Intelligenza artificiale, strumenti di identificazione e tutela dell'identità

Edoardo C. Raffiotta, Massimiliano Baroni*

ARTIFICIAL INTELLIGENCE, IDENTIFICATION TOOLS AND IDENTITY PROTECTION

ABSTRACT: The essay starts from the consideration that the new frontiers of the AI are forcing the jurist to rethink the fundamental categories of personal identity and identification. Today, these categories are characterised by greater fluidity and interchangeability: identification relies on data, while the analysis of big data makes it possible to trace the (digital) identity of each individual. In this complex scenario, the EU appears to be driven by the will to build an anthropocentric protection system. That is made possible through what is identified in the contribution as an equilateral triangle whose sides are cybersecurity, data protection, and AI regulation. After a brief examination of the current regulatory framework, the essay analyzes two case studies that illustrate the opportunities/criticalities inherent in the relationship between AI and personal identity. In conclusion, the question arises as to what the frontiers of the next AI regulatory framework might be.

KEYWORDS: AI; personal identity; identification; big data; anthropocentrism.

SOMMARIO: 1. Premessa. Fondamento costituzionale del (diritto alla) identità personale. La distinzione giuridica tra identità e identificazione – 1.2. Internet, identificazione e identità: come la diffusione del digitale ha contribuito a sfumare i contorni giuridici del fenomeno. – 2. Dall'informazione al dato: come (e perché) cambiano le vie di tutela – 2.1. Direttiva NIS; Article 4(1) GDPR: personal data identification, identifiability, re-identification); EU Proposal: un modello triangolare di protezione e tutela, tra identità digitale, strumenti di identificazione e limiti giuridici – 3. Case study: il caso TikTok. identificazione, identità e sistemi di age verification "AI-based": non ci sono alternative? – 4. Case study: il riconoscimento facciale nei luoghi pubblici – 5. Intelligenza artificiale, identificazione, identità: le prospettive di regolazione alla luce della Proposta di Regolamento. Verso un *algorithmic social contract*?

* *Edoardo C. Raffiotta, Professore associato presso il Dipartimento di Scienze Economico-Aziendali e Diritto per l'Economia dell'Università di Milano Bicocca. Mail: edoardo.raffiotta@unimib.it; Massimiliano Baroni, PhD Student in Diritto costituzionale, Università degli Studi di Parma. Mail: massimiliano.baroni@unipr.it.* *Il presente lavoro è frutto della collaborazione fra i due autori; tuttavia si deve a E. C. Raffiotta la redazione dei paragrafi nn. 1, 1.2, 3, 4; e a M. Baroni la redazione dei paragrafi nn. 2; 2.1, 5. Contributo sottoposto a doppio referaggio anonimo.*

ISSN 2284-4503

1. Premessa. Fondamento costituzionale del (diritto alla) identità personale. La distinzione giuridica tra identità e identificazione

«Sapere dove è l'identità è una domanda senza risposta» scriveva José Saramago. Parafrasando il premio Nobel portoghese, parrebbe utile chiedersi non tanto dove è ma, piuttosto, dove *va* l'identità (e, soprattutto, dove andrà nel prossimo futuro).

Quello di identità personale è un concetto – pur se non inedito – mutevole ed *in parte qua* inafferrabile: Aristotele vi ricollegava la nozione di *hypokeimenon* (sostanza); la dottrina cristiana ne rivela sovente le similarità con l'anima; mentre da Locke in poi sarà il criterio psicologico a prendere il sopravvento[1] nei confronti del criterio fisico quale ipotetico mezzo di definizione dell'identità personale. Sul piano giuridico, ben più recentemente, l'identità personale è stata fatta coincidere con il «diritto a non vedere travisare la propria personalità individuale»[2] e, soprattutto, con «l'interesse, ritenuto generalmente meritevole di tutela giuridica, [a che ciascuno sia] rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta»[3]. Un diritto, dunque, di per sé meritevole di tutela ed in grado di oltrepassare le colonne d'ercole rappresentate dagli artt. 7 e 10 del codice civile, rispettivamente posti a tutela del diritto al nome e del diritto all'immagine: mentre questi attengono, invero, all'*identificazione* (intesa come possibilità – per gli altri – di procedere a identificare un soggetto come quella persona, specificamente individuata), l'identità può indicarsi come elemento caratterizzante della persona[4], parte integrante – quasi colonna portante – di quest'ultima, strumentale al pieno sviluppo dell'individuo e perciò meritevole di riconoscimento in Costituzione[5]. L'identità rappresenta, in estrema sintesi, l'immagine della persona, a sua volta composta in modo binario: da un lato la considerazione che l'individuo ha di sé stesso, dall'altro ciò che la società vede nell'individuo, formandone la proiezione sociale.

Questi sono, altresì, i termini in cui la stessa Corte costituzionale ha riconosciuto il fondamento di un diritto all'identità personale. Dopo quasi un decennio dal "caso Veronesi", tramite il quale fece la propria comparsa nell'ordinamento la nozione di identità personale come «formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni»[6], e complice anche il successo riscosso – nelle more – dall'interpretazione "a fattispecie aperta" dell'art. 2 Cost.[7], con la sent. n. 13/1994 la Consulta incluse a pieno titolo, tra i diritti

[1] Tra esperimenti e modifiche: *ex multis* si v., tra i contemporanei, il pensiero di Shoemaker.

[2] Così Pretura di Roma, 6 Maggio 1974, unanimemente riconosciuto come primo caso giurisprudenziale relativo all'identità personale.

[3] Cass. Pen. n. 3769/1985, c.d. "caso Veronesi". Sul punto sia altresì consentito il rinvio a C. DOMENICALI, M. BARONI, *Identità personale in internet: il diritto all'oblio e la deindicizzazione sui media online,* in A. MORRONE, *Il diritto costituzionale nella giurisprudenza*, VIII ed., Milano, 2020.

[4] Così già E.C. RAFFIOTTA, *Appunti in materia di diritto all'identità personale*, in *Forum di quaderni costituzionali*, 2010.

[5] Più diffusamente, in prospettiva analogica, si v. L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 2004.

[6] Cass. Civ., n. 3769/1985.

[7] Oggi comunemente accettata, eppure già terreno di numerosi e prolifici confronti dottrinari. *Contra*, *ex multis*, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984 nonché A. PACE, *Il c.d. diritto alla identità personale e gli art. 2 e 21 della Costituzione*, in G. ALPA, M. BESSONE, L. BONESCHI, *Il diritto alla identità personale*, Padova, 1981.

componenti il «patrimonio irretrattabile della persona umana», quello all'identità personale, intesa come il «diritto ad essere sé stesso», alla luce dell'insieme di convinzioni, opinioni ed esperienze che qualificano ogni individuo (rendendolo, in definitiva, ciò che *è* e *sente* di essere)[8]. Veniva così inaugurata una stagione di apertura nei confronti del (diritto alla) identità personale che (attraverso altre pronunce della Corte, *ex multis* la nota 297/1996, la n. 120/2001 o la n. 494/2002, e più recentemente la n. 278/2013, la parimenti nota 221/2015 o la n. 180/2017) permetteva di arricchire e precisare il contenuto del diritto, così ampliandone e rendendone più efficace la tutela (offrendo altresì una sponda alle evidenti difficoltà definitorie incontrate dal legislatore).

Identificazione e identità sarebbero dunque concetti collegati, eppure separati.

Gli strumenti di identificazione – quali un nome[9], una voce – esulano (almeno formalmente, *ndr*) dall'identità propriamente detta, essendo naturalmente circoscritti ad un ambito prima di tutto fisico e materiale, legato all'esteriorità. Lo stesso potrebbe dirsi, esemplificativamente, per un indirizzo, o un numero di telefono: informazioni (prima ancora che "dati") non richiedenti una dimensione digitale e, soprattutto, utilizzabili per la mera identificazione di un soggetto[10].

D'altro canto, è identità il risultato non solo – non tanto – di un'attività identificativa, ma – anzi – di un'opera di ricostruzione della personalità individuale, corrispondente al sopracitato insieme degli elementi caratterizzanti una persona (anche intellettualmente; e dunque privilegiando la dimensione dell'interiorità): in tal senso, l'identità non può che rappresentarsi come un *quid pluris* rispetto alla (mera) identificazione, richiedendo – per tale motivo – una tutela *ad hoc*, previa un'interpretazione necessariamente estensiva dei segni di identificazione che, come si dirà, oggi più di allora travalicano i propri tradizionali confini, ben potendo interferire con la protezione dell'identità individuale.

Si rileva, tra l'una e l'altra, un rapporto di strumentalità (conoscere l'identità implica una previa identificazione) ed al contempo di reciprocità (regolamentare i mezzi di identificazione come garanzia dell'identità; garantire l'identità per proteggerne le singole componenti) che tuttavia non parrebbe intaccarne le vicendevoli differenze.

1.2. Internet, identificazione e identità: come la diffusione del digitale ha contribuito a sfumare i contorni giuridici del fenomeno.

Certamente così poteva dirsi, almeno, sino a qualche decennio fa. Attualmente, infatti, il quadro generale si mostra estremamente più complesso, articolato, indefinito, principalmente per effetto dell'inarrestabile diffusione di internet (in forza del quale hanno fatto altresì il loro ingresso nell'ordinamento il diritto all'oblio – oggi normativamente previsto dall'art. 17 GDPR, ma nelle sue proto-forme già introdotto con Cass. nn. 3679/1998 e 5525/2012, cui ha fatto seguito il *leading case* Google Spain

[8] Esemplificativa, in tal senso, i più recenti sviluppi – giurisprudenziali e *a fortiori* culturali – in tema di identità sessuale.

[9] Più diffusamente sul rapporto tra nome, identificazione e identità si v. anche CGUE C-208/09, *Ilonka Sayn-Wittgenstein c. Landeshauptmann von Wien*.

[10] Impone invece riflessioni più complesse – come si vedrà nel prosieguo – il volto.

– e alla deindicizzazione)[11]. Alle singole componenti di un'informazione si è sostituito il dominio del dato (*rectius*: dei *big data*), e ciò obbliga il giurista a ripensare i concetti tradizionali sopra menzionati, rendendo più difficoltoso distinguere tra identità e identificazione. Da un lato, quest'ultima non richiede più – oggi – un nome o un'immagine, né tantomeno la necessità di collegare l'uno all'altra, ben potendosi identificare qualcuno sulla mera base delle "tracce" disseminate online (a partire dall'indirizzo IP, tramite cui è possibile identificare il luogo fisico – nonché lo strumento tecnico – di accesso a internet). Ancora maggiore è tuttavia il cambiamento registratosi in termini di identità personale, a mente della considerazione per cui ogni nostra azione su internet viene – per il tramite di algoritmi e, da ora in poi sempre più, di intelligenze artificiali – raccolta, processata, analizzata ed infine interpretata affinché, unita con gli altri dati disponibili, possa offrire uno spaccato della personalità di ciascun utente, sin nelle sue componenti più intime. In breve, della sua *identità*. Così, i caratteri fondamentali che tradizionalmente compongono l'identità personale – orientamento sessuale, convinzioni religiose, idee politiche – subiscono una duplice trasformazione: da un lato perdono il proprio carattere di unitarietà, divenendo invece frazionabili e leggibili (come un nome, un'immagine, un indirizzo: quelli che tradizionalmente erano meri strumenti di identificazione); mentre dall'altro lato acquistano una rilevanza tale da espandere la nozione stessa di identità personale oltre i confini del mondo reale, tanto che l'identità digitale acquista una *sua* identità, non di rado indipendente dalla dimensione fisica.

Addirittura, la più attenta letteratura ricorda come i colossi digitali possiedano una quantità tale di informazioni, relative ad ogni utente della rete, che rende loro possibile non solo indirizzare bensì anche prevedere – con certezza pressoché assoluta – le preferenze individuali, creando una società dell'anticipazione[12] in cui, sostanzialmente, le *Big Techs* non si limiterebbero a "leggere" il comportamento dei propri utenti, ben potendo invece aprioristicamente indirizzarlo[13].

Ancora, e sempre in tema di identità personale, non possono dimenticarsi le implicazioni pratiche del cambiamento: là dove vi era un'informazione analogica, per sua natura soggetta al trascorrere del tempo e dunque precaria, oggi vi è un dato cristallizzato e parcellizzato, potenzialmente eterno nella propria immutabilità e scollegato da ogni evento esterno (con effetti tutt'altro che trascurabili all'atto della (ri)costruzione dell'identità personale, specie con riferimento al diritto ad essere dimenticati).

Qualche anno fa ci si chiedeva[14] dove collocare il *discrimen* tra tutela dell'identificazione della persona online e della sua identità personale attraverso internet: oggi può certamente affermarsi che l'esito più evidente della transizione digitale consiste in un'alterazione dei rapporti tra le tradizionali categorie di identificazione e identità personale, i cui confini vanno inevitabilmente sfumandosi, rendendo più

[11] Per cui, da ultimo, si vv. le linee guida dell'European Data Protection Board, alla luce anche di CGUE C-507/17, *Google Inc. c. CNIL* (che ha come noto definito – limitandolo – l'ambito di applicazione del diritto alla deindicizzazione). EDPB, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, 7 Luglio 2020.

[12] A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019.

[13] Compie un ulteriore passo E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, London, 2012, che – nel coniare ed illustrare il concetto di filter bubble – evidenzia come gli algoritmi di motori di ricerca e social network creino una realtà a misura di utente, assecondando le preferenze – e le convinzioni – di questi.

[14] E.C. Raffiotta, *Appunti in materia di diritto all'identità personale*, cit.

ISSN 2284-4503

difficoltoso distinguere dove inizi l'una e finisca l'altra; ovvero – e a maggior ragione – quando un determinato dato afferisca all'una o all'altra dimensione individuale.

2. Dall'informazione al dato: come (e perché) cambiano le vie di tutela

La quantità di informazioni attualmente in circolazione e, soprattutto, il crescente valore commerciale delle stesse ha condotto, come noto, ad una *società dell'informazione*, caratterizzata – come da alcuni acutamente pronosticato – dal crescente valore della conoscenza (tanto che, scriveva Lyotard, «la questione del sapere nell'era dell'informatica è più che mai la questione del governo»). Oggi, il sapere ha la forma del *dato*. Anche quest'ultimo, come l'*informazione* di analogica memoria, ha un valore commerciale, ed anche questo – come la sua controparte analogica – cela al proprio interno una notizia. Terminano qui, tuttavia, le similarità. Invero, in chiara discontinuità rispetto al passato, il dato cresce in valore tanto più quanto il medesimo viene condiviso (anche per il suo essere, notoriamente, un bene inesauribile)[15]. Soprattutto, la naturale vocazione del dato è quella di abbracciare l'identificazione come l'identità, potendo essere utilizzato sia per arrivare alla prima che per ricostruire la seconda (e la scelta, naturalmente, risiede nelle mani – *rectius*: nei software, e nella volontà – del possessore del dato).

Non stupisce allora l'attenzione riservata dal legislatore – nazionale nonché, in via prioritaria, europeo – alla disciplina del dato e specificamente, per ovvi motivi di tutela, del dato personale, definito all'art. 4 del Regolamento 679/16 come «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[16] ed esteso, *ex multis*, agli indirizzi IP (statici prima – CGUE C-70/10 – dinamici poi – CGUE C-582/14)[17], oltre che – più generalmente – ad *ogni* informazione in grado di condurre, anche indirettamente, all'identificazione del soggetto interessato (CGUE C-434/16)[18]. Ciò che maggiormente rileva è, invero, l'idoneità di quel determinato dato a fungere da strumento identificativo del soggetto; un soggetto che – a conti fatti – si trova in una posizione aprioristicamente debole[19], esposta alla pervasività delle tecniche digitali e delle intelligenze artificiali di raccolta ed analisi dai dati (in grado, come detto, di ricostruire l'identità di un utente tramite le operazioni di aggregazione dei c.d. *big data*, così da delinearne un profilo composto da preferenze, idee, abitudini, convinzioni).

[15] A.F. FONDRIESCHI, *A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorithmic Data Processing under the GDPR*, in *Oss. Dir. Civ. e Comm.*, 2, 2019.

[16] Mentre «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (art. 4 (1) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016).

[17] CGUE C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)*, 24 Novembre 2011; e CGUE C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 Ottobre 2016.

[18] C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 Dicembre 2017, in cui la Corte ha stabilito che «*the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data*». Nel corpo della decisione viene, altresì, espressamente richiamato il caso Breyer (per cui anche C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Juscivile*, 2/2020).

[19] R. MESSINETTI, *Comunicare nell'infosfera. La vulnerabilità della persona digitale*, in *federalismi.it*, 18, 2021.

Coerentemente con l'approccio tipico dell'Unione[20], il legislatore di Bruxelles è dunque da tempo orientato ad una disciplina non tanto e non solo a garanzia del dato in sé, quanto piuttosto ad una protezione del dato in funzione strumentale alla tutela individuale. È ormai noto, infatti, che la mole di dati disponibili in rete possa essere processata solo tramite intelligenze artificiali, capaci di operare in condizioni di *insights-overload*. Se però il futuro è diviso tra *big data* e *AI*, gli interrogativi si moltiplicano e si fanno più pressanti: qual è il confine tra attività umana e trattamento *AI-based*? Come elaborare metodi e tecniche di controllo sull'attività di un'intelligenza artificiale sempre più intelligente e, ben lungi dall'essere mero esecutore di pre-impartite istruzioni, già ora capace di *imparare* nuove abilità? In altri termini, la zona grigia tra le opportunità del *deep learning* e le criticità delle *black boxes* è destinata a rimanere una *no-fly zone* per il diritto? Le domande si affastellano, ed ogni tentativo di fornirvi risposta ci consegna un diritto sovente costretto ad inseguire l'ordine spontaneo[21] dell'evoluzione tecnologica (tanto da essersi paventato il rischio di una *disruption* del giuridico)[22].

2.1. Direttiva NIS; Article 4(1) GDPR: personal data (identification, identifiability, re-identification); EU Proposal: un modello triangolare di protezione e tutela, tra identità digitale, strumenti di identificazione e limiti giuridici.

Non può che salutarsi con favore, *rebus sic stantibus*, il percorso intrapreso dall'UE, manifestamente orientato alla costruzione di una griglia di strumenti di tutela *ex ante*, i cui capisaldi sono senza dubbio da individuarsi in tre differenti regolamentazioni, tra loro interconnesse: *cibersecurity* (da ultimi, la direttiva NIS e il Cybersecurity Act)[23]; *data protection* (GDPR, naturalmente), e *artificial intelligence* (con la Proposta di Regolamento recentemente presentata dalla Commissione)[24].
Un triangolo equilatero, in cui ogni lato è funzionale all'effettività del *framework* regolatorio complessivo (*simul stabunt*, *simul cadent*) e per effetto del quale identificazione e identità appaiono come crocevia sul quale convergono gli interessi di diversi settori della riflessione scientifica odierna[25].
Solo un background digitale adeguatamente sicuro può garantire un'autentica protezione dei dati personali, degli interessati, nonché in definitiva della loro identità. Ne è ben consapevole il *Cybersecurity Act* che – pur non espressamente menzionando identificazione e identità digitale – ricorda[26] come «l'economia dei dati e l'Internet degli oggetti possono prosperare solo se i cittadini sono convinti che

[20] A differenza, invece, di quanto accade in altre esperienze giuridiche: si v., da ultimo ed esemplificativamente, il caso cinese; solo recentemente interessato dall'entrata in vigore – a far data dal 1 Novembre 2021 – della prima legge sui dati personali (pur se con alcune differenze sostanziali, tra cui esemplificativamente una maggiore discrezionalità governativa circa la possibilità di far riferimento ad interessi di sicurezza nazionale).
[21] *Ex multis* l'opera di Friedrich August von Hayek.
[22] G. MOBILIO, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal*, 2, 2020. Più diffusamente, del medesimo A., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.
[23] Direttiva (UE) 2016/1148; Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).
[24] *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on. Artificial Intelligence (artificial intelligence act) and amending certain union legislative acts*.
[25] E.C. RAFFIOTTA, *Appunti in materia di diritto all'identità personale*, cit.
[26] Considerando n. 65, Reg. 2019/881, *cit*.

tali prodotti, servizi e processi offrono un determinato livello di cibersicurezza»: rendendo evidente, così, la *ratio* delle due principali innovazioni introdotte dal Regolamento (sistema europeo per le certificazioni di cybersicurezza e potenziamento dell'ENISA, che non a caso «coopera con le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali»)[27]. Il GDPR è, invece, dichiaratamente orientato alla protezione dell'identità e alla tutela dell'identificazione secondo – pare potersi riassumere – due direttrici fondamentali: da un lato si rileva il tentativo del legislatore UE di minimizzare il rischio di furto, usurpazione o «altre forme di abuso» dell'identità[28], dall'altro la volontà di incentivare l'anonimizzazione dei dati in quanto buona pratica in grado di impedire l'identificazione del soggetto persona fisica cui i dati si riferiscono (sottraendoli, così, al campo applicativo del Regolamento medesimo)[29]. Un'ulteriore conferma, insomma, di come in campo digitale la distinzione tra identificazione e identità vada sfumando, anche sul piano strettamente normativo. Compie un ulteriore passo avanti la Proposta di Regolamento sull'intelligenza artificiale, che canalizza l'attenzione legislativa sulla nozione (non di *dato*, bensì) di *dato biometrico*, oltre che (non di mera *identificazione*, bensì) di *identificazione biometrica a distanza*. Appartengono alla prima categoria i «dati personali risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che permettono o confermano l'identificazione unica di tale persona fisica, come le immagini facciali o i dati dattiloscopici»[30], mentre si qualifica come *identificazione biometrica a distanza* quella procedura che consenta di identificare un soggetto sulla base di alcuni suoi tratti distintivi senza richiedere la fisica interazione uomo - macchina (dunque l'immagine di un volto *in primis*, ma anche andatura, espressioni facciali, comportamento somatico). Un concetto, si noti, che pur se già introdotto nel GDPR (considerando 51, che invero identifica una fotografia in un dato biometrico quando venga trattata tramite un «dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica»), trova solo nell'intelligenza artificiale la propria specifica disciplina, poiché è solo con l'AI che può inaugurarsi la sottoponibilità delle caratteristiche *fisiche* di una persona a trattamenti (*real-time* o *ex post*) indipendenti dall'umano (e dunque esposti alle note criticità, in termini di definizione giuridica del dato e delle tipologie di dati, spiegabilità dei processi di elaborazione, oltre che con riferimento ai dilemmi – anche etici[31] – circa l'affidabilità dell'AI e il *range* di autonomia decisionale della medesima).

Il quadro così composto permette, in ogni caso, di porre alcuni punti fermi circa lo stato dell'arte del framework normativo in tema di identità e identificazione digitale. Schematizzando, infatti, si osservano in via prioritaria:

[27] Art. 7, comma 2

[28] Considerando nn. 75, 85, 88 GDPR, che dunque offre all'identità digitale una protezione a sé stante, indipendente dall'identità fisica (pur rimanendovi, naturalmente, strettamente connessa).

[29] Considerando n. 26, che esclude l'applicazione del Regolamento per «informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato»; considerando n. 30, per cui gli identificativi online «possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche». artt. 4 e art. 5.

[30] Considerando art. 3 (33) della Proposta.

[31] Per una recente panoramica U. RUFFOLO, *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Milano, 2020.

a) un innovativo – e gradito – protagonismo dell'Unione, intenzionata a stabilire una leadership globale, e soprattutto a farlo con un "approccio europeo"[32]. Tali iniziative sono inoltre il segno evidente di come il futuro della regolamentazione giuridica non possa prescindere, su temi come quelli d'interesse, né da un impianto sovranazionale (e, in particolare, glocale) – né tantomeno dal confronto tra sviluppi scientifico – tecnologici e scienze sociali[33] (*ubi societas*, *ibi ius*);

b) la compresa necessità, anche tra i banchi europei, di rinnovare il diritto delle fonti, adottando un'impostazione umanocentrica per default e utilizzando strumenti normativi rispondenti ad un paradigma flessibile, sussumibili nelle ipotesi concrete tramite un approccio caso per caso (fortemente *risk-based*)[34];

c) un approccio multidisciplinare (e, per ora, spiccatamente trilaterale: *cybersecurity*, *data protection*, *AI*) al mondo digitale.

Più in dettaglio, inoltre:

d) una lettura estensiva – tanto a livello normativo quanto, e ancor di più, giurisprudenziale – dei *key-concepts* di dato (e dato biometrico), identità (analogica, e digitale), identificazione (in termini di astratta riconducibilità dell'informazione all'interessato, nonché quale forma di protezione della sua identificabilità – come persona fisica – e nella sua identità);

e) l'ampio uso del sistema delle *certificazioni*, per testare (e attestare)[35] il rispetto dei requisiti di sicurezza e legittimità del trattamento (art. 57 Reg. 2019/881; art. 42 GDPR; art. 44 Proposta Reg.), ingenerando fiducia in cittadini, consumatori e mercato[36];

---

[32] Commissione Europea (COM (2021)), *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Promuovere un approccio europeo all'intelligenza artificiale*, 24 Aprile 2021.

[33] A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, 1, 2019.

[34] Come noto, la Proposta di Regolamento sull'AI introduce invero una classificazione di astratta pericolosità dei prodotti facenti uso di software *AI-based* sulla base del rischio di un impatto negativo delle operazioni su diritti fondamentali, distinguendo tra quattro diverse fasi di rischio e corrispondenti limiti d'uso (Prop. Reg., artt. 5; 6; 52).

[35] Anche fissando standard minimi di trattamento e protezione dei dati, che possano superare il modello *consent-based*. Sul punto A. MANTELERO, *La* privacy *all'epoca dei* Big Data, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, ove si evidenzia che «il consenso è sempre meno, in concreto, strumento di reale autodeterminazione. Anzi, paradossalmente, quest'ultimo può divenire la soluzione più agevole per raccogliere dati per le finalità più disparate, stanti i limiti che affliggono sia lo strumento dell'informativa sia la reale libertà di scelta», come ricorda S. SCAGLIARINI, *La tutela della* privacy *e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta Online*, II/2021, che con riferimento ad Immuni scrive di una «lettura del canone di libertà del consenso» eccessivamente prudente, non proporzionale al vantaggio che ne sarebbe altrimenti potuto derivare in termini di tutela della salute. Il tema del consenso, e della utilità/veridicità del medesimo, compariva già in S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, in cui l'A. sosteneva che il consenso non fosse una "scelta reale", prevedendo giocoforza come unica alternativa l'esclusione dall'utilizzo del servizio. La giurisprudenza europea non è comunque priva di tentativi volti a rendere maggiormente effettivo il consenso (da ultimo CGUE, C-61/19, *Orange România SA contro Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, che ha tra le altre cose ribadito la non efficacia di un consenso pre-flaggato dal fornitore del servizio).

[36] Vale la pena ricordare G. PITRUZZELLA, *L'applicazione delle regole di concorrenza a livello locale e globale: istanze di tutela, sfide ed opportunità*, V Convegno Antitrust di Trento, 16-18 Aprile 2015, in *osservatorioantitrust.eu*, per cui «un'economia di mercato dinamica e competitiva produce risultati positivi non solo sotto il profilo strettamente economico, ma anche sotto quello sociale poiché in grado di determinare il prevalere nella società di

f) il crescente rilievo – il ruolo strategico[37] – delle autorità di controllo indipendenti, dotate di strumenti (regolamentari e sanzionatori), e di capacità (interpretativo-giurisprudenziali) specificamente disegnati per garantire una tutela uniforme sul territorio dell'Unione;
g) la volontà di creare un argine alla pervasività delle nuove tecnologie artificiali, abbracciando nozioni di identificazione e identità inclusive di ogni loro parziale manifestazione (sotto forma di dati, *ndr*) oltre che di ogni complesso significato (ricostruibile a partire da quei dati: identità sessuale, identità biologica, identità online come proiezione dell'entità fisica).

3. Case study: il caso TikTok. Identificazione, identità e sistemi di age verification "AI-based": non ci sono alternative?

Inizialmente fondato con il nome di *musical.ly*, il social network attualmente denominato TikTok ha conosciuto in brevissimo tempo un successo dirompente, in grado di garantirgli a Settembre 2021[38] 1 miliardo di utenti attivi su base mensile, la maggior parte dei quali compresi nella fascia di età 10-19 anni[39].
Nel Gennaio 2021, tuttavia, il social network di estrazione cinese è divenuto tristemente noto ai media italiani per il tragico incidente occorso ad una bambina palermitana di 10 anni, deceduta per soffocamento in seguito – pare – ad un tentativo di emulazione di una *challenge* (una sfida) popolare sulla piattaforma. Immediata la reazione del Garante per la protezione dei dati, che – data la giovanissima età della vittima – decideva di accelerare il proprio intervento nei confronti del social[40], operando in via d'urgenza e disponendo nei confronti del popolare sito – con apposito Provvedimento datato 22 Gennaio 2021[41] – il blocco immediato dell'uso dei dati degli utenti per i quali non fosse stata accertata con sicurezza l'età anagrafica (invero, ai sensi del Codice per la protezione dei dati personali, l'età minima valida per esprimere il proprio consenso al trattamento è fissata in 14 anni: limite al di sotto del

inclusione, creatività, soddisfazione e sviluppo individuale». Sul punto si v. anche la *Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale (2018/2088(INI))*, ove si specifica che «la crescente integrazione della robotica nei sistemi umani richiede un orientamento strategico deciso quanto al modo in cui massimizzare i benefici e minimizzare i rischi per la società, nonché garantire uno sviluppo sicuro ed equo» dell'AI.

[37] F. FAINI, *Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico*, in *BioLaw Journal*, 1/2019.

[38] https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok. Solo a Settembre 2020 gli utenti attivi erano circa 500 milioni: una crescita del 200% in un anno.

[39] https://backlinko.com/tiktok-users (dati relativi al mercato USA).

[40] Si v. la *nota n. 47853* del 15 dicembre 2020, con cui vengono rilevate dal Garante criticità, oltre che dal punto di vista della questione anagrafica menzionata, «sotto il profilo della corretta base giuridica applicata al trattamento dei dati personali dei suoi utenti, delle modalità di rilascio dell'informativa, del trasferimento dei dati all'estero, del periodo di conservazione dei dati, del rispetto dei principi di privacy by design e by default». Meno noto è che, invero, già nel Dicembre 2020 il Garante aveva avanzato plurime contestazioni a TikTok, facenti riferimento alle «forme previste per verificare l'età anagrafica degli utenti medesimi con evidente riferimento, in particolare, ai minori».

[41] Garante per la protezione dei dati personali (GPDP), *Provvedimento del 22 gennaio 2021 [9524194]*, su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb- display/docweb/9524194. Il Provvedimento è stato reso noto il giorno stesso tramite apposito comunicato (Garante per la protezione dei dati personali (GPDP), *Tik Tok: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco dei social*, su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb- display/docweb/9524224).

quale dovrebbe intervenire il soggetto esercente la potestà sul minore)[42]. Tre le ragioni del provvedimento (comunque adottato, come precisato dal Garante medesimo, in via cautelare): l'art. 24, par. 2, della Carta dei diritti fondamentali dell'Unione europea, per cui «in tutti gli atti relativi ai minori, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere considerato preminente»; il considerando 38 del GDPR, in forza del quale «i minori meritano una specifica protezione relativamente ai loro dati personali in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti» (specie in caso di servizi forniti loro direttamente); ed infine l'art. 25, paragrafo 1, del GDPR, che impone al titolare del trattamento di «implementare adeguate misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati al fine di soddisfare i requisiti del Regolamento e per proteggere i diritti degli interessati» (a nulla rilevando l'eventuale dichiarazione mendace dell'utente che abbia dichiarato *ab initio* un'età maggiore di quella reale, *ndr*: diverse interpretazioni non potrebbero infatti che apparire contrarie al principio di *accountability*)[43]. La Società ha successivamente reso noto che si sarebbe resa *compliant* con quanto richiesto dal Garante italiano, dicendosi decisa a riservare il proprio servizio ai soli ultratredicenni (come invero da termini d'uso della stessa piattaforma), essenzialmente[44] utilizzando a tal fine – anche tramite un apposito tavolo di confronti con la *privacy authority* irlandese (ove la società ha il proprio stabilimento principale) – strumenti di *age verification AI-based*. Che la scelta del colosso digitale sia ricaduta sull'AI conferma non solo l'estrema familiarità dell'azienda verso tale tecnologia[45], quanto anche – e piuttosto – come il tema dell'identificazione e dell'identità digitale si ponga, quasi in via emblematica, al centro dell'equilatero composto da cybersicurezza, protezione dei dati e trattamento biometrici dei medesimi. Ben potendo dunque prestarsi a terreno fertile per qualche preliminare considerazione. In primo luogo, il caso ha mostrato alcune evidenti debolezze

[42] Art. 2-quinquies *(Consenso del minore in relazione ai servizi della società dell'informazione)*. - 1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. L'articolo del Codice – novellato dal D. Lgs. 101/2018 – è da leggersi in coordinamento con l'art. 8 GDPR, che fissa la soglia del consenso ad anni 16, pur prevedendo la possibilità per i singoli Stati di stabilire soglie inferiori purché non inferiori ad anni 13.

[43] Per un'applicazione giurisprudenziale maggiormente dettagliata del principio di *accountability* si v. CGUE (C-3111/18), c.d. *Schrems II*.

[44] Tra le ulteriori misure annunciate dalla Società, oltre al citato tavolo di lavoro: una campagna di sensibilizzazione diretta ai propri giovani utenti; una rivisitazione dell'informativa; l'introduzione di un pulsante tramite cui segnalare agevolmente gli account di coloro che parrebbero avere meno di 13 anni.

[45] Per una panoramica tecnica sul funzionamento dell'AI in Tik Tok si vv. D. TREHAN (a firma di), *The inescapable AI algorithm: TikTok*, su *Towards Data Science*, 2020 e M. RANGAIAH (a firma di), *What is TikTok and How is AI Making it Tick?*, su *Analytic Steps*, 2020, ove si specifica – citando Connie Chan – che "*TikTok is the first mainstream consumer app where artificial intelligence IS the product. It´s representative of a broader shift*". Un esempio di software per l'*age verification AI-based* è la startup britannica Yoti, che dichiara un margine di errore di +/- 1 anno: il sistema sarebbe già impiegato in alcuni supermercati in Estonia per la verifica dell'età alle casse automatiche e da una piattaforma di intrattenimento per adulti tedesca.

dell'impianto normativo attuale, su tutte il sistema del *one stop shop*[46]: la cooperazione (e non, dunque, il mero coordinamento) tra le *authorities* dell'Unione diviene innegabilmente essenziale per una protezione efficace[47]. Condivisibile, altresì, la decisione del Garante, riservatosi di accertare l'efficacia delle misure adottate: potrebbe ipotizzarsi, allora, l'estensione degli strumenti di verifica *ex post*, oltre che dei poteri d'indagine dell'autorità garante[48]. Infine, se da un lato certamente l'apporto dell'AI è da ritenersi in buona sostanza indispensabile quando vi sia in gioco una simile mole di dati, e posto che la scelta di una compagnia di agire tramite AI non pare aprioristicamente da contrastare, è ipotizzabile prevedere anche l'utilizzo di altri sistemi, meno invasivi? Alcune proposte sono già state avanzate[49], e l'introduzione di un "doppio binario" potrebbe costituire un compromesso tra esigenze aziendali di rapida identificazione e obblighi di protezione dell'identità.

4. Case study: il riconoscimento facciale nei luoghi pubblici

L'impiego dell'intelligenza artificiale, come accennato, è spesso orientato al perfezionamento dei sistemi di riconoscimento facciale. Ne sono prova, d'altronde, gli smartphone di ultima generazione, capaci di leggere i dati biometrici dell'utente in condizioni di luce parziale, o addirittura di buio, persino quando si abbia una mascherina sul volto[50].

Quello del riconoscimento facciale è invero un campo di estremo interesse, per gli attori privati come per le pubbliche autorità. Gli uni possono contare sui *Big data* e, guidati naturalmente da obiettivi commerciali volti alla massimizzazione del profitto, su una mole di informazioni sconosciuta persino agli Stati. Non di rado le seconde rivelano invece, a ben vedere, una posizione ambigua: divise tra la volontà di porsi quali baluardi a difesa dei diritti della persona (proprio in contrasto ai nuovi sovrani privati)[51], e – dall'altro lato – la tentazione di utilizzare le promesse dell'identificazione tramite AI come mezzo di contrasto alle minacce all'ordine pubblico (il che potrebbe facilmente portare a scoperchiare

[46] In forza del quale è notoriamente competente, dal punto di vista sanzionatorio in primis, l'autorità garante del Paese ove ha sede il fornitore del servizio: nel caso specifico (ed invero per tutte – o quasi – le Big tech, come anticipato, l'Irlanda).

[47] E in tal senso paiono potersi salutare con favore le due indagini recentissimamente aperte dal garante irlandese nei confronti della Società, attualmente pendenti.

[48] Per i quali, ad oggi, si v. art. 58 GDPR (che prevede, tra le altre cose, la possibilità per l'Autorità di chiedere che le venga fornita "ogni informazione di cui necessiti", potendo condurre indagini "sotto forma di attività di revisione sulla protezione dei dati" (Art. 58, 1 (a) e (b)).

[49] S. QUINTARELLI (a firma di), *TikTok, così accerta l'età ed esclude i bambini: gli strumenti utilizzabili*, su *Agenda Digitale*, 24 Gennaio 2021, che propone l'utilizzo di un «meccanismo di controllo con una attestazione indiretta», che imponga al minore di richiedere un token di autenticazione SPID o numero di carta di pagamento ad un maggiorenne (il quale naturalmente nel fornire la citata autenticazione si assumere ogni responsabilità circa il consenso all'uso dell'applicazione da parte del minore). Sul punto si segnala come anche Sandra Zampa, sottosegretario alla Salute, abbia successivamente proposto un sistema di autenticazione dell'identità dei minori tramite SPID (su https://www.privacyitalia.eu/sandra-zampa-divieto-di-smartphone-ai-bimbi-anche-spid-per-i-social/14745/).

[50] Apple sembra avervi trovato soluzione con la release di iOS 14.5, consentendo l'unlock del FaceID dell'iPhone tramite Apple watch.

[51] «Chi sono i sovrani?» si chiede Gaetano Azzarriti (G. AZZARRITI, S. DELLAVALLE, *Crisi del costituzionalismo e ordine giuridico sovranazionale*, Napoli, 2014); mentre – pur se con sfumature differenti – si deve a M. LUCIANI, *L'antisovrano e la crisi delle costituzioni*, in *Riv. dir. cost.*, 1/1996, la nozione di Antisovrano.

il vaso di Pandora, rischiando – nel travalicare il punto di non ritorno[52] – di confondere protezione con repressione, terrorismo con attivismo).

La L. 205/2021, legge di conversione del decreto-legge 139/2021 («Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali»), ha previsto[53], tra le altre cose, la sospensione sino al 31 Dicembre 2023 dell'installazione e dell'utilizzazione in luogo pubblico di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici[54], in considerazione della necessità di una disciplina adottata per legge[55] (trattandosi evidentemente di tema implicante un necessario bilanciamento tra differenti interessi e principi, non ultimo quello di proporzionalità ex art. 52 della Carta di Nizza). Fanno eccezione i trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali.

Il punto non è banale e merita un approfondimento: nel 2018, invero, il Garante si esprimeva favorevolmente all'utilizzo di un sistema automatico di ricerca dell'identità di un volto presente in un'immagine all'interno di una banca dati (il noto SARI), ritenendo che l'identificazione tramite dati biometrici in parola costituisse «un mero ausilio all'agire umano»[56]. Ebbene, diverso è stato invece l'orientamento del Garante in ordine al SARI Real-Time: la possibilità di un siffatto scrutinio in tempo reale non potrebbe infatti contare su alcuna valida base giuridica legittimante, come invece richiederebbe la «forte interferenza con la vita privata»[57] rappresentata da un tale sistema, *a fortiori* considerando che si sarebbe trattato di un trattamento automatizzato su larga scala, in grado di riguardare «anche coloro che siano presenti a manifestazioni politiche e sociali», dunque potenzialmente rivelatore di dati – quali convinzioni politico – sindacali e religiose – sensibili.

Anche l'attività del Garante nel caso (*rectius*: nei casi) "SARI" permette e impone alcune considerazioni. Si tratta, innanzitutto, di problematiche in relazione alle quali il bilanciamento *case by case* richiede

[52] F. RESTA, O. POLLICINO, *Riconoscimento facciale e protezione dati: attenzione al punto di non ritorno*, in *Diritti Comparati*, 30 Gennaio 2020 (in cui emerge tra le altre cose anche il problema del consenso – per cui *supra* – qui indicato come asimmetria informativa foriera di «servitù volontarie» nei confronti dei fornitori di servizi digitali).

[53] Testo coordinato del D.l. 139/2021, in GU n. 291 del 7/12/2021. Capo IV, *Disposizioni urgenti in materia di protezione dei dati personali*, art. 9, comma 9.

[54] Come, tra l'altro, si era inizialmente ipotizzato – altresì – in sede europea, durante le consultazioni che hanno successivamente portato al *White Paper on Artificial Intelligence*.

[55] «*Fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023*», art. 9, *cit*. In questi termini già l'emendamento 9.500 (testo 2), Senato della Repubblica XVIII Legislatura, *Fascicolo Iter DDL S. 2409*, 21/11/2021. Del tema si è recentemente occupata anche la rivista online Wired, su *wired.it*, L. Carrer (a firma di), 19 Novembre 2021.

[56] «…avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato», GPDP, *Sistema automatico di ricerca dell'identità di un volto* -26 luglio 2018 [9040256], 26 Luglio 2018.

[57] GPDP, *Parere sul sistema Sari Real Time -25 marzo 2021 [9575877]*, 25 marzo 2021. Recentemente il Garante si è inoltre espresso favorevolmente all'utilizzo delle c.d. *body cam* da parte del Ministero dell'Interno e dell'Arma dei Carabinieri, purché prive di tecnologie di *facial recognition* (GPDP, 9698442, 10 Settembre 2021). Coerentemente, la Proposta di Regolamento indica l'identificazione biometrica remota in real-time come «*particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights*». 2021/0106 (COD) Proposal, *Considerando n. 28*.

una inedita sensibilità, costituendo il paradigmatico caso in cui l'utilizzo della medesima tecnologia potrebbe rappresentare – come precisa il Centre for European Policy Studies[58] – *both a blessing and a curse*. Ne pare ben consapevole il Consiglio d'Europa quando precisa che il riconoscimento facciale non può essere utilizzato in ambienti incontrollati, al solo scopo di carpire dati che possano condurre all'identità dell'interessato[59]: l'esistenza di una valida motivazione (ed il conseguente scrutinio di legittimità) assurgono dunque, come è stato efficacemente sintetizzato[60], al rango di vero e proprio diritto (si noti inoltre come analoghe problematiche emergano naturalmente anche in prospettiva comparata, *a fortiori* in Paesi le cui autorità pubbliche fanno da tempo uso dell'AI: ne è un esempio paradigmatico l'India, la cui Corte Suprema si è di recente pronunciata sulle condizioni di legittimità del sistema – *Aadhaar* – adottato dalla più popolosa democrazia del pianeta per identificare tramite dati biometrici i propri cittadini)[61]. Lo stesso EDPS aveva d'altronde chiesto – e poi ribadito – un *ban* sui sistemi di identificazione biometrica da remoto nei luoghi pubblici[62]. Altresì, ai tempi del riconoscimento biometrico la distinzione tra identificazione e identità assume le fattezze di una china estremamente scivolosa: il volto dell'individuo è infatti – nella società dell'informazione, tra capitalismo della sorveglianza[63] e *dataveglianza*[64] – il segno d'identificazione per eccellenza, attraverso cui collegare un nome a un volto, ma – anche – conoscere le idee politiche o – di più – comprendere lo stato d'animo di una persona[65]. Trasformare (non le azioni, bensì) le *espressioni* in dati, implica il superamento dell'identificazione, arrivando al cuore dell'identità personale intesa come insieme di convinzioni, pensieri e sentimenti qualificanti ogni soggetto come un *unicum* (cade, insomma, il più importante baluardo di tutela individuale)[66].

[58] CEPS, *Artificial Intelligence and cybersecurity. Benefits and perils*, su www.ceps.eu, 2021.

[59] «*For the sole purpose of determining a person's skin colour, religious or other belief, sex, racial or ethnic origin, age, health or social status to be prohibited*», Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Convention 108: Guidelines on facial recognition*, 28 gennaio 2021. Citato anche da F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021.

[60] C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE Online*, 3, 2020, che tuttavia ne parla con specifico (ma, potrebbe dirsi, non preclusivo) riferimento alla giustizia (per cui anche F. DONATI, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1, 2020).

[61] *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors*, 24 Agosto 2017.

[62] EDPS, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, 23 Aprile 2021.

[63] Ormai nota espressione riconducibile a S. ZUBOFF, *The Age of Surveillance Capitalism*, London, 2019. Più di recente si v. anche D. LYON, *La cultura della sorveglianza. Perché la società del controllo ci ha reso tutti controllori,* Roma, 2020.

[64] P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, 2020.

[65] M. MURGIA (a firma di), *Emotion recognition: can AI detect human feelings from a face?*, in *Financial Times*, London, 12 Maggio 2021.

[66] Non a caso la Proposta di Regolamento qualifica tale tipo di identificazione biometrica («*for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data*») come «ad alto rischio». 2021/0106 (COD) Proposal (Article 3(34)).
Più diffusamente sul tema si v. anche G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.

Nell'identificazione biometrica, potrebbe quasi dirsi, si confondono *habeas data* e una nozione letterale di *habeas corpus*, dato che il corpo diviene – egli stesso – dato, aprendo le porte del foro individuale interno.

Infine, come anticipato, sul campo dell'identificazione personale e dell'identità si giocherà, nessun dubbio in merito, la partita del futuro tra nuove forze private e potere pubblico, obbligando quest'ultimo a riformare le proprie tecniche di produzione del diritto per cercare, ammesso che non sia già troppo tardi – di riscrivere le regole fondamentali della grammatica giuridica[67] e, così, recuperare (parte della) propria rappresentanza politica.

5. Intelligenza artificiale, identificazione, identità: le prospettive di regolazione alla luce della Proposta di Regolamento. Verso un algorithmic social contract?

L'art. 3 della Proposta di Regolamento considera sei differenti tipologie di sistemi *AI-based*: ad una descrizione, potrebbe dirsi, generale e onnicomprensiva di *artificial intelligence system* (art. 3 (1)) fanno infatti seguito le definizioni di *emotion recognition system* ((art. 3 (34))[68]; *biometric categorisation system* (definito – art. 3 (35)[69] – come un sistema non solo capace di ma specificamente designato per classificare gruppi di soggetti in categorie o gruppi – sociali, economici, razziali – comuni); nonché di identificazione biometrica remota, a distanza e senza una previa conoscenza in tal senso da parte del soggetto – dei soggetti – identificati, art. 3 (36): quest'ultima categoria di *AI-based system* viene ulteriormente distinta dalla Proposta in sistemi operanti in *real-time* (art. 3 (37))[70] o in differita (*'post' remote biometric identification system'*, art. 3 (38))[71]. Ogni tipologia di sistema viene classificata in base al rischio che il relativo utilizzo implica per i diritti fondamentali degli interessati. Da tale suddivisione discende, conseguentemente, la concreta ammissibilità o meno delle operazioni di trattamento dei dati biometrico-identificativi, oltre alla fissazione dei limiti di legittimità del medesimo: i sistemi in grado di influenzare e distorcere in via subliminale il comportamento individuale sono *in toto* vietati; quelli ad alto rischio richiedono necessariamente una previa valutazione di stretta conformità e, poi, il rispetto di stringenti requisiti obbligatori; mentre viene richiesto il rispetto degli standard minimi di sicurezza ed affidabilità ai sistemi implicanti un rischio limitato o minimo.

---

[67] F. MUSELLA, *Legge e amministrazione digitale. Lo spazio conteso della regolazione pubblica*, in *Diritto e nuove tecnologie tra comparazione e interdisciplinarità*, *Rivista del Gruppo di Pisa*, 3/2021. Del resto, pur se con una differente sfumatura, anche CGUE C-507/17 ha contribuito ad evidenziare ancora una volta quanto la territorialità del diritto presti il fianco alla vocazione globale del digitale.

[68] «*emotion recognition system 'means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data*».

[69] «*biometric categorisation system 'means an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data*».

[70] «*real- time'remote biometric identification system 'means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention*».

[71] «*post 'remote biometric identification system 'means a remote biometric identification system other than a 'real- time 'remote biometric identification system*».

D'altronde, la pur breve analisi diacronica dell'evoluzione concettuale che ha investito i modelli tradizionali di identificazione e identità, alterandone la disciplina in profondità, ha contribuito ad appalesare le difficoltà metodologiche con cui giocoforza il diritto si confronta durante ogni tentativo d'interpretazione di una società in perenne – e rapidissimo – movimento. Anche per tale ragione, allora, è pienamente condivisibile l'approccio, *made in* Bruxelles, spiccatamente *risk-based*; potendosi – solo così – aspirare ad una regolamentazione adattiva (*adaptive*), capace di resistere allo stress definitorio che l'evoluzione artificiale impone e imporrà alle menzionate categorie.

Certamente, l'AI del futuro dovrà essere quanto più possibile un'AI *explainable* (che, dunque, compia un passo ulteriore rispetto alla mera interpretabilità degli *output* algoritmici)[72]. Quando invece adottare soluzioni XAI non sarà possibile, l'intelligenza artificiale dovrà necessariamente essere sicura e *trustworthy*[73], in grado cioè di ingenerare fiducia nei cittadini (che ne sono invero utilizzatori ed al contempo destinatari designati).

Tutto ciò vale, *a fortiori*, quando vengano in considerazione concetti – come quelli di identificazione e identità personale – da un lato particolarmente permeabili al decorso del tempo, all'evoluzione tecnologica e al mutamento della sensibilità collettiva, dall'altro comunque imprescindibilmente legati alle garanzie costituzionali (dunque, immutabili) della persona. Aree, dunque, la cui disciplina giuridica deve avere come faro il rapporto tra individui, solamente *mediato* dalle macchine (e non, invece, dalle stesse sostituito né controllato). Recente letteratura scrive, in proposito[74], di un *algorithmic social contract*, orientato ad un modello istituzionale basato sull'interazione tra umani e algoritmi di *governance*, integrato da meccanismi per negoziare i valori dei vari stakeholder interessati dai sistemi di AI e, in definitiva, monitorare il rispetto dell'accordo: certo è che, come ricordato[75] in una nota congiunta a firma European Data Protection Board – European Data Protection Supervisor, *a lot of work remains to be done*.

[72] Sul punto si v. anche *Orientamenti etici per un'IA affidabile*, Commissione Europea, Aprile 2019.

[73] M. TADDEO, T. MCCUTCHEON, L. FLORIDI, *Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword*, in *Nature Machine Intelligence*, n. 1, 2019 distinguono tra *reliance* e *trust*, evidenziando come la "fiducia" diverga dal cieco e acritico - dunque intrinsecamente pericoloso - affidamento.

[74] I. RAHWAN, *Society-in-the-loop: programming the algorithmic social contract*, in *Ethics Inf. Technol*, Massachusetts Institute of Technology (MIT), Cambridge, 2018.

[75] EDPB- EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 Giugno 2021.