento richieda l'identificazione dei soggetti candidati, questa procedura ben potrebbe essere svolta senza l'uso di dati biometrici; in linea di principio, dunque, il reclutamento in sé e per sé costituisce scopo diverso dalla identificazione univoca (sebbene entrambi possano essere realizzati nell'ambito di un medesimo sistema automatizzato complesso, il che renderebbe le cose ancora più complicate), sicché, in linea teorica, l'uso di dei dati biometrici in quest'ipotesi sarebbe al di fuori dalla disciplina di cui all'art. 9 GDPR, per essere, però, esplicitamente compreso nell'ambito del rinvio che l'art. 88 fa al diritto nazionale.

Nel caso del diritto italiano, il processamento di dati dei lavoratori è soggetto a misure assai più restrittive e un tale un approccio è presente anche nei confronti di quei soggetti che si occupano costitutivamente del reclutamento.

Infatti, l'art. 8 dello Statuto del Lavoratori, L. 300/1970 - concepito con lo scopo di proteggere la dignità, la libertà e la confidenzialità dei lavoratori in un'ottica di tutela preventiva – vieta al datore qualsiasi indagine, schedatura, classificazione in relazione alle opinioni politiche, religiose o sindacali e su fatti non rilevanti al fine della valutazione della sua attitudine professionale[34].

Inoltre, ai sensi dell'art. 10 del D. Lgs. 10 settembre 2003, n. 276, è fatto divieto alle "agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro,

[34] Cfr. Rota, 2017.

a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento dell'attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo"

Come si vede, sebbene nessuna di queste disposizioni tratti esplicitamente di biometria, molte tipologie di dati sensibili qui indicate sono tratte da caratteristiche fisiche o comportamentali.

In ogni caso, entrambe adottano un approccio assai restrittivo di principio per quanto riguarda il trattamento dei dati dei lavoratori o dei candidati. Nello stesso tempo, sono alquanto complesse, pertanto proviamo a riassumere i punti principali con riferimento soltanto alle procedure di reclutamento:

- nessun dato sensibile può essere trattato a meno che non si riferisca a una caratteristica che incida sulle modalità di svolgimento della specifica attività o sia un requisito essenziale e determinante per l'attività lavorativa. L'onere della prova grava sul *recruiter* e il consenso eventualmente prestato dal candidato non gioverebbe[35];
- nemmeno i dati non sensibili possono essere processati a meno che essi non siano strettamente connessi con le attitudini professionali dei lavoratori e siano necessari per il loro inserimento al lavoro. In questo caso, il libero consenso è rilevante[36], ma, di nuovo, l'onere della prova rimane a carico del *recruiter*.

Si noti che il divieto di processare dati a meno che non siano strettamente relativi alle attitudini professionali, a rigore, dovrebbe implicare l'impossibilità di utilizzare tecniche di *data mining* idonee a ritrovare indirettamente dati pur utilizzabili a partire da dati non utilizzabili[37]. Ad esempio, nel caso si voglia utilizzare i dati tratti dai movimenti oculari per rilevare caratteristiche della personalità rilevanti per le specifiche competenze richieste. Se per fare ciò il sistema di recruiting intende utilizzare altri dati presi da misurazioni biometriche del volto, questo uso dovrebbe essere considerato illegittimo in

[35] Sicché, l'irrilevanza del consenso impedisce la possibilità di invocare la deroga di cui all'art. 9, § 2, quando si fosse nell'ambito di tale disciplina.

[36] La rilevanza del consenso in questa ipotesi appare in linea con la *litera legis* che, qui, appare diversa dall'ipotesi sopra riferita di dati "sensibili" per la quale il legislatore l'ha *espressamente* esclusa. Tuttavia, l'Autorità Garante per i dati Personali nel § 1.4.1 del "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101**",** accomuna le due ipotesi nel senso di escludere la possibilità che il libero consenso del candidato possa costituire una deroga al divieto in ogni caso.

[37] Per l'ovvia ragione che il *data mining* costituisce già un "trattamento" dei dati in questione. In merito alla nozione, al rapporto con la profilazione e alle criticità del *data mining* si vedano: Sarra, 2019b, pp. 75 ss nonché la copiosa bibliografia ivi citata.

quando tali misurazioni non sarebbero strettamente connesse, nel senso rigoroso di cui alla disposizione.

É interessante notare che, apparentemente, la necessità di inserimento al lavoro di per sé stessa non può essere invocata per aggirare la proibizione. La formulazione della disposizione, infatti, connette tale requisito a quello del collegamento stretto con le attitudini professionali in maniera non alternativa ma cumulativa ("e"). Sicché, la liceità del trattamento dei dati deve essere valutata alla luce del doppio requisito: nessun dato del candidato può essere processato a meno che non sia strettamente correlato alle sue attitudini professionali *e* sia necessario per il suo inserimento al lavoro.

Il che equivale a dire che le agenzie di reclutamento interessate ad usare sofisticate tecniche *hi-tech* per sviluppare il loro business dovrebbero essere pronte a fornire concrete giustificazioni ed evidenze della relazione stretta tra i dati dei candidati che intendano processare come pure della necessità in ragione dello specifico inserimento al lavoro.

Data la relazione tra il quadro generale europeo e il diritto nazionale, dobbiamo concludere che – almeno per l'Italia – lo spazio per l'uso di strumenti di Intelligenza Artificiale con la finalità di *recruiting* sia alquanto stretto[38], e comunque che, laddove siano usati, debba esservi una struttura organizzativa e delle procedure aziendali in grado di fornire giustificazioni e spiegazioni di alto livello circa le modalità di utilizzo dei dati dei candidati[39].

Ma proprio su questo punto, interviene ora la Proposta sull'IA che, come detto, si pone esplicitamente, nelle intenzioni, come complementare con il GDPR[40]. Per quanto riguarda la biometria, la proposta presenta un quadro più complicato trattando di sistemi biometrici di IA che possano essere usati per "il riconoscimento delle emozioni", "l'identificazione remota", "l'identificazione remota in tempo reale"[41], tutti individuati sulla base della medesima definizione di "dato biometrico" di cui al GDPR. A parte i sistemi di "riconoscimento delle emozioni" – che sono "sistemi di IA con lo scopo di identificare o inferire le emozioni o le intenzioni delle persone fisiche sulla base dei loro dati biometrici" (art. 3, n. 34), tutte le altre espressioni si riferiscono a sistemi di IA mirati all'identificazione univoca, sicché essi sono, di nuovo, mezzi sofisticati per praticare la c.d. biometria di "prima generazione".

[38] Pertanto, condivido sul punto le osservazioni di Rota, 2017, p. 39.

[39] Ed è per tale ragione che le nuove regole che la Proposta sull'IA dovrebbe introdurre circa la documentazione, l'analisi del rischio, la gestione dei dati e la vigilanza umana sono della massima importanza.

[40] La complementarità tra il GDPR e la Proposta sull'IA è espressamente indicate dalla Commissione Europea stessa nell'*Explanatory memorandum* che introduce il testo della proposta, cfr. §1.2.

[41] Sui sistemi di identificazione biometrica a distanza e sulle problematiche di diritto costituzionale si veda Mobilio, 2021.

Data la complementarità dei due atti regolativi, nulla di quanto si trova nella Proposta dovrebbe contraddire il quadro stabilito dal GDPR, sicché, la sua lettura non dovrebbe portare a conclusioni differenti. Eppure, l'art. 10, §5, della Proposta sull'IA stabilisce che "nella misura in cui sia strettamente necessario allo scopo di assicurare il monitoraggio, l'individuazione e la correzione di *bias* in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono processare speciali categorie di dati di cui all'art. 9(1) del Regolamento (EU) 201/2016 [...] fornendo adeguate misure di salvaguardia dei diritti e delle libertà fondamentali delle persone fisiche, incluse limitazioni tecniche per il ri-uso e l'utilizzo di misure di protezione della privacy allo stato dell'arte, quali la pseudonimizzazione o la criptazione laddove l'anonimizzazione possa incidere significativamente sullo scopo perseguito"[42].

Perciò, ci si può chiedere: se e quando il nuovo Regolamento sull'Intelligenza Artificiale sarà in vigore, potrà invocarsi l'art. 10, § 5 per l'utilizzo di dati biometrici oltre le limitazioni stabilite dal GDPR e dal diritto nazionale?

5. Coordinamento delle fonti

La Proposta sull'IA consente il trattamento di dati "di cui al par. 1, art. 9 GDPR" - che, come abbiamo visto, contiene la disciplina generale sui dati meritevoli di particolare protezione – al fine di monitorare e correggere eventuali *bias* nel sistema.

In tale articolo sono inclusi anche i dati biometrici (e genetici) ma – a rigore, seguendo la lettera del richiamato art. 9, §1 - solo quando usati con il fine di identificare univocamente una persona fisica.

Come pure abbiamo visto, quando tale non è lo scopo del processamento, a rigore, i dati biometrici non godono di una protezione ulteriore rispetto al quadro generale. Inoltre, quando essi consistano in misurazioni fisiche o comportamentali ma non "consentono o confermano" l'identificazione, secondo le definizioni stesse di cui all'art. 4 GDPR, essi non sono nemmeno "biometrici" e, nuovamente, ricadranno nella disciplina generale sulla protezione dei dati personali.

Il panorama normativo europeo, dunque, sebbene discutibile, appare coerente: a) i dati che derivino da misurazioni fisiche o comportamentali possono essere trattati purché ricorrano le condizioni di legittimità stabilite in generale nonché siano adempiuti tutti gli altri adempimenti previsti in generale; b) essi possono essere, utilizzati, in questo contesto, anche per il controllo e la correzione dei *bias* di sistema; c) i dati biometrici che non siano

[42] La Proposta sull'IA classifica esplicitamente come "sistemi ad alto rischio" quelli dedicati al *recruitment*, si veda l'Annex III, §1, n. 4.

usati col fine di identificare univocamente la persona fisica seguono le medesime regole; d) il trattamento dei dati biometrici che siano, invece, usati a tale scopo, incontrerà la proibizione generale di cui all'art. 9, e potrà essere svolto solo nei casi in deroga di cui al §2. A tali deroghe dovrebbe, dunque, aggiungersi quella di cui all'art. 10, §5 della Proposta sull'IA, se e quando sarà approvata, che consente l'utilizzo di tali dati per il monitoraggio e la correzione dei *bias* di sistema.

L'art. 9, § 2, lett. b), introduce una possibile deroga alla proibizione generale di cui al § 1 nel caso in cui il trattamento sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato".

Ma, per quanto riguarda i dati biometrici, questa disposizione deroga solo al divieto di cui al §1 che si riferisce a dati utilizzati per procedure di identificazione univoca, non per il reclutamento di per sé solo.

Questo significa che, quando si ha a che fare con sistemi di identificazione univoca, l'uso di dati biometrici è proibito, a meno che non ricorra una delle deroghe di cui al §2, e, nel caso del reclutamento, la deroga di cui al §2, lett. b) può consistere nel Regolamento sull'IA, una volta che sia approvato, trattandosi di un atto di diritto dell'Unione.

D'altro canto, questo non pare incidere sulla disciplina restrittiva di diritto nazionale del lavoro che, come si è visto, trova la sua legittimità nel rinvio ad essa da parte dell'art. 88 GDPR, anche quando si tratti di dati biometrici, nella misura in cui essi non siano, si ripete, usati per finalità di identificazione univoca.

Come già ricordato, l'art. 88 GDPR consente al diritto nazionale giuslavoristico, inclusa la contrattazione collettiva, di agire quale *lex specialis* così derogando il quadro generale per una maggiore protezione dei lavoratori.

Tale articolo non risulta menzionato né, quindi derogato, dall'art. 10, §5 della Proposta sull'IA.

Pertanto, in conclusione, l'uso di dati biometrici per il reclutamento, anche per il controllo e la correzione dei *bias* di sistema è soggetto alla medesima disciplina restrittiva eventualmente disposta dalla legislazione nazionale. Nel caso italiano, ad esempio, tutto ciò che si è detto circa le potenziali limitazioni all'uso di sistemi di IA nel reclutamento appare doversi mantenere anche nel caso in cui sia approvata la proposta sull'IA, a meno che non subisca modificazioni sul punto (per esempio prevedendosi esplicitamente che il

trattamento indicato per finalità di controllo e correzione dei *bias* di sistema possa avvenire in deroga anche all'art. 88 GDPR).

Certamente corrisponde ad un interesse del candidato quello di essere selezionato attraverso procedure prive di *bias,* sicché questo elemento potrà essere preso in considerazione nella valutazione dell'attinenza al suo "inserimento lavorativo" (art. 10 del D. Lgs. 10 settembre 2003, n. 276) ma, come si è detto, questo elemento costituisce solo la metà dell'onere probatorio gravante sull'agenzia di reclutamento che intenda utilizzare procedure avanzate di trattamento dei dati.

6. Conclusioni

Il fatto che non ogni misurazione fisica o comportamentale sia considerata meritevole di una protezione particolare nel contesto del GDPR può lasciare perplessi. L'amplissima diffusione di strumenti idonei a registrare immagini di persone fisiche, sia da parte di privati per ragioni di intrattenimento e socializzazione che da parte pubblica per ragioni di sicurezza, e l'alta probabilità che tali registrazioni disponibili nel Web possano essere utilizzate può lasciare l'impressione di aver ormai perduto ogni sostanziale dimensione di "*privacy* informazionale" [43].

I dati biometrici erano un tempo di scarsa disponibilità e difficili da estrarre senza la consapevole collaborazione del soggetto o un atto di coercizione su di lui.

Questo ha portato a collegare le misurazioni biometriche a utilizzi particolarmente importanti quali quelli di identificazione univoca per gravi ragioni oppure per ragioni mediche, ad esempio.

Ma il fatto che oggi dati estratti da caratteristiche fisiche o comportamentali possano essere recuperati e collazionati molto facilmente senza alcuna collaborazione da parte del soggetto, senza nemmeno che costui lo sappia, non rende tali operazioni prive di invasività, al contrario. Il controllo remoto e le misurazioni sono comunque manipolazioni dell'immagine personale che costituisce una diretta proiezione degli elementi primari dell'auto consapevolezza di sé del soggetto. Sicché, escludere dalla protezione speciale e perfino dalla stessa nozione giuridica di "dati biometrici" quelle misurazioni fisiche o comportamentali che non siano collegate immediatamente a pro-

[43] Ricorda Luciano Floridi che vi sono almeno quattro definizioni possibili di *privacy* nel contesto contemporaneo: fisica, mentale, informazionale e decisionale. La *privacy Informazionale* è definita come "freedom from informational interference or intrusion", cfr. Floridi (2014), p. 103.

cedure di identificazione univoca, può far apparire la disciplina del GDPR, oggi, troppo tollerante.

Val la pena notare che il GDPR stesso riposa su una tensione – che riflette la comprensione attuale del problema – tra la libera circolazione dei dati e la protezione della persona umana[44]. Il *chiasmo assiologico* di cui all'art. 1, è un sintomo di questa tensione irrisolta. Il §3 di tale articolo, infatti, invertendo l'ordine dei valori fondamentali tutelati dal Regolamento secondo il primo comma dello stesso articolo, dispone che "La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"[45].

Questa tensione giustifica molte scelte regolatorie introdotte da questo importante atto normativo. Per esempio, l'efficacia, forse eccessivamente ampia, attribuita al consenso dell'interessato considerando lo sproporzionato potere in gioco nelle relazioni che costui intraprende con le grandi società dell'informazione che sono ormai intermediari pressoché necessari per lo svolgimento delle sue incombenze quotidiane.

Anche la visione generale della relazione tra i soggetti protagonisti della vicenda dei dati presupposta dal GDPR appare obsoleta. L'immagine di fondo è ancora quella di un soggetto in una sorta di "posizione naturale" nel pieno controllo del "pacchetto" di dati che lo riguardano, che affida a (o non si oppone a che) altri li processi, in forza di diritti e obblighi reciproci e sotto la supervisione di autorità pubbliche di garanzia.

Ebbene, oggigiorno la presupposizione di una tale "posizione naturale" si configura come un'astrazione di livello troppo elevato per mantenere un'adeguata capacità descrittiva e su cui basare una regolazione davvero tutelante.

La permanenza di queste due problematiche principali rischia di minare anche l'idoneità della Proposta sull'IA – che in quel quadro esplicitamente si inserisce - di offrire una chiara e sicura disciplina per quel che si dice una IA "sostenibile".

Il caso del reclutamento è emblematico. Da una parte, nuovi sviluppi tecnologici nell'analisi biometrica, specialmente "soft", rivelano grande poten-

[44] E secondo l'analisi proposta in Kindt, 2018, la disciplina Europea sui dati biometrici non è in grado di fornire un corretto bilanciamento tra questi due valori.

[45] Tale disposizione non costituisce una novità, essa è presente in termini sostanzialmente identici sia nella vecchia Direttiva 95/46/CE (art. 1), che nella Direttiva 2016/680 (art. 1, §2, lett. b) sulla Protezione dei dati personali da parte delle autorità competenti nell'ambito di attività di prevenzione, indagine, accertamento e perseguimento dei reati o l'esecuzione penale. La tensione tra i valori della protezione della persona e la circolazione dei dati è strutturale alla impostazione generale del diritto dell'Unione.

zialità per un inserimento al lavoro sempre più mirato; dall'altro lo *status* complicato di tali dati da interpretarsi tra l'approccio tollerante del GDPR e le restrizioni delle leggi nazionali (ove vi siano) lascia sia i candidati che le agenzie di reclutamento in una incertezza problematica.

Ce n'è abbastanza per augurarsi una decisa riconsiderazione del tema biometrico molto oltre quello dell'uso per finalità di identificazione univoca, come pure di quello del diritto all'immagine di sé che sia inteso includere tutte le possibili proiezioni simboliche della persona, siano esse "pittoriche" o no.

Bibliografia

Alfrink, K., Keller, I., Kortuem, G. *et al.* (2022). 'Contestable AI by Design: Towards a Framework' in *Minds & Machines*. https://doi.org/10.1007/s11023-022-09611-z

Almada, M. (2019). 'Human intervention in automated decision-making: Toward the construction of contestable systems' in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law*, 2–11. ICAIL '19. Montreal, QC, Canada: Association for Computing Machinery.

ART29WP (2018). '*Guidelines on Automated individual decision-making and Profiling for the Purposes of Regulation 2016/679*', last Revised and Adopted on 6 February 2018.

Bryce, J. & M. Klang (2009). 'Young people, disclosure of personal information and online privacy: Control, choice and consequences' in *Information Security Technical Report* 14, 3:160-166.

Brkan, M. (2019). 'Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond' in *International Journal of Law and Information Technology* 27, n. 2: 91–121.

Bygrave, L. A. (2019). 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' in *SSRN Scholarly Paper.* Available at https://papers.ssrn.com/abstract=3329868.

Comitato Nazionale di Bioetica (2010). *L'identificazione del corpo umano. Profili bioetici della biometria.* 26 novembre 2010.

Cojan, M., Verzea, I., & A. Vilcu (2017). 'An introductory guide to self-presentation for professional purposes in a video format' in *eLearning & Software for Education*, 1: 363-369.

Das, R. (2019). *The Science of Biometrics.* New York: Routledge.

De Hert, P. & V. Papakonstantinou. (2016). 'The New General Protection Regulation: Still a Sound System for the Protection of Individuals?' in *Computer Law and Security Review* 32: 179-194.

Fairhurst, M. (2018). *Biometrics: A Very Short Introduction.* Oxford: Oxford University Press.

Floridi, L. (2014). *The Fourth Revolution.* Oxford: Oxford University Press.

Fraij, J., Várallyai, V. (2021). '*A Literature Review: Artificial Intelligence Impact on the Recruitment Process'* in *International Journal of Engineering and Management Sciences* 6, 1:108-119.

Friedman, B. & Nissenbaum, H. (1996). 'Bias in Computer Systems' in *ACM Transactions on Information Systems* 14, 3: 330–347.

Garg, R., A. Arora, S. Singh & S. Saraswat (2018). 'Biometric Authentication using Soft Biometric Traits' *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*: 259-264, doi: 10.1109/PDGC.2018.8745766.

Geetha, R. & D., Bhanu Sree Reddy (2018). 'Recruitment through Artificial Intelligence: A conceptual study' in *International Journal of Mechanical Engineering and Technology* 9, 7:63-70.

Hassan, B., Izquierdo, E. & Piatrik, T. (2021). 'Soft biometrics: a survey'. *Multimed Tools Appl* (2021). https://doi.org/10.1007/s11042-021-10622-8.

Hickman, L., Bosch, N., Ng, V., Saef, R., Tay L. & S.E. Woo (2021). 'Automated video interview personality assessments: Reliability, validity, and generalizability investigations' in *Journal of Applied Psychology* 107, 8:1323-1351.

Jain, A.K., Ross, A., Nandakumar K. (2011). *Introduction to Biometrics.* Cham: Springer International Publishing.

Jain, A. K., Ross, A., Prabhakar, S. (2004). '*An Introduction to Biometric Recognition*' in *IEEE Transactions on Circuits and System for Video Technology* 14, 1:4-20.

Kindt, A. J. (2018). 'Having yes, using no? About the new legal regime for biometric data' in *Computer Law and Security Review* 34:523-538.

Malik, J. & D. Girdhar (2014). 'Reference Threshold Calculation for Biometric Authentication' in *I.J. Image, Graphics and Signal Processing* 2: 46-53.

Mendoza, I., & L. A. Bygrave. (2017) 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (eds.) *EU Internet Law: Regulation and Enforcement*, 77–98. Cham: Springer International Publishing.

Mittelstadt, B. D., P. Allo, M. Taddeo, S. Wachter, & L. Floridi (2016) 'The Ethics of Algorithms: Mapping the Debate' in *Big Data & Society* 3, n. 2:1-21.

Mobilio, G. (2021). 'I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale' in *Consulta Online* III: 738-748.

Mordini, E., Tsovaras D. & H. Ashton (2012). 'Introduction', in Mordini, E. & D. Tsovaras (eds.) *Second Generation Biometrics: The Ethical, Legal and Social Context,* 1-19. S.l.: Springer.

Mordini, E. & D. Tsovaras (2012). Mordini, *Second Generation Biometrics: The Ethical, Legal and Social Context.* S.l.: Springer.

Nawaz, N. (2019). 'How Far We Come With The Study of Artificial Intelligence for Recruitment Processes' in *International Journal of Scientific & Technology Research* 8, 7:488-493.

North-Samardzic, A. (2020). 'Biometric Technology and Ethics: Beyond Security Applications' in *Journal of Business Ethics* 167, 3: 433–450.

Ollington, N., Gibb, J. & Harcourt, M. (2013), 'Online social networks: an emergent recruiter tool for attracting and screening' in *Personnel Review* 42, 3:248-265.

Rasipuram, S., Pooja Rao S. B., & D. B. Jayagopi (2016). 'Asynchronous video interviews vs. face-to-face interviews for communication skill measurement: a systematic study' in *Proceedings of the 18th ACM International Conference on Multimodal Interaction (ICMI '16). Association for Computing Machinery,* 370–377.

Roig, A. (2018) 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' in *European Journal of Law and Technology*, 3: 1-17.

Ross A. & A. K. Jain (2004). 'Multimodal biometrics: An overview' *2004 12th European Signal Processing Conference,* 1221-1224.

Ross A. & A. K. Jain (2006). 'Multimodal Human Recognition', in Bum R. S. & Z. Liu (eds) *Multi-Sensor Image Fusion and Its Applications,* 289-302. Boca Raton: Taylor & Francis.

Rota, A. (2017). 'Rapporto di lavoro e big data analytics: profili critici e risposte possibili' in *Labour and Law Issues* 3, 1:33-52.

Sarra, C. (2020). 'Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design in: Global Jurist' in *Global Jurist*, doi: https://doi.org/10.1515/gj-2020-0003

Sarra, C. (2020a). 'Defenceless? An Analytical Inquiry into the Right to Contest Fully Automated Decisions in the GDPR' in D. A. Frenkel, A. Chronopoulou (eds), *An Anthology of Law,* 235-252. Athens: ATINER.

Sarra, C. (2019). 'Data Mining and Knowledge Discovery. Preliminaries for a Critical Examination of the Data Driven Society', in *Global Jurist* 20, 1:1-12.

Sarra, C. (2019b). *Il Mondo Dato. Saggi su datificazione e diritto.* Padova: Cleup.

Smith, M., Miller, S. (2021). *Biometric Identification, Law and Ethics.* Cham: Springer.

Tomičić, I., Grd, P. & M. Bača (2018). 'A review of soft biometrics for IoT' *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*: 1115-1120, doi: 10.23919/MIPRO.2018.8400203.

Tsamados, A., Aggarwal N., Cowls, J., Morley, J., Roberts, H., Taddeo, M. & L. Floridi (2021). 'The ethics of algorithm: keys problems and solutions' in *AI & Society,* https://doi.org/10.1007/s00146-021-01154-8.