*Dipartimento di Giurisprudenza*

*Cattedra di Metodologia della scienza giuridica*

# LE TECNICHE DI RICONOSCIMENTO FACCIALE: LA NECESSITA' DI UN BILANCIAMENTO TRA SICUREZZA E TUTELA DEI DIRITTI FONDAMENTALI. QUESTIONI GIURIDICHE E FILOSOFICHE.

**RELATORE**

Chiar.mo Prof.

Antonio Punzi

**CORRELATORE**

Chiar.mo Prof.

Filiberto E. Brozzetti

**CANDIDATA**

Francesca Venditti

Matricola n. 133303

ANNO ACCADEMICO 2022/2023

*A mia sorella Serena,*

*l'altra parte della mia Anima.*

*Ti prometto che in questa vita vivrò per due.*

# INDICE

## CAPITOLO TERZO

## *LAW IN ACTION*: LE TRF AL VAGLIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

**CAPITOLO QUARTO**

**DAL *PANOPTICON* BENTHAMIANO AL PANOTTICO DIGITALE: LA SOCIETA' DELLA SORVEGLIANZA**

# INTRODUZIONE

Nonostante le comprensibili resistenze, è ormai chiaro che il futuro stia andando sempre più nella direzione dell'Intelligenza Artificiale e degli algoritmi. Negli ultimi anni, sono evidenti gli innumerevoli benefici apportati dall'Intelligenza Artificiale, che sta rivoluzionando il nostro modo di vivere, di lavorare, di rapportarci all'Altro e probabilmente anche di pensare. Stiamo già vivendo nel futuro, quando pensiamo che macchine e *software* sempre più intelligenti e sofisticati sono in grado di guidare autonomamente i veicoli, di eseguire con successo attività sempre più complesse, di archiviare quantità enormi di dati in spazi ridotti e così via[1]. Insomma, la rivoluzione tecnologica *in fieri* ci ha catapultato direttamente nel futuro.

Senza dubbio, complice l'incremento del settore biometrico, una delle tecnologie maggiormente innovative e versatili, in quanto presenta il non trascurabile vantaggio di poter essere applicata nei più svariati ambiti, è costituita dal riconoscimento facciale (d'ora in avanti anche TRF), che consiste nel «trattamento automatizzato di immagini digitali che contengono volti di persone, ai fini di verifica/autenticazione, identificazione o categorizzazione»[2]. Dunque, è bene sottolineare sin da ora, per evitare fraintendimenti in chi legge, che le c.d. "videocamere intelligenti" non costituiscono *sic et simpliciter* un sistema di riconoscimento facciale, dovendosi verificare volta per volta la sussistenza delle summenzionate caratteristiche. A tal proposito, nel Capitolo Primo, si cercherà di indagare più da vicino le caratteristiche e il funzionamento delle TRF, mettendo in luce che i sistemi *de quibus* soltanto nell'ultimo ventennio hanno avuto ampio sviluppo, grazie a Intelligenza Artificiale, *machine learning* e *big data.* Questa operazione permetterà di comprendere meglio – ma non di giustificare – lo sviluppo dell'*affective computing*, cioè le tecniche di analisi delle emozioni che aspirano a riprodurre l'intelligenza umana. Una prima ed elementare analisi dei sistemi di riconoscimento delle emozioni permetterà di studiare meglio, nel Quarto Capitolo, le implicazioni etiche e filosofiche che i sistemi di riconoscimento facciale pongono.

[1] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino, 2018, 224.
[2] Autorevole definizione adottata da GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* 22 marzo 2012*,* 2.

In assenza di una disciplina giuridica che si riferisca direttamente ai sistemi di riconoscimento facciale, nel Capitolo Secondo, partendo dalla nozione di dato biometrico, si cercherà di offrire un inquadramento giuridico più organico delle TRF, mediante l'analisi dei principi applicabili enucleati nel Regolamento (UE) 2016/679 (c.d. GDPR) e nella Direttiva (UE) 95/46/CE (c.d. LED): i principi di liceità, correttezza e trasparenza, di limitazione delle finalità, di minimizzazione dei dati, di esattezza, di limitazione della conservazione, nonché quelli di proporzionalità e di necessità. Non si mancherà di analizzare la recentissima Proposta di Regolamento (UE) sull'Intelligenza Artificiale, avanzata dalla Commissione europea, più volte modificata, la quale contiene numerosissime norme che si riferiscono ai sistemi di identificazione biometrica. A tal proposito, si evidenzieranno le manchevolezze della normativa, che ha dato una risposta non soddisfacente alla richiesta (proveniente da tutto il mondo giuridico) di organicità e di tutela dei diritti fondamentali dei cittadini nello spazio digitale, risultando la Proposta disorganica e priva di carattere. Seguirà una sintetica disamina sulle funzioni affidate al Comitato europeo per la protezione dei dati personali.

Prendendo atto della lacunosità della disciplina giuridica e della forte discrezionalità di cui gode il regolatore nell'applicare i principi generali, nel Capitolo Terzo si cercherà di ricostruire l'orientamento nel tempo espresso dal Garante per la protezione dei dati personali e dal Comitato europeo per la protezione dei dati sulle tecniche di riconoscimento facciale, analizzando più da vicino, tra gli altri, anche casi che hanno preoccupato l'opinione pubblica (ci si riferisce, in particolare, al caso *Clearview AI Inc.* e al caso S.A.R.I. *Real Time*). In un contesto così tecnicamente complesso e normativamente frammentato, pur nella scarsità dei casi direttamente riferibili alle TRF che si sono presentanti sulla scrivania del Garante *privacy,* risulta evidente il delicato e complesso bilanciamento tra gli importanti interessi in gioco: da un lato, l'esigenza di una maggiore sicurezza nelle nostre città, dall'altro lato, la tutela delle libertà e dei diritti fondamentali dei cittadini.

Orbene, oltre che preziose risorse, le tecnologie innovative come quelle di riconoscimento facciale pongono evidenti criticità, in quanto sono in grado di creare inedite forme di limitazione delle libertà e dei diritti fondamentali: stiamo assistendo all'ascesa di una nuova società della sorveglianza?

Per tale motivo, nel Capitolo Quarto, l'indagine si sposterà sulle implicazioni etiche poste dai sistemi di riconoscimento facciale. I sistemi di riconoscimento delle

emozioni, che aspirano addirittura a classificare e riconoscere le emozioni umane, invero, si ascrivono in un fenomeno antichissimo, cioè il desiderio di pochi di stringere l'essere umano nelle fitte maglie del potere e di governarlo, e anzi costituiscono il punto culminante di tale processo. In una *climax* ascendente, tratteggiando un percorso tanto preciso quanto soffocante, si cercherà di ricostruire il modo in cui da sempre la vita umana si è lasciata dominare dal potere.

Innanzitutto, nel suo saggio *"Sorvegliare e punire: nascita della prigione"*, il filosofo e storico francese Michel Foucault disegna il passaggio storico dal vecchio codice della sovranità, tipico dell'*Ancien Régime,* in cui il potere regio si manifesta come diritto di vivere o morire, ad un nuovo codice biopolitico, tipico della società disciplinare, ove il potere si arroga il diritto di individuare, classificare e organizzare minuziosamente il corpo, nella sua dimensione biologica, e si manifesta come una «scrupolosa amministrazione dei corpi» e una «pianificazione contabile della vita»[3].

Facendo un balzo in avanti, il filosofo sudcoreano con cattedra all'Università di Berlino Byung-Chul Han, nella sua *"Psicopolitica",* descrive una nuova fisica del potere, espressione dell'epoca contemporanea, che – tramite i *big data* e la dittatura della trasparenza che ne consegue – mira a dominare la psiche. Impregnato di questa nuova cultura – che enfatizza la motivazione, il progetto, la *performance,* l'ottimizzazione delle azioni e dei pensieri – sembra ormai che l'individuo sia divenuto incapace di riconoscere l'Altro. La sensazione che ne scaturisce è che l'*homo digitalis* stia perdendo lentamente, ma inesorabilmente, il proprio diritto al tempo futuro. È compito del diritto, indipendentemente dallo strumento giuridico impiegato, ricollocare al centro del mondo la tutela dell'individuo.

In fin dei conti, all'Unione Europea e a tutti gli Stati membri è stata concessa un'ultima occasione per dimostrare che «il futuro dipende ancora da noi», chiamati, come specie, a definire «l'esatta linea di confine tra l'uomo e la macchina»[4].

[3] M. FOUCAULT, *La volontà di sapere,* Feltrinelli, Milano, 2004, 121.
[4] C. CALDAROLA, *L'intelligenza artificiale: l'ombra sulla specie umana in un pianeta dominato dalla tecnica? O l'alba di una nuova umanità?,* in A. F. AURICCHIO, G. RICCIO, U. RUFFOLO, *Intelligenza artificiale tra etica e diritti: prime riflessioni a seguiti del Libro Bianco dell'Unione europea,* Bari, Cacucci, 2020, 32.

# CAPITOLO PRIMO

# I CARATTERI GENERALI DELLE TECNICHE DI RICONOSCIMENTO FACCIALE

## 1.1.I sistemi biometrici: identificazione e autenticazione

Non è possibile pensare di avviare uno studio sulle problematiche giuridiche e filosofiche afferenti alle tecniche di riconoscimento facciale (d'ora in avanti anche TRF), senza prima condurre un'attenta e accurata indagine sui sistemi biometrici. Difatti, l'ipotesi di fondo alla presente analisi si sostanzia nell'assunto secondo il quale i dati tipicamente processati dalle tecniche di riconoscimento facciale dovrebbero essere ascritti nell'alveo dei dati biometrici[5]. Tale operazione – di carattere squisitamente descrittivo – non è affatto scontata, in quanto il campo della biometria si presenta assai vasto e complesso, oltre che carente di consolidate riflessioni dottrinali e giurisprudenziali in materia.

È connaturata nella civiltà umana l'esigenza di identificare i soggetti, e di indentificarli per mezzo del corpo, nonostante ai suoi primordi si trattasse di un'esigenza fortemente circoscritta[6]. Solamente a partire dalla seconda metà del XIX secolo, invero, si sviluppa in Europa in ambito forense una scienza sistematica che utilizza il corpo a fini di identificazione dei criminali nelle indagini di polizia: l'antropometria, infatti, è all'origine dell'attuale biometria, con cui condivide lo scopo (l'identificazione) e il mezzo (il corpo). Fu Alphonse Bertillon (1853-1914), un impiegato della prefettura della polizia di Parigi, a ideare un vero e proprio sistema di riconoscimento – divenuto noto all'epoca come sistema *bertillonage* – basato sulla misurazione di alcune parti del corpo umano (altezza del torso, ampiezza delle braccia, misura del tronco e dell'orecchio, ampiezza della testa, distanza tra il gomito e l'estremità del dito medio, lunghezza del piede

[5] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 29. Ai fini del presente elaborato, rileva soprattutto la distinzione tra "dato personale" e "dato biometrico": in merito alle definizioni, si rinvia, *infra,* al Capitolo Secondo, in particolare §2.1.

[6] E. MORDINI, *The ethical and social Implications of Biometricsì Technologies,* in *Biometrics: Biometrics; Enhancing Security or Invading Privacy? Proceedings of the Irishi Council For Bioethics' Conference,* 26 novembre 2008, Dublic, 12. Per una ricostruzione storica più approfondita si vedano S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria: i codici a barre del corpo,* Giappichelli, Torino, 2013, 28 ss.; A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani,* Tirrenia Stampatori, Torino, 2004, 1 ss.

sinistro)[7]. Di contro, va attribuito all'antropologo Francis Galton (1822-1911) il merito di aver studiato le impronte digitali – scoprendo che sono una caratteristica unica di ogni individuo, essendo impossibile che due persone abbiano le stesse impronte digitali – e averne favorito l'effettiva adozione nelle aule dei tribunali[8]. Da allora, i sistemi biometrici hanno subito una rapida evoluzione.

Il termine "biometria" – che corrisponde sostanzialmente all'inglese *"biometrics"*, al plurale – si riferisce oggi all'«uso automatizzato di caratteristiche fisiologiche o comportamentali per determinare o verificare l'identità»[9]. Per "sistemi biometrici", invece, si indicano le applicazioni di tecnologie biometriche che consentono l'identificazione e/o l'autenticazione/verifica automatica di un soggetto[10]. Nonostante il documento *Biometric-based techologies* dell'OECD operi una distinzione tra *biometrics* e *biometric system,* nella prassi tali termini vengono utilizzati come sinonimi[11].

Esaminata la definizione di "biometria", pare opportuno analizzarla più attentamente, in quanto contiene aspetti cruciali ai fini di una corretta delimitazione della nostra indagine giuridica.

Innanzitutto, è di fondamentale importanza che la raccolta, la conservazione e il trattamento dei dati biometrici avvengano tramite un «uso automatizzato»: viceversa, non

---

[7] Tali caratteristiche fisiche venivano annotate su una scheda e dal confronto tra questa e il soggetto avveniva il riconoscimento. Erano stati addirittura ideati e costruiti specifici e molteplici strumenti per operare tali misurazioni. Cfr. A. BERTILLON, *La photographie judiciaire: avec un appendice sur la classification et l'identification antropométrique,* Gauthier-Villars, Parigi, 1980, 15.

[8] F. Galton, insieme a Sir Edward Henry, studiò le impronte digitali dei gemelli omozigoti, indagandone anche l'ereditarietà, per verificare che effettivamente nessun individuo condividesse le stesse impronte digitali. S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria: i codici a barre del corpo,* Giappichelli, Torino, 2013, 18-19.

[9] «*The automated use of physiological or behavioural characteristics to determine or verify identity»,* secondo la definizione adottata dall'INTERNATIONAL BIOMETRIC GROUP (IBG), "*How is «biometrics» Defined?"* in https://www.biometricsinstitute.org/what-is-biometrics/ e ripresa nel Documento dell'OECD: WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based techologies,* 30 giugno 2004, 10-11. Altre definizioni di *"biometrics"* sono contenute in vari documenti in materia di biometria, nonostante essi sostanzialmente coincidano. Si veda, a titolo esemplificativo, COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, Aprile 2013, in https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81, che stabilisce che "*biometrics"* si riferisce a quei sistemi che utilizzano caratteristiche misurabili, fisiche o comportamentali, allo scopo di riconoscere l'identità o verificare l'identità dichiarata di un individuo.

[10] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria*, 1° agosto 2003, in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_it.pdf.

[11] A. AGOSTINI, *Biometria e privacy: i presunti nemici a confronto,* Edis, Bologna, 2006.

potrebbe essere qualificato come "sistema biometrico" un sistema di documenti che si basa su immagini confrontate manualmente da una persona[12].

In secondo luogo, un sistema biometrico può elaborare sia caratteristiche fisiche e fisiologiche sia caratteristiche comportamentali. Tra le prime è possibile annoverare la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento facciale, la geometria della mano, il riconoscimento della forma dell'orecchio, l'analisi del DNA e così via. Le seconde – le quali misurano il comportamento di un individuo – comprendono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura e così via[13]. Tali caratteristiche, il più delle volte, sono variamente incrociate e utilizzate congiuntamente[14].

Le caratteristiche biometriche, siano esse fisiche o comportamentali, devono soddisfare dei requisiti essenziali (i c.d. "sette pilastri"): l'universalità, nel senso che quella caratteristica deve essere presente in ogni individuo; l'unicità, nel senso che non è possibile che due persone diverse abbiano la stessa identica caratteristica biometrica; la catturabilità, nel senso che la caratteristica deve poter essere raccolta facilmente; la permanenza nel tempo; un grado elevato di accuratezza nell'identificazione; accettazione da parte degli utenti; maggiore sicurezza rispetto ai tradizionali elementi identificativi[15]. È ovvio che non tutte le tecniche di identificazione biometrica sono in grado di soddisfare al massimo grado tali requisiti, pur dovendo essere tutti presenti ai fini della qualificazione di un dato come biometrico[16].

---

[12] OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based techologies,* 30 giugno 2004, in http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/NT000070D6/$FILE/JT00166988, il quale afferma che – volendo essere precisi – il termine "*automated*" dovrebbe essere sostituito con l'espressione "*automated-assisted*".

[13] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003.

[14] Si parla, in tal caso, di *multimodal biometrics.* Cfr. THE IRISH COUNCIL FOR BIOETHICS, *Biometrics: Enhancing Security or Invading Privacy?,* Dublin, 2009, 54-58.

[15] EUROPEAN COMMISION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Commettee on Citizen's Freedoms and rights, Justice and Home Affaire (LIBE),* 2005, 37, in http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf, che fa riferimento a «*universality, distinctiveness, permanence, acceptability, resistance to circumvention*». Invece, GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, 3, menziona soltanto i primi tre requisiti.

[16] A titolo esemplificativo, l'impronta digitale – al pari dell'iride o della geometria della mano – può non soddisfare appieno il requisito dell'universalità, in quanto vi possono essere limiti dovuti a menomazioni fisiche o disabilità, laddove il riconoscimento facciale soddisfa integralmente questa proprietà. Viceversa, il requisito della permanenza è integrato al massimo grado nel caso dell'impronta digitale o dell'iride, mentre lo stesso non può dirsi per il riconoscimento del volto.

Infine, lo scopo che si propone la biometria è quello di determinare (c.d. identificazione) ovvero di verificare (c.d. verifica/autenticazione) l'identità di un soggetto. Si tratta di una distinzione cruciale, in quanto le prestazioni biometriche, gli algoritmi, i vantaggi e i rischi dell'implementazione, dell'impatto sulla *privacy* e i costi differiscono notevolmente[17].

Nello specifico, mediante la procedura di identificazione, il sistema automatizzato confronta il campione biometrico in ingresso con tutti i *template* registrati nel *database*[18], senza dichiarare l'identità dell'individuo cui appartiene il dato biometrico grezzo. I sistemi di autenticazione rispondono alla domanda: "Chi sono io?" e non richiedono che l'utente rivendichi un'identità prima che avvenga il confronto biometrico. Tale procedura – che dunque realizza una comparazione uno-a-molti (1-n) – implica necessariamente la consultazione di archivi e *database* di grandi dimensioni ed è utilizzata soprattutto nel campo della giustizia e della pubblica sicurezza[19]. Il sistema biometrico può realizzare un'identificazione positiva o negativa, dichiarando che l'individuo appartiene o non appartiene al gruppo di utenti noti al sistema[20].

Viceversa, mediante la procedura di verifica/autenticazione, il sistema automatico opera un raffronto tra le caratteristiche biometriche catturate (*feature extraction*) e il dato biometrico preregistrato nel *database* (c.d. *template*)[21], allo scopo di accertare l'effettiva identità dichiarata dal diretto interessato. Tale procedura risponde alla finalità di accertare la corrispondenza univoca – tramite una comparazione uno-a-uno (1-1) – tra le caratteristiche fisiche o comportamentali di un soggetto e un *set* di informazioni biometriche già presenti e registrate nel *database* o nel dispositivo mobile. I sistemi di verifica, in sostanza, rispondono alla domanda: "Sono chi affermo di essere?", richiedendo che l'utente rivendichi un'identità per poter eseguire un confronto

---

[17] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 12.

[18] CNIPA, *Linee guida per le tecnologie biometriche,* 8 ottobre 2004, 12, in www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf.

[19] F. CASCETTA, M. DE LUCCIA, *Sistemi di identificazione personale*, in *Mondo digitale n. 1*, marzo 2004, 54.

[20] CNIPA, *Linee guida per le tecnologie biometriche,* 8 ottobre 2004, 12, in www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf.

[21] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, aprile 2013, in https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81, che prevede che la verifica/autenticazione significa «*comparing a presented biometric sample with the corresponding enrollement biometric data pertaining to one single person*».

biometrico[22]. Le tecnologie di identificazione biometrica sono impiegate soprattutto per garantire la sicurezza nel controllo degli accessi fisici e informatici (in banche, tribunali, uffici giudiziari, settori strategici di industrie ecc.), ovvero per l'accreditamento a servizi o presso istituzioni (firma digitale), ovvero per garantire l'anticontraffazione dei documenti di identità[23].

Oltre al fine che si intende perseguire, anche i vantaggi pratici che presenta ciascun sistema possono orientare la scelta tra i sistemi di identificazione e i sistemi di autenticazione/verifica: i primi richiedono un elevato potere computazionale, in quanto sono deputati ad operare una vasta quantità di raffronti, ragione per cui è maggiore il margine di errore; i secondi, invece, sono generalmente più rapidi e accurati[24].

Una volta analizzati, a grandi linee, la definizione e gli scopi della biometria, è possibile dar conto delle diverse fasi cui si articola il processo biometrico, per comprendere come i dati biometrici – oggetto della presente analisi giuridica – siano estrapolati[25].

Il procedimento biometrico prende avvio con la c.d. fase di *enrollment,* durante la quale il dispositivo, munito di apposito sensore, rileva la caratteristica biometrica (c.d. "dato biometrico grezzo" o "campione biometrico"), cioè la parte del corpo interessata, sottoforma di immagine (ad esempio, l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione vocale). Se di qualità soddisfacente, il campione biometrico viene successivamente convertito con un algoritmo in una rappresentazione matematica, cioè in una stringa di caratteri alfanumerici, ottenendo in tal modo il c.d.

---

[22] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 12.

[23] F. CASCETTA, M. DE LUCCIA, *Sistemi di identificazione personale*, in *Mondo digitale n. 1*, marzo 2004, 52-53. In particolare, con riferimento all'anticontraffazione dei documenti di identità, è ormai in uso in numerosissimi Paesi, tra cui l'Italia, il passaporto elettronico (c.d. *e-passport*), allo scopo di dare una prima risposta alla crescente esigenza di sicurezza internazionale.

[24] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 13-14.

[25] Quanto alle nozioni di carattere tecnico, si vedano S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 15 ss.; J. D. WOODWARD, N. M. ORLANS, P. T. HIGGINGS, *Identity Biometrics*, McGraw-Hill, 2003, 28 ss.; I. K. SETHY, *Biometrics, Overview and Applications,* in STRANDBURG-RAICU, *Privacy and Technologies of Identity. A cross disciplinary conversation,* Springer, 2006, 119 ss.; A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy,* EPC LIBRI, Roma, 2002, 30 ss.; S. GIROTTO, *Il trattamento dei dati biometrici,* in *Il governo del corpo*, Giuffrè, Milano, 2011, 1239 ss.; G. PREITE, *Il riconoscimento biometrico. Sicurezza versus privacy,* Editrice Uni Service, Trento, 2007, 47 ss.; CNIPA, *Linee guida per le tecnologie biometriche,* 8 ottobre 2004, 13 ss., in www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf.; GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, 3-4.

*template* o "modello biometrico"[26]. È di fondamentale importanza che il campione biometrico raccolto sia di alta qualità, nel senso che, da un lato, il dato biometrico grezzo deve permettere di identificare la caratteristica biometrica e, dall'altro, deve avere il carattere dell'unicità, dovendo essere difficile che venga confuso con il campione biometrico appartenente ad altro soggetto. Il successo di ogni sistema di identificazione personale dipende in gran parte dalla qualità dei campioni memorizzati nel *database*[27].

È importante precisare che la distinzione tra "dato biometrico grezzo" e "*template*" – sebbene possa sembrare *ictu oculi* cavillosa e di poco conto – è fondamentale per comprendere alcune problematiche connesse alla protezione dei dati biometrici. Come vedremo, con particolare riferimento alla conservazione dei dati biometrici, generalmente ad essere archiviati sono i *template,* e non i dati biometrici grezzi generati nel processo di acquisizione, i quali dovrebbero essere immediatamente cancellati, nonostante non pare vietato che in alcune circostanze possano essere conservati anche i campioni biometrici[28], a seconda dei sistemi utilizzati e delle finalità perseguite[29].

Una volta conclusa la fase di iscrizione, la procedura prosegue con la fase di *matching,* cioè con il confronto dei *template* (o, appunto, dei dati biometrici grezzi), al fine di determinare il loro grado di somiglianza[30]. Nello specifico, in caso di verifica/autenticazione, la comparazione avviene tra il modello biometrico archiviato mediante il processo di *enrollment* (c.d. *enrollment template*) e il modello creato, seguendo il medesimo procedimento di iscrizione, nel momento in cui l'utente fornisce il proprio dato dispositivo biometrico (c.d. *verification template*), il quale generalmente viene cancellato immediatamente. In caso di identificazione, invece, la comparazione

[26] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, 4, ha tradotto il termine inglese "template" con l'espressione "campione biometrico". Inoltre, quando si fa riferimento, genericamente, al "dato biometrico", ci si riferisce generalmente al "*template*".

[27] ICT Security, *Biometria e Sicurezza Informatica*, n. 39-40-4-42, Novembre 2005 – Febbraio 2006. Ovviamente, la qualità del campione biometrico dipende dalla collaborazione degli utenti.

[28] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, 4, il quale lascia aperta tale possibilità; per un approfondimento, *infra,* nel Capitolo successivo, paragrafo §2.1.5.

[29] Un settore nel quale è necessaria la conservazione dei campioni biometrici è quello dei passaporti. Dal momento che in questo caso i sistemi biometrici sono costruiti in maniera tale che il *template* creato da un sistema non possa essere letto da un altro sistema, l'Organizzazione Internazionale dell'Aviazione Civile richiede che sia memorizzato il campione biometrico, e non il *template,* allo scopo di garantire l'interoperabilità tra i sistemi, in una società globalizzata come la nostra. Cosi, ICAO, *Biometric deployment of Machine Readable Travel Documents,* in ICAO TAG MRDT/NTWG, *Technical Report,* 21 maggio 2004, 31.

[30] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 20.

avviene tra il modello fornito dal soggetto e i modelli o campioni biometrici di altri soggetti archiviati nel *database*[31].

All'esito della comparazione, tramite speciali algoritmi utilizzati dai sistemi biometrici, viene assegnato un punteggio (c.d. *matching score*), che rappresenta il grado di somiglianza tra i due *template,* rispetto ad un valore-soglia, in genere prestabilito dall'amministratore del sistema[32]. Se il punteggio assegnato supera la soglia, allora avrà luogo l'identificazione o verifica/autenticazione (c.d. *match*), mentre in caso contrario, non vi sarà alcun riconoscimento (c.d. *non match*)[33]. Dunque, la risposta che è in grado di dare il sistema biometrico non è se i *template* (o, eventualmente, i campioni) sono identici, ma solamente qual è il loro grado di similarità.

Da tale considerazione, si può trarre un'importante osservazione: dal momento che non è possibile raggiungere tra i *template* confrontati un livello di somiglianza pari al 100%, nonostante i massicci sviluppi dell'intelligenza artificiale e degli algoritmi, necessariamente il sistema biometrico dà luogo ad un riconoscimento approssimativo e persiste una percentuale variabile di errore, dipendente dai calcoli probabilistici effettuati dall'algoritmo, il quale deve pur sempre elaborare una grande quantità di dati. Sono stati, dunque, individuati dei parametri che danno conto dell'inesattezza della risposta del sistema di riconoscimento biometrico.

In particolare, il parametro FMR *(false match rate*) indica la probabilità che il sistema di identificazione biometrica abbia abbinato due *template* che rappresentano campioni biometrici appartenenti a soggetti diversi, con la conseguenza che qualcuno potrebbe accedere ad un sistema, pur non avendone il titolo (FAR, *false acceptance rate*). Viceversa, il parametro FNMR *(false non match rate)* indica la probabilità che il sistema biometrico non associ correttamente l'*enrollment template* con il *verification template,* appartenenti al medesimo soggetto, di modo che qualcuno, pur essendone titolato, non sia in grado di accedere ad un sistema (FRR, *false rejecton rate*). Infine, il parametro FTE

---

[31] S. GIROTTO, *Il trattamento dei dati biometrici,* in *Il governo del corpo*, Giuffrè, Milano, 2011, 1240.

[32] Come sottolineato da S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 22, non esistono scale *standard,* adottate da tutti i sistemi biometrici, ma ogni amministratore può scegliere il valore-soglia ritenuto opportuno: alcuni sistemi fanno riferimento ad una scala che va da 1 a 100, altri da -1 a 1. È, quindi, possibile scegliere il sistema biometrico da utilizzare, anche in funzione della soglia più o meno elevata e, conseguentemente, del grado di sicurezza desiderato, con una elasticità non possibile per quei sistemi di sicurezza che utilizzano PIN o *password.*

[33] CNIPA, *Linee guida per le tecnologie biometriche,* 8 ottobre 2004, 25 ss., in www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf.

*(failure to enroll*) indica la probabilità che un individuo non possa essere registrato nel sistema biometrico[34].

### 1.2.Le tecniche di riconoscimento facciale: funzionamento e caratteristiche

Senza dubbio, le tecnologie biometriche oggi maggiormente diffuse nei più svariati ambiti applicativi sono quelle basate sul riconoscimento facciale, che consiste nel «trattamento automatizzato di immagini digitali che contengono volti di persone, ai fini di verifica/autenticazione, identificazione o categorizzazione»[35].

In generale, l'unicità dei dati biometrici offre notevoli vantaggi rispetto ai tradizionali metodi di riconoscimento, quali PIN o *password*, perché non possono essere rubati, cancellati o duplicati[36]. Il campo della biometria, infatti, considera le caratteristiche fisiche, fisiologiche o comportamentali di una persona, che sono uniche per quell'individuo. Mentre per le persone è relativamente facile mentire, gli identificatori biometrici – cioè la geometria della mano, il volto, l'iride o le impronte digitali – sono più sicuri, perché "il corpo non mente mai" ed è particolarmente difficile alterare i propri tratti biometrici. Tuttavia, anche le caratteristiche biometriche presentano degli inconvenienti. Ad esempio, il riconoscimento dell'iride è molto accurato, ma economicamente costoso; le impronte digitali sono poco costose, ma difficilmente possono essere catturate a individui non collaborativi.

Rispetto alle altre caratteristiche biometriche, il volto è probabilmente la caratteristica fisica maggiormente identificativa dell'essere umano, perché disvela la sua identità unica, le sue emozioni, la sua età e attraverso di esso il contatto sociale diventa più facile. Altre proprietà, quali l'universalità e la catturabilità, sono maggiormente elevate per il viso

---

[34] Per una trattazione completa, si veda S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 23.

[35] Autorevole definizione adottata da GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* 22 marzo 2012*,* 2, ripresa da G. MOBILIO, op. cit., 32.

[36] Non a caso, il GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, 4, opera una triplice ripartizione tra i sistemi attraverso i quali, allo stato delle conoscenze tecnologiche attuali, un utente può essere identificato: ci si può basare su qualcosa che l'utente conosce (come un PIN o una *password*), ovvero su qualcosa che l'utente possiede (un dispositivo di autenticazione o *token,* una *smart card*), ovvero su qualcosa che è proprio del soggetto (appunto, una caratteristica biometrica). È ovvio che tali sistemi possano essere utilizzati congiuntamente. Tale distinzione è ripresa anche in altri contributi, quali E. SANNA, *Le garanzie di sicurezza e autenticità delle informazioni in rete; in particolare del mandato informatico di pagamento,* in *Riv. Giur. Sarda, 2001,* fasc. 1, 311; S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica,* in *Ciberspazio e diritto,* 2005, 9.

rispetto ad altri dati biometrici: il volto è generalmente esposto e può facilmente essere catturato[37]. In aggiunta, le TRF risultano di più facile utilizzo: si tratta di sistemi che sfruttano dispositivi in grado di compiere prestazioni sempre più efficienti e precise, il cui costo – complice la grande diffusione cui si assiste – è sempre più accessibile. Gli algoritmi di cui si servono sono sempre più performanti e sofisticati; le telecamere o videocamere sono in grado di rilevare immagini a centinaia di metri, di giorno o di notte. Inoltre, tali sistemi sono incorporati in dispositivi divenuti ormai di uso quotidiano, quali smartphone, pc, tablet, smart TV[38]. Secondo un rapporto del *National Institute of Standards and Technology (NIST)* del 2010, *Face Recognition Techniques* – che è considerata tra le TRF più precise e performanti – il tasso di identificazione di un soggetto sconosciuto, su un *database* che considera 1,6 milioni di volti, è pari al 92%. Addirittura, in un recente aggiornamento del 2018, il NIST suggerisce che l'accuratezza del *software* di riconoscimento facciale sta aumentando notevolmente, con un tasso di errore ridotto dello 0,2%[39].

A livello tecnico, tenendo a mente la complessità e la molteplicità degli algoritmi utilizzati per il riconoscimento facciale, con inevitabile approssimazione, è possibile enucleare le diverse fasi cui si articola il procedimento di riconoscimento facciale[40].

Il procedimento di riconoscimento facciale prende avvio con la fase di acquisizione dell'immagine (c.d. *image capturing*), durante la quale il dispositivo cattura e converte in formato digitale l'immagine del volto di una persona, acquisita tramite una fotografia o una videoregistrazione. L'acquisizione può avvenire in un ambiente controllato e con la cooperazione e partecipazione attiva dell'interessato (c.d. sistemi biometrici interattivi o partecipativi) ovvero in un ambiente non controllato e senza che il soggetto ne abbia percezione o consapevolezza (c.d. sistemi biometrici passivi), come avviene ad esempio per le videocamere a circuito chiuso[41]. Come è stato accennato, *mutatis mutandis* il successo del riconoscimento facciale dipende in gran parte dalla qualità dei campioni memorizzati nel *database* e, quindi, anche dalle modalità di acquisizione dell'immagine.

---

[37] P. KAUR, K. KRISHAN, S. K. SHARMA, T. KANCHAN, *Facial recognition algorithms: a literature review,* in *Medicine, Science and the Law,* Volume 60 (2), aprile 2020, 1 ss.
[38] G. MOBILIO, op. cit., 37.
[39] P. KAUR, K. KRISHAN, S. K. SHARMA, T. KANCHAN, *Facial recognition algorithms: a literature review,* in *Medicine, Science and the Law,* Volume 60 (2), aprile 2020, 1 ss.
[40] *Ibidem;* G. MOBILIO, op.cit., 32 ss.
[41] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 12 novembre 2014*, in *Gazzetta ufficiale della Repubblica Italiana*, Serie generale – n. 280, 3.

Il procedimento prosegue con la fase di rilevamento del volto (c.d. *face detection*) – nella quale il *software* identifica e isola, all'interno dell'immagine, il volto rispetto allo sfondo – e con la fase di normalizzazione, durante la quale il *software* corregge e attenua le imperfezioni dell'immagine dovute alla posizione o alla scarsa illuminazione, tramite ad esempio la rotazione, la variazione dei colori o la conversione ad una dimensione *standard*[42].

Segue la fase di estrazione delle caratteristiche (c.d. *feature extraction*), durante la quale, dal volto rilevato, il *software* riconosce ed estrae le c.d. caratteristiche biometriche distintive della persona – quali occhi, naso, bocca o contorno facciale – e le converte in una rappresentazione matematica, cioè in una stringa di caratteri alfanumerici, ottenendo in tal modo il c.d. *template* o "modello biometrico", analogamente a quanto accade per tutti i sistemi biometrici. L'estrazione delle caratteristiche può essere *olistica,* nel senso che l'intera immagine facciale viene convertita in rappresentazione matematica ovvero basata sui *singoli tratti biometrici,* nel qual caso sono convertite in rappresentazione matematica le singole caratteristiche biometriche[43].

L'immagine o il modello biometrico vengono, dunque, registrati e conservati in un *database,* di modo che possa avvenire la fase finale di confronto (c.d. *matching*), in cui il sistema procede alla comparazione dei *template* (o, in alcuni casi, dei dati biometrici grezzi), al fine di determinare il loro grado di somiglianza[44].

Come si è già detto, il confronto può essere operato per diverse finalità: la verifica/autenticazione e l'identificazione, cui va aggiunta oggi la categorizzazione[45].

Nello specifico, la verifica/autenticazione, la quale opera una comparazione uno-a-uno (1-1), può avvenire in una duplice modalità. Nel caso della verifica, il sistema automatico opera un confronto tra le caratteristiche biometriche catturate e una persona già conosciuta e individuata, tramite ad esempio la presentazione di un documento di identità. Questa modalità comincia ad essere utilizzata negli aeroporti, ove il personale raffronta l'immagine dei passeggeri e il *template* contenuto nel *chip* dell'*e-passport,* per verificare che il passeggero sia effettivamente chi dichiara di essere. Nel caso

[42] G. MOBILIO, op.cit., 32 ss.
[43] *Ibidem.*
[44] *Ibidem.*
[45] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* 22 marzo 2012*,* 2, indica le tre diverse finalità, a differenza di quanto avveniva nel precedente GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* 1° agosto 2003, il quale faceva riferimento solamente alla verifica/autenticazione e all'identificazione.

dell'autenticazione, il *software* si limita a verificare la corrispondenza biunivoca tra le caratteristiche biometriche e *template* registrato nel *database,* senza che sia avvenuta però l'identificazione della persona. È quanto avviene, ad esempio, quando sblocchiamo un comune *smartphone* tramite il riconoscimento facciale[46].

Viceversa, avendo riguardo all'identificazione – che realizza una comparazione uno-a-molti (1-n) – il sistema automatizzato confronta il campione biometrico in ingresso con tutti i *template* registrati nel *database,* senza che sia nota l'identità dell'individuo cui appartiene il dato biometrico grezzo, alla ricerca di una possibile corrispondenza. È proprio questa la finalità tipica cui le TRF potrebbero mostrare tutta la loro potenzialità e straordinarietà, soprattutto a fini di tutela della cosa pubblica e, quindi, ad esempio, per l'identificazione dell'autore di un reato[47].

Infine, la categorizzazione si pone l'obiettivo di estrarre le caratteristiche biometriche dall'immagine di una persona (identificata o meno), per poi classificarla in base a determinati parametri (ad esempio, età, sesso, abitudini di consumo). Lo scopo, dunque, non è l'individuazione del soggetto, ma l'estrazione delle sue caratteristiche, da impiegare con le più disparate finalità[48].

Da notare che le TRF si fondano su tecniche induttive e di inferenza probabilistica (c.d. *data analytics*)[49], che prescindono totalmente dalla comprensione del dato processato (si tratta pur sempre di Intelligenza Artificiale e non di intelligenza umana), assumendo le proprie determinazioni attraverso algoritmi che effettuano calcoli probabilistici circa la rispondenza o meno tra due *template:* il sistema, una volta effettuata la ricerca, restituisce un certo numero di risultati, ordinati sulla base della loro probabilità[50]. Ne consegue che, come accade per tutti i sistemi biometrici, anche le TRF – nonostante l'incremento esponenziale della tecnologia in questo settore – non si sottraggono ad una percentuale variabile di errore, che dipende non solo dalla qualità e risoluzione dell'immagine, dalla distanza dal sensore, dal tipo di illuminazione, dall'inclinazione o dalla posa del volto, ma anche dall'età, dal colore della pelle,

[46] GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* 22 marzo 2012, 3.
[47] *Ivi,* 7.
[48] G. MOBILIO, op.cit., 35.
[49] *Infra,* in questo Capitolo, §1.2.1.
[50] *Infra,* in questo Capitolo, §1.1.

dall'espressione facciale, dal trucco, dalle caratteristiche somatiche simili (ad esempio, si pensi ai gemelli, che sicuramente mettono in difficoltà anche le più sofisticare TRF)[51].

In particolare, un errore può dar luogo ad un "*false acceptance rate"* (falso positivo) nel caso in cui il sistema riconosca erroneamente una corrispondenza tra *template* appartenenti a soggetti diversi, permettendo ad un soggetto non titolato di accedere ad un determinato ambiente fisico o logico; viceversa l'errore può determinare un "*false non match rate"* (falso negativo) nel caso in cui il sistema erroneamente non riconosca la corrispondenza tra due *template* che invece appartengono al medesimo soggetto, impedendo così l'accesso ad un soggetto che ne ha titolo[52].

In quei sistemi che utilizzano algoritmi altamente sofisticati, qualora l'immagine facciale sia acquisita in ambienti controllati, il tasso di errore sfiora lo 0,1%[53], mentre il tasso di errore può toccare il 2,8% nel caso in cui siano utilizzati sistemi passivi di riconoscimento e in presenza di una scarsa risoluzione dell'immagine[54]. È ovvio che il margine di errore accettabile dipende dall'uso per cui sono impiegate le TRF: per scopi di marketing sarà tollerato un maggiore margine di errore rispetto al caso in cui siano utilizzate per scopi di polizia o di *intelligence*[55].

### 1.2.1. *(Segue):* L'impulso dato da Intelligenza Artificiale, *machine learning* e *big data*

Seppure si sia mostrato interesse per il riconoscimento facciale già a partire dagli Anni Sessanta del secolo scorso[56], soltanto nell'ultimo ventennio, fattori come

[51] G. MOBILIO, op.cit., 35 ss.
[52] *Ibidem.* Ovviamente, il tasso di falsi positivi o di falsi negativi dipende dalla sensibilità e accuratezza del sistema prescelto.
[53] P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 2: Identification,* NIST Interagency/Internal Report (NISTIR) - 8271, dicembre 2020, 4.
[54] J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System,* EUR 29808 EN, Publication Office of the European Union, Luxemburg, luglio 2019, 67.
[55] *Ibidem.*
[56] Già negli Anni Sessanta, è stato sviluppato dai matematici americani Woody Bledsoe, Helen Chan Wolf e Charles Busson un sistema semi-automatico per il riconoscimento facciale, in cui però la misurazione delle caratteristiche biometriche, quali lo spessore delle labbra o l'analisi dei capelli, erano calcolate manualmente. Nel 1997, invece, è stato sviluppato e commercializzato il *software* ZN-Face, che per la prima volta ha riconosciuto, tramite un trattamento automatizzato, le immagini facciali, anche quelle non perfettamente frontali. Cfr. P. KAUR, K. KRISHAN, S. K. SHARMA, T. KANCHAN, *Facial recognition algorithms: a literature review,* in *Medicine, Science and the Law,* Volume 60 (2), Aprile 2020, 1.

Intelligenza Artificiale, *machine learning* e *big data* hanno dato forte impulso al settore delle TRF.

Il vertiginoso sviluppo delle TRF è stato favorito, innanzitutto, dalle rapide innovazioni tecnologiche, quali l'accesso a tecnologie a basso costo, lo sfruttamento di potenti sistemi computazionali, l'elaborazione di algoritmi sempre più avanzati e, soprattutto, la crescente quantità di *big data*[57].

La branca dell'informatica relativa all'estrazione delle informazioni dalle immagini, nonostante qualche peculiarità, rientra ancora a pieno titolo nel settore dell'*Artificial Intelligence*[58]*,* fenomeno epocale che ha dato origine alla quarta rivoluzione industriale e che ha generato un cambiamento profondo di quella che è stata definita da Malraux "la condizione umana"[59].

Senza voler entrare nel merito del dibattito scientifico, l'Intelligenza Artificiale è stata recentemente definita dall'*High-level expert group on Artificial Intelligence*, istituito dalla Commissione europea nel 2019, come «*software* (ed eventualmente *hardware*) progettati dall'uomo che – dato un obiettivo complesso – agiscono in una dimensione fisica o digitale, percependo il loro ambiente attraverso l'acquisizione di dati, interpretando dati strutturati o non strutturati raccolti, elaborando informazioni derivanti da tali dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato»[60]. In altri luoghi, è stata efficacemente qualificata come «una scienza e un insieme di tecnologie computazionali che sono ispirate – ma da cui si differenziato – ai modi con cui le persone usano il loro sistema nervoso e il corpo per percepire, imparare, ragionare e agire»[61]. A partire dal momento in cui Alan M. Turing – considerato il padre

---

[57] G. MOBILIO, op. cit., 38; M. EBERS, *Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges,* in M. EBERS, S. NAVAS NAVARRO (a cura di), *Algorithms and Law,* Cambridge University Press, Cambridge, 2020, 61.

[58] G. MOBILIO, op. cit., 38 ss.

[59] U. RUFFOLO, *Prefazione,* in A. F. AURICCHIO, G. RICCIO, U. RUFFOLO, *Intelligenza artificiale tra etica e diritti. Prime riflessioni a seguito del Libro Bianco dell'Unione europea,* Cacucci, Bari, 2020, 25; A. MALRAUX, *La condition humaine,* Editions Gallimard, 1933.

[60] «*Software (and possibly also hardware) systems designed by humans that, given a complex goal, act in a physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasining on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal» ,* secondo l'autorevole definizione adottata da HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, SET UP BY THE EUROPEAN COMMISSION, *A definition of AI: main capabilities and disciplines. Definition developed for the purpose of the AI HLEG's deliverables,* Bruxelles, aprile 2019.

[61] «*A science and a set of computational technologies that are inspiring by -but tipically quite differently from – the ways people use their nervous system and bodies to sense, learn, reason and take actions»,* definizione adottata da AA. VV, *Artificial Intelligence and life in 2030 – One hundred year study on artificial intelligence,* Stanford University, settembre 2016, 4.

dell'informatica – pubblicò il saggio "*Computing Machinery and Intelligence"*, molte altre definizioni si sono succedute nel tempo, che si differenziano a seconda che sia valorizzato l'uno o l'altro tra gli elementi distintivi dell'AI: *"thinking humanly, acting humanly, thinking rationally, acting rationally"*[62].

Com'è noto, i "processi mentali" che muovono l'Intelligenza Artificiale sono rappresentati dagli algoritmi[63] – nozione per nulla pacifica e in merito alla quale gli studiosi hanno proposto diverse definizioni[64]. Ciononostante, una caratterizzazione sufficientemente rigorosa del concetto di algoritmo – che includa le proprietà della finitezza (l'algoritmo deve portare alla soluzione tramite una sequenza finita di istruzioni) e del determinismo (dati gli stessi dati in *input,* l'algoritmo deve fornire gli stessi *output*) – impone che l'algoritmo debba essere qualificato come «una sequenza finita di istruzioni ripetibili e non ambigue. Tale sequenza di istruzioni, se eseguita con determinati dati di ingresso (*input*), produce in uscita dei risultati (*output*), risolvendo una classe di problemi in un tempo finito»[65].

L'origine degli studi relativi al settore dell'Intelligenza Artificiale affonda le sue radici nel tentativo di riprodurre le facoltà cognitive e mentali dell'essere umano, alla ricerca della riproduzione della "comprensione" umana[66]. Tuttavia, sul piano tecnico prima ancora che etico-filosofico, le ricerche tese a riprodurre in componenti artificiali questa capacità umana sono storicamente perdenti: si è raggiunta la consapevolezza che è impossibile replicare computazionalmente la complessità del pensiero umano, l'ingegno, l'intuizione intellettuale, la capacità di cogliere il senso globale delle cose, indipendentemente dalla possibilità di spiegare il ragionamento logico seguito per arrivare ad una certa conclusione[67].

---

[62] R. ANGELINI, *Intelligenza Artificiale e governance*. *Alcune riflessioni di sistema,* in F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, 293.
[63] G. MOBILIO, op. cit., 39.
[64] Per una breve rassegna delle definizioni adottate dai vari studiosi si veda G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica,* Giappichelli, Torino, 2022, 103 ss. Ad esempio, illustri informatici (Donald Knuth) richiedono che l'algoritmo sia dotato del carattere della finitezza, limitando la nozione di algoritmo alle procedure finite, laddove altri studiosi (come Stephen Kleene o Marvin Minsky) ritengono che tale proprietà non sia necessaria, estendendo il concetto anche a procedure la cui esecuzione possa non avere termine. Alcuni ritengono che l'algoritmo debba essere ripetibile (determinismo), nel senso che l'algoritmo deve condurre sempre al medesimo *output,* mentre altri ammettono algoritmi non-deterministici. Ovviamente, a seconda della definizione di algoritmo adottata, certe procedure di calcolo possono integrare o meno un algoritmo.
[65] G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica,* Giappichelli, Torino, 2022.
[66] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino, 2018, 258.
[67] G. MOBILIO, op. cit., 41; M. A. BODEN, *L'intelligenza Artificiale,* il Mulino, Bologna, 2019, 119 ss.

Quanto osservato vale anche con riferimento alle TRF. I computer captano un'immagine e isolano il volto rispetto allo sfondo in modo completamente differente rispetto ad un essere umano: mentre l'uomo è in grado di *comprendere* nello spazio la presenza del viso e le sue espressioni facciali, dal punto di vista dell'algoritmo, l'immagine non è altro che un insieme di punti colorati (i *pixel*), che *verosimilmente* indicano la presenza di una faccia umana. Nonostante sia questo lo stato dell'arte attuale, si stanno facendo strada, nel campo del riconoscimento facciale, tecniche di analisi delle emozioni (c.d. *affective computing*), che mirano a riprodurre finalmente l'intelligenza umana e che si dichiarano capaci di decifrare le emozioni di una persona[68]. Tali ricerche si fondano sul presupposto, da un lato, che le espressioni facciali della persona siano una chiara manifestazione esterna del suo stato emotivo, e dall'altro, che le TFR siano in grado di cogliere tutte le micro-espressioni facciali e, da queste, risalire alle emozioni del soggetto. Ciononostante, non si può trascurare di sottolineare come tale scienza ometta di considerare che lo stato emotivo di una persona non possa essere *compreso* senza che entrino in gioco qualità propriamente umane, quali il legame empatico, la capacità di immedesimarsi nell'altro, la sensibilità culturale, le concrete dinamiche interpersonali[69].

Originariamente basata sulla creazione di algoritmi in grado di fornire risposte precise a *input* corrispondenti, oggi l'intelligenza artificiale si sta piuttosto muovendo nella direzione di una programmazione di sistemi che si evolvono e "migliorano" sulla base della propria stessa esperienza (c.d. *machine learning*). In questo modo, le risposte che il sistema è in grado di fornire dipendono non più solamente dagli *input* che sono immessi dall'uomo, ma sono anche frutto dell'analisi predittiva (in questo senso "intelligente") degli stessi *output* che sono stati generati precedentemente dal sistema stesso. In questo modo, può diventare difficile per gli stessi programmatori comprendere le sequenze logiche seguite dal sistema, che funzionano in modo completamente autarchico: quest'ultimo è in grado di imparare continuamente da se stesso e di assumere decisioni "autonomamente", senza la necessità che l'uomo immetta degli *input*[70]. Persino il Libro Bianco della Commissione europea mette in guardia dal rischio che l'uomo potrebbe non avere i «mezzi per verificare come sia stata presa una determinata decisione

[68] R. V. PICARD, *Affective computing,* MIT Press, Cambridge, 1997.
[69] G. MOBILIO, op. cit., 43-44; D. LESLIE, *Understanding bias in facial recognition technologies: an explainer,* in *The Alan Turning Institute,* 2020, 33.
[70] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino, 2018, 294 ss.

con il coinvolgimento di sistemi di IA e, di conseguenza, se sia stata rispettata la normativa pertinente»[71].

Non a caso, i maggiori sviluppi nel settore del riconoscimento facciale si sono avuti negli ultimi anni grazie allo sviluppo del *machine learning,* che ha consentito di raggiungere risultati prima d'allora impensabili. Con riferimento specifico alle TRF, gli algoritmi vengono "allenati" a ricavare autonomamente, a partire da enormi *dataset* di immagini, le caratteristiche dei volti che si ritengono più ricorrenti, per gradi successivi di astrazione, a prescindere, quindi, dal fatto che l'uomo abbia "insegnato" alla macchina come riconoscere un volto e a distinguere le singole parti. In buona sostanza, l'uomo scrive l'algoritmo e specifica quali siano le caratteristiche da ricercare (i c.d. *pattern,* come bocca, naso, occhi), ma poi sarà l'algoritmo stesso a ricercare automaticamente tali caratteristiche, a partire dallo stacco tra la linea degli occhi e la fronte, tra le labbra e la pelle e così via[72].

Un discorso simile vale anche per gli algoritmi di *deep learning,* che si avvalgono di reti molti simili alle reti neurali, ma distribuite su un numero elevato di strati: ogni strato è composto da vari nodi, ognuno dei quali riceve *input* e restituisce *output.* Durante la fase di allenamento (c.d. *training*), la rete neurale è in grado di imparare autonomamente dai propri errori, sfruttando il "peso" delle connessioni che si instaurano tra i "neuroni" – diventando ogni volta sempre più efficace per il problema che si vuole risolvere. Si comprende bene come il funzionamento logico di tali macchine sfugga al totale controllo dell'uomo[73].

Negli ultimi anni, il *deep learning* ha avuto un notevole impatto e ha prodotto ottimi risultati con riguardo ai sistemi di riconoscimento facciale. Gli algoritmi di *deep learning* hanno permesso di superare alcuni limiti presentati dal machine learning, in particolare quelli relativi alle tecniche di estrazione delle caratteristiche[74]. Ad esempio, utilizzando algoritmi di *deep learning*, un sistema è in grado di captare i *pixel* di un'immagine, anche molto sfuocata, farli passare attraverso i vari strati della propria rete

---

[71] COMMISSIONE EUROPEA, *Libro Bianco sull'Intelligenza Artificiale – Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19 febbraio 2020, 13.
[72] A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo,* Il Saggiatore, Milano, 2019, 65.
[73] N. ALAY, H. H. AL-BAITY, *Deep learning approach for multimodal biometric recognition system based on fusion of Iris, Face and Finger Vein Traits,* Sensors*,* 2020.
[74] *Ibidem*.

e riuscire a stabilire se l'immagine rappresenti un cane, un gatto o una persona[75]. Nel 2012, ha destato scalpore la capacità degli algoritmi di *Google* di distinguere tra volti umani e felini[76]. Ad oggi, essi sono in grado non solo di distinguere un viso umano, ma addirittura anche di distinguere volti appartenenti alla medesima persona e, conseguentemente, di classificarli in base alla persona cui appartengono[77].

Nondimeno, tra i principali fattori che possono consentire all'Intelligenza Artificiale e alle TRF di progredire, o di arrestarsi, rientra senz'altro la grande disponibilità di big data. Com'è stato efficacemente osservato, se l'IA rappresenta il motore della rivoluzione digitale, i dati sono il carburante[78].

Con il termine "*big data"* non si intende semplicemente una quantità enorme di dati o di immagini da elaborare, ma altre sono le caratteristiche intrinseche che li descrivono: volume, varietà, velocità dei dati, che costituiscono le celebri "tre V". Più nello specifico, il volume dei dati raccolti rappresenta la caratteristica preminente dei *big data:* ad esempio, nel 2017, Mark Zuckerberg ha dichiarato che due milioni di utenti al mese si iscrivono a Facebook, i quali postano 350 milioni di foto al giorno[79], mentre si prevede che nel 2025 verrà raccolta una mole di dati pari a 163 *zettabyte.* La varietà dei dati si riferisce, invece, all'eterogeneità delle fonti da cui vengono estratte le informazioni. Infine, la velocità dei dati si riferisce non solo ai tempi con cui le banche dati vengono implementate, ma anche alla necessità di processare i dati in maniera rapida, quasi in tempo reale (c.d. *reale-time action* e *real time processing*). Nonostante siano state individuate numerosissime altre caratteristiche dei *big data* (addirittura si parla di 70 V), quella che maggiormente rileva – e che permette di qualificarli come "bene economico" – è la capacità di estrarre valore (economico) dai *big data* e, conseguentemente, di crearci sopra un *mercato implicito*, di cui non abbiamo ancora compreso bene i contorni[80].

---

[75] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino, 219-220.
[76] Cfr. L. CLARK, *Google's Artificial Brain Learns to Find cat Videos,* in *Wired,* 26 giugno 2012, in https://www.wired.com/2012/06/google-x-neural-network/.
[77] Cliccando sul singolo volto, Google è in grado di restituire tutte le immagini presenti sul dispositivo che corrispondano al volto della medesima persona: G. MOBILIO, op. cit., 55.
[78] M. PURDY, P. DAUGHERTY, *Why artificial intelligence is the future of growth,* Accenture, 2016, 11.
[79] J. BENNET, *Saving face: Facebook Wants Access Without Limits,* in *The Center for Public Integrity,* 31 luglio 2017, in https://publicintegrity.org/inequality-poverty-opportunity/saving-face-facebook-wants-access-without-limits/.
[80] M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo,* Il Mulino, Bologna, 2019, 25 ss.; inoltre, STUDIO LEGALE MONDINI RUSCONI, *Big data: privacy, gestione, tutele: acquisizione e protezione dati, linee guida GDPR, concorrenza e mercato, proprietà intellettuale, valorizzazione,* Altalex Editore, Milano, 2018, 16 ss. descrive le tre diverse fasi che compongono la c.d. «filiera del dato», in grado di trasformare i dati grezzi in nuove informazioni economicamente rilevanti.

La possibilità di disporre di una enorme quantità di dati ha implementato anche il settore del riconoscimento facciale. Tuttavia, ciò che preme mettere in luce è che – come già osservato – dal momento che gli algoritmi non sono in grado di comprendere il significato dei dati e delle immagini processate, ma sviluppano schemi e correlazioni su base statistica, il rischio paventato da queste tecnologie consiste nella possibilità di "forzare" i dati, individuando correlazioni e nessi inesistenti sul piano della causalità, sviluppandosi tutto su un piano statistico. Il pericolo maggiore è quello di rievocare le conclusioni cui è giunto il determinismo antropologico di carattere lombrosiano, secondo il quale determinate caratteristiche somatiche rivelano una presunta degenerazione morale dell'individuo, che è naturalmente portato a diventare un criminale[81]. In questo senso, analizzando i tratti somatici, le TRF sarebbero in grado di prevedere l'orientamento sessuale di una persona[82] ovvero alcuni tratti della personalità, come nevroticismo o scrupolosità[83]. Si stanno, infine, mettendo a punto anche altre applicazioni, come dei moderni poligrafi che sono in grado di capire dalle espressioni facciali se la persona stia mentendo o dicendo la verità[84].

Nella prima fase di tale schema tripartitico, troviamo la fase di *input,* vale a dire la generazione e cattura dei dati grezzi (o "informazioni di primo livello") che possono essere raccolti e archiviati in *data-warehouses* o in piattaforme; la fase di *output* riguarda l'attività di elaborazione e manipolazione dei dati grezzi, secondo diverse tecniche (*data mining e cleansing, data aggregation e integration, analytics*); all'ultimo stadio, vi è la fase di *insight,* cioè la creazione del nuovo valore (o "informazione di secondo livello"), che rappresenta la fase economicamente più rilevante, in quanto qui risiede il valore aggiungo dei *big data.*

[81] F. MANTOVANI, *Il problema della criminalità. Compendio di scienze criminali,* Cedam, Padova, 1984, 99 ss.

[82] Cfr. Y. WANG, M. KOSINSKY, *Deep neural networks are more accurated than humans at detecting sexual orientation from facial images,* in *Journal of personality and Social Psycology,* 114 (2), 2018. Questo studio si basa sulla c.d. teoria dell'ormone prenatale, secondo la quale ci sarebbe una correlazione l'orientamento sessuale di una persona e la vita prenatale.

[83] Cfr. A. KACHUR et AL, *Assessing the big five personality traits using real-life static facial images,* in *Nature Scientific Reports 10,* Article number: 8487*,* 2020. In tale studio sono stati analizzati 1.245 individui tramite il ricorso a reti neurali artificiali.

[84] Cfr. J. BITTLE, *Lie detectors have always been suspect. AI has made the problem worse,* in *MIT Technology Review,* 13 marzo 2020.

# CAPITOLO SECONDO

# LA DISCIPLINA DELLE TECNICHE DI RICONOSCIMENTO FACCIALE NELL'ORDINAMENTO ITALIANO

## 2.1. La cornice normativa del trattamento dei dati biometrici: il Regolamento (UE) 2016/679 e il d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018 e dalla L. n. 205/2021

Innanzitutto, bisogna prendere atto della circostanza che né a livello europeo, né a livello nazionale – così come accade anche in altri ordinamenti giuridici – è prevista una normativa che disciplini espressamente le tecniche di riconoscimento facciale. Di conseguenza, bisogna avere riguardo, innanzitutto, ai principi previsti dalla normativa sulla tutela dei dati personali, i quali possono essere applicati estensivamente anche alle TRF. Nel panorama internazionale e nazionale esiste una pluralità di strumenti posti a protezione della *privacy* e dei dati personali.

In sede internazionale, la "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" (c.d. Convenzione 108) del 1981, ratificata in Italia con la L. 21 febbraio 1989, n. 98, e la conseguente Raccomandazione n. R(87) 15 del Comitato dei Ministri per "regolamentare l'utilizzo dei dati a carattere personale nel settore della polizia", del 17 settembre 1987 – avendo previsto per la prima volta un regime di protezione dei dati personali in molti degli Stati firmatari – hanno costituito il punto di partenza della disciplina comunitaria. La c.d. Convenzione 108 è stata poi profondamente modificata da un protocollo di modifica (c.d. Convenzione 108+).

Accanto alla normativa emanata in seno al Consiglio d'Europa, è particolarmente rilevante ai fini della presente trattazione la disciplina emanata dalle istituzioni dell'UE, in attuazione dell'art. 8 TUE e dell'art. 16 TFUE: il Regolamento (UE) 2016/679, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (di seguito anche "GDPR" o "Regolamento") e la direttiva (UE) 2016/680, "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento

di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati" (di seguito anche "LED"), che insieme costituiscono il c.d. "pacchetto protezione dati"[85].

Com'è noto, il Regolamento europeo sulla protezione dei dati personali – applicabile in tutti gli Stati membri dal 25 maggio 2018 – nasce dall'esigenza di assicurare un'applicazione uniforme della normativa vigente e di fornire ai *players* internazionali un quadro giuridico certo, con il dichiarato intento di disegnare un mercato unico digitale, rimuovendo gli ostacoli costituiti dalla frammentazione della disciplina e dalla conseguente incertezza giuridica in materia di protezione dei dati personali. Allo stesso tempo, il legislatore europeo – nel segno di un clima di fiducia per lo sviluppo dell'economia digitale – ha inteso consolidare la posizione europea nel quadro globale degli ambienti *online.* Da qui la scelta dello strumento normativo: il GDPR, in ragione della fonte adottata, non si limita a promuovere un'armonizzazione in tema di protezione dei dati personali, come accadeva con la precedente Direttiva 95/46/CE (c.d. Direttiva Madre), ma è immediatamente applicabile a tutti gli Stati membri dell'Unione, senza la necessità di atti di recepimento. Sono state così eliminate *ab origine* tutte quelle piccole differenze che costituivano un freno per la realizzazione di un mercato unico digitale[86].

Ciononostante, il Regolamento europeo rappresenta un atto normativo atipico rispetto al *genus* cui appartiene, dal momento che non disciplina *in toto* la materia, ma esplicitamente rinvia alle legislazioni dei singoli Stati membri, vuoi per facoltizzare integrazioni o deroghe, vuoi per richiedere opportunamente l'intervento dei legislatori

[85] Invero, dato che il quadro giuridico risulta alquanto frammentario, i due strumenti normativi non sempre sono perfettamente coordinati e coerenti tra di loro nello stabilire la disciplina e il livello di protezione effettivo dei dati personali, con pregiudizio sia per la tutela del singolo sia della cooperazione tra le autorità pubbliche. In particolare, GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati,* WP233, 1° dicembre 2015, 4, sottolinea che il Regolamento prevede garanzie di protezione più elevate e impone obblighi più stringenti al titolare del trattamento rispetto alla LED; inoltre l'ambito di applicazione della LED può essere più o meno esteso, a seconda di come venga interpretata e attuata dai singoli Stati membri la nozione di "autorità competente" di cui all'art. 3, par. 1, n. 7 della LED, con la conseguenza che le autorità di contrasto appartenenti a diversi Stati membri potrebbero essere tenute ad osservare discipline diverse a seconda del diverso modo in cui è stata declinata tale nozione. Nonostante tali problematiche di coordinamento, va sottolineato che numerose previsioni della LED ricalcano o riprendono quelle contenute nel GDPR.

[86] G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 13-14.

nazionali con riferimento a quegli aspetti della disciplina che risentono delle specificità nazionali[87].

A tale compito non si è sottratto il legislatore italiano che, dopo un dibattito vivace nei toni e un lungo e travagliato *iter*, ha deciso di mantenere la veste esteriore del Codice per la protezione dei dati personali per il d.lgs. 30 giugno 2003 n. 196 (di seguito anche "Codice *privacy*"), il quale è stato novellato ad opera del d.lgs. n. 101/2018 e dal D.L. n. 139/2021, convertito, con modificazioni, dalla L. 205/2021[88]. Dunque, muovendo dalla fonte sovraordinata, sono state eliminate tutte quelle disposizioni del Codice *privacy* – adottato in attuazione della Direttiva Madre oramai abrogata – che erano incompatibili con la nuova disciplina contenuta nel Regolamento. In definitiva, gran parte del Codice *privacy* è stata sostanzialmente abrogata.

Il quadro normativo va integrato con la LED, che si presenta come una direttiva complementare rispetto al GDPR, in quanto la finalità di tutela dei dati personali deve essere contemperata con la necessità di prevenzione e repressione dei reati: da qui la scelta di ricorrere allo strumento della direttiva e di rimettere un significativo margine di discrezionalità ai singoli Stati membri dell'Unione[89].

Recepisce pressoché integralmente i contenuti della direttiva il d.lgs. n. 51/2018, attuativo della LED nel nostro ordinamento giuridico.

La lettura del quadro verrà poi completata dagli atti adottati, nell'esercizio della loro funzione paranormativa, sia dal Garante europeo per la protezione dei dati personali (anche GEPD o EDPS) sia dal Garante della *privacy* italiano, nonché dal Comitato europeo per la protezione dei dati personali (anche EDPB), i quali nel tempo hanno

[87] S. SCAGLIARINI, *Il nuovo codice in materia di protezione dei dati personali: la normativa italiana dopo il d.lgs. n. 101/2018,* G. Giappichelli Editore, Torino, 2019, 3. Del resto, il termine di due anni tra l'entrata in vigore e l'effettiva applicazione del Regolamento era giustificata dall'esigenza di lasciare ai legislatori nazionali il tempo per adeguarsi alla nuova disciplina sulla protezione dei dati personali.

[88] In senso critico si esprime G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 3 ss., che sottolinea come, a seguito di un vivace dibattito, si è scelto di mantenere in vita tre diversi strumenti normativi (il Regolamento, il Codice *privacy* e il d.lgs. n. 101/2018), nonostante la Commissione incaricata dal Ministero della Giustizia – presieduta proprio da G. FINOCCHIARO – ritenesse più razionale, in un'ottica di semplificazione e riordino, eliminare il Codice *privacy* e trasferire le sopravvissute disposizioni del Codice nel decreto, lasciando agli operatori due soli testi normativi. In seguito all'entrata in vigore del Regolamento (UE) 2016/679, risultano abrogate quelle norme del d.lgs. n. 196/2003 relative al trattamento dei dati in generale, mentre sono state profondamente modificate le previsioni relative alle peculiarità dell'ordinamento nazionale, come il diritto del lavoro, penale o amministrativo, oltre alle numerose disposizioni finali e di coordinamento.

[89] T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework,* in *Computer Law e Security Review,* Volume 33, Issue 33, 2017, 328 ss.

favorito una concretizzazione dei precetti legislativi e una più effettiva tutela dei dati personali.

Da ultimo, nel corso della trattazione si farà frequentemente cenno anche gli indirizzi giurisprudenziali elaborati dalla Corte di Giustizia dell'Unione (c.d. CGUE) e della Corte europea dei diritti dell'uomo (c.d. Corte EDU), tenendo conto del diverso rango riconosciuto alle norme appartenenti ai due ordinamenti, essendo riconosciuta alle prime la prevalenza sul diritto interno incompatibile e rivestendo le seconde la qualità di norme "interposte" che integrano il parametro costituzionale ai sensi dell'art. 117, c. 1, Cost.

Ne risulta un quadro composito, costituito da diversi livelli normativi e paranormativi, regole di *hard law* e di *soft law*[90].

### 2.1.1. *(Segue):* Le condizioni di liceità per il trattamento dei dati biometrici: la necessità di un consenso esplicito

Primo aspetto da chiarire è il regime giuridico dei dati che sono estratti dal procedimento di riconoscimento facciale, vale a dire i dati biometrici.

Innovando rispetto alla disciplina previgente[91], il Regolamento, la LED e la Convenzione 108+ introducono una specifica definizione di "dato biometrico", prevedendo per tale categoria di dati una precisa disciplina.

Ai fini del presente discorso, rileva anzitutto la distinzione tra "dato personale" e "dato biometrico": per "dato personale" si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. «interessato»); 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»[92]. I "dati biometrici" – i quali rientrano nell'alveo delle «categorie particolari di dati» disciplinati all'art. 9 del Regolamento – sono, invece, qualificati come «i dati

[90] G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 5.
[91] La direttiva 95/46/CE e la Convenzione 108 non dettavano una definizione specifica di "dato biometrico", facendo solamente riferimento alla più generale categoria di "dato personale".
[92] Art. 4, par. 1, n. 1 del Regolamento e art. 3, par. 1, n. 1 della LED.

personali *ottenuti da un trattamento 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»[93].

In particolare, le immagini facciali vanno inquadrate nella nozione di "dato personale" quando non sono idonee a identificare di per sé il soggetto ritratto ovvero a ricollegarlo alle sue generalità (si pensi alle comuni fotografie)[94]. Viceversa, le fotografie e le videoriprese rientrano nel novero dei "dati biometrici" solamente ove ricorrano i criteri indicati dalla normativa, afferenti alla *natura dei dati* (si deve trattare di «dati che riproducono le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica»); ai *mezzi* e alle *modalità del trattamento* (si deve trattare di «dati ottenuti mediante la loro sottoposizione ad un trattamento tecnico specifico»); alla *finalità del trattamento* (i dati devono essere «finalizzati a identificare in modo univoco una persona fisica»)[95].

Diviene, dunque, fondamentale indagare non solo la natura dei dati e le modalità con cui essi sono trattati, ma anche le diverse finalità perseguite mediante il riconoscimento facciale.

Senza alcun dubbio, la disciplina sui dati biometrici si applica nel caso in cui la finalità della raccolta sia l'identificazione di un soggetto attraverso una comparazione uno-a-molti (1-n), mentre la questione è più complessa nel caso di verifica/autenticazione, che comporti una comparazione uno-a-uno (1-1). Con riguardo a tale finalità, il Comitato europeo per la protezione dei dati ha espressamente chiarito[96] che si configura un trattamento di dati biometrici, rientrante nell'ambito di applicazione dell'art. 9 del Regolamento, nel caso in cui non sia nota l'identità del soggetto, ma comunque il sistema di riconoscimento facciale effettui una conservazione del *template* biometrico, anche solo qualora i dati siano utilizzati esclusivamente come modelli di riferimento per tracciare l'interessato. Da ciò consegue che la disciplina *de qua* si applica sia nei casi in cui la verificazione avvenga nei confronti di persone conosciute e ben determinate, sia nei casi in cui non vi sia la possibilità di risalire all'interessato, ma avvenga la conservazione del

[93] Art. 4, par. 1, n. 14 del GDPR e art. 3, par. 1, n. 13 della LED; enfasi aggiunta.
[94] Considerando n. 51 al GDPR; Cfr. anche COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020, 7; G. MOBILIO, op. cit., 137-138.
[95] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020, 19.
[96] *Ivi*, 20.

*template* biometrico – nel qual caso sarebbe più opportuno parlare di semplice "rilevamento" che non di autenticazione o verificazione[97].

All'opposto, se il sistema impiega esclusivamente algoritmi di *"face detenction",* ma non di *"face recognition",* vale a dire algoritmi di mero rilevamento del viso, senza che vi sia alcuna conservazione del modello biometrico, non si ricade nel regime giuridico relativo ai dati biometrici, ma si applica la disciplina generale in tema di dati personali «comuni»[98].

Nel caso in cui, infine, la finalità del trattamento sia quella di operare categorizzazioni, ossia classificare le persone in categorie specifiche, in base a determinati attributi (quali età, sesso, abitudini di consumo e così via), senza che però avvenga l'identificazione dell'interessato e la conservazione del *template* biometrico, non si ricade nell'ambito di applicazione dei dati biometrici; tuttavia, nel caso in cui tali dati siano idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale oppure i dati genetici, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, si ricade nel novero delle «categorie particolari di dati», comunque sottoposte alla disciplina di cui all'art. 9, par. 1 del GDPR.

Ebbene, a seconda che l'immagine facciale rientri nell'una o nell'altra categoria di dati, troverà applicazione una disciplina parzialmente differente.

Anzitutto, principio cardine in materia di protezione dei dati personali è il principio di liceità, correttezza e trasparenza, in virtù del quale i dati personali devono essere «trattati in modo lecito, corretto e trasparente nei confronti dell'interessato»[99]. Tale principio si esplica in modo differente in ragione della distinzione sopra operata tra dati biometrici e dati non biometrici (o anche, dati «comuni»).

---

[97] Nel caso appena descritto, il processo non si conclude con la fase di *matching* – in cui il sistema procede alla comparazione dei *template,* al fine di determinare il loro grado di somiglianza – ma si arresta alla fase di registrazione, con la conservazione dell'immagine o del modello biometrico nel *database.* Di conseguenza, non avviene alcuna autenticazione o verifica. Si veda, *infra,* nel Capitolo Primo, paragrafo §1.2.

[98] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria,* 21 dicembre 2017 (doc. web. 7496252). In questo caso, va osservato che, addirittura, il processo si arresta ancor prima, vale a dire alla fase di estrazione delle caratteristiche, in cui il *software* estrae le c.d. caratteristiche biometriche distintive della persona e le converte in una rappresentazione matematica, cioè in una stringa di caratteri alfanumerici, ottenendo in tal modo il c.d. *template* o "modello biometrico". Si veda, *infra,* nel Capitolo Primo, paragrafo §1.2.

[99] Art. 5, par. 1, lett. a) del Regolamento UE 2016/679.

Nei rari casi in cui le TRF producano dati non biometrici, si applica la disciplina generale dettata con riferimento ai dati personali[100].

In particolare, l'art. 6 del Regolamento fissa i presupposti di legittimità del trattamento dei dati personali, che il legislatore europeo definisce «condizioni», enfatizzando il loro ruolo di *condicio sine qua non* nell'ambito del processo di valutazione della liceità del trattamento. Peraltro, a differenza del precedente impianto normativo[101], il GDPR contempla condizioni tra loro equiordinate, essendo necessario (ma non sufficiente) che ve ne sia almeno una per ritenere fondato il giudizio di liceità[102].

Innanzitutto, la tutela del soggetto i cui dati personali sono oggetto di trattamento viene assicurata mediante l'obbligo – posto a carico del titolare del trattamento – di raccogliere il suo consenso all'utilizzo dei dati personali per una o più specifiche finalità. A tale condizione, che indubbiamente mantiene grande rilevanza, fanno seguito altri cinque presupposti di legittimazione al trattamento, alternativi tra loro: il trattamento è lecito qualora (i) sia necessario procedere all'esecuzione di obblighi contrattuali o precontrattuali ovvero (ii) quando il titolare pone in essere il trattamento per adempiere ad un obbligo di legge ovvero (iii) di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ovvero (iv) qualora il trattamento risulti necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica ovvero (v) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi[103].

Come abbiamo avuto modo di anticipare, tuttavia, nella maggior parte dei casi, le immagini facciali costituiscono dati biometrici, rientranti oggi nel novero delle «categorie particolari di dati personali» di cui all'art. 9 del GDPR[104].

---

[100] G. MOBILIO, op. cit., 144.

[101] Nel d.lgs. 196/2003, che recepiva l'ormai abrogata Direttiva 95/46/CE, si era assegnato un ruolo centrale al principio del consenso quale condizione di liceità del trattamento, assurgendo gli altri presupposti a mere eccezioni alla regola generale.

[102] F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019, 110-193.

[103] Art. 6, par. 1 del GDPR, rispettivamente lett. b), c), e), d), f). Per una disamina analitica delle diverse condizioni di liceità del trattamento si vedano, in particolare, F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* e G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019.

[104] G. MOBILIO, op. cit., 145. Rispetto alla precedente normativa, i dati biometrici (assieme ai dati genetici) sono stati inseriti *ex novo* tra le «particolari categorie di dati» di cui all'art. 9 del Regolamento, come sottolineato da A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019, 209.

In ragione della presunta intrinseca rischiosità di tali dati per i diritti e le libertà delle persone fisiche[105], nell'articolo *de quo*, il legislatore muta l'approccio di fondo nella costruzione delle «condizioni di liceità»[106], in quanto dapprima[107] pone un divieto generale di trattamento dei dati biometrici, mentre successivamente[108] prevede un elenco tassativo di ipotesi eccezionali, in presenza della quali il trattamento dei dati biometrici è consentito[109].

Così, il legislatore europeo ritiene legittimo il trattamento dei dati biometrici, quando questo è (i) fondato sul «consenso esplicito» dell'interessato; (ii) necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in determinate materie; (iii) necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona specifica; (iv) effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; (v) ha ad oggetto dati resi pubblici dall'interessato; (vi) necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; (vii) necessario per motivi di interesse pubblico rilevante; (viii) 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; (ix) necessario per motivi di interesse pubblico nel settore della sanità pubblica; (x) necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[110].

---

[105] A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019, 212.

[106] F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, Z*anichelli, Bologna, 2019, 117.

[107] Art. 9, par. 1 del Regolamento UE 2016/679.

[108] Art. 9, par. 2 del GDPR.

[109] Oltre che all'art. 9 del GDPR, le categorie particolari di dati sono elencate, salve limitate differenziazioni, anche in altri atti normativi, quali l'art. 6 della Convenzione di Strasburgo del 1981, oltre che all'art. 8 dell'abrogata Direttiva 95/46/CE. Si ricorda che la norma *de quo* indica come «categorie particolari di dati», «i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Tale definizione è stata recepita anche nel nostro Codice *privacy,* come novellato dal d.lgs. n. 101/2018. È su questa definizione che si basa la presente trattazione. Cfr. A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, 206 ss.

[110] Art. 9, par. 2, rispettivamente lett. a), b), c), d), e), f, g), h, i), j), del Regolamento UE 2016/679.

Beninteso, la sussistenza di una di tali condizioni non è elemento di per sé sufficiente a fondare la liceità del trattamento dei dati biometrici. Come avremo modo di approfondire, in presenza di dati biometrici, il Regolamento pone in capo ai titolari (e ai responsabili) del trattamento obblighi aggiuntivi, tra cui quello di predisporre un apposito registro dei trattamenti – in alcuni casi facoltativo, ma sempre obbligatorio qualora siano trattati dati biometrici[111] –, ovvero l'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati – obbligatoria nel caso di trattamento su larga scala di categorie particolari di dati[112] – e di designare il responsabile per la protezione dei dati – egualmente obbligatorio nel caso di trattamento su larga scala di categorie particolari di dati[113].

Inoltre, in ragione della delicatezza del trattamento dei dati biometrici, l'art. 9 del GDPR prevede la possibilità per gli Stati di introdurre ulteriori limitazioni relative al trattamento di dati biometrici. Esercitando tale facoltà, l'art. 2-septies del d.lgs. n. 196/2003 prevede che il Garante della *privacy* italiano possa assumere un provvedimento generale con cui individuare le misure di garanzia le eventuali altre misure necessarie per garantire i diritti degli interessati[114].

Venendo ad una disamina più completa delle condizioni di liceità del trattamento dei dati biometrici, pare opportuno, anzitutto, soffermare l'attenzione sulla necessità di ottenere «un consenso *esplicito* al trattamento di tali personali per una o più finalità specifiche»[115].

Il consenso dell'interessato è espressamente qualificato come «qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati che lo riguardano siano oggetto di trattamento»[116]. Tale

[111] Art. 30, par. 5 del Regolamento UE 2016/679.
[112] Art. 35, par. 3 lett. b) del GDPR.
[113] Art. 37, par. 1 lett. c) del Regolamento UE 2016/679. Con riguardo agli obblighi aggiuntivi summenzionati, si rinvia, *infra,* in questo capitolo, §2.1.6.
[114] Rispettivamente, art. 9, par. 4 del Regolamento UE 2016/679 e art. 2-*septies*, c. 5 del d.lgs. 196/2003. Si veda, *amplius,* il paragrafo §2.1.8, reso a commento dell'art. 2-*sexies* e 2-*septies* del Codice.
[115] Art. 9, par. 2, lett. a) del GDPR.
[116] Art. 4, par. 1, n. 11 del Regolamento UE 2016/679. Quanto all'inquadramento giuridico, F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, 140 afferma che il consenso *de quo* ha «natura autorizzatoria di tipo integrativo»: anzitutto, l'autorizzazione, diversamente dall'approvazione, deve essere preventiva e non successiva rispetto al trattamento; in secondo luogo, essa è di tipo integrativo, in quanto – similmente all'autorizzazione amministrativa – è idonea a rimuovere un limite all'esercizio di un diritto o di un potere che già è stato attribuito dalla legge al soggetto interessato. Laddove l'ordinamento richieda il consenso dell'interessato, quest'ultimo ha il potere di effettuare egli stesso una valutazione, e un conseguente bilanciamento, fra tutti gli interessi in gioco; in altre ipotesi è lo stesso titolare che opera aprioristicamente tale bilanciamento, sulla

definizione fissa i requisiti del consenso: il medesimo deve essere *libero*, *specifico*, *informato* e *inequivocabile*.

Anzitutto, il consenso deve essere espresso *liberamente* e *specificamente* in merito ad un trattamento, o ad una parte di esso, chiaramente individuato. Da ciò discende, da un lato, la necessità che l'interessato abbia una «scelta effettiva» in merito alla propria manifestazione di volontà e «il controllo sui propri dati»[117] e, dall'altro, che il consenso sia reso con riferimento ad aspetti del trattamento individuati in modo puntuale e non generico. Lo stesso, poi, deve essere *informato*, essendo richiesto che l'interessato abbia piena conoscenza di tutte le informazioni relative al trattamento[118], in ossequio al principio di completezza. Altro requisito del consenso è la sua *inequivocabilità,* nel senso che l'autorizzazione deve essere espressa mediante un atto positivo che non possa essere travisato nel suo significato.

Da ultimo, con riferimento ai dati biometrici, l'art. 9 del Regolamento richiede espressamente che il consenso sia, in più, *esplicito,* nel senso che, generalmente, esso deve essere reso mediante dichiarazione scritta, in modo tale che sia possibile «dissipare tutti i possibili dubbi e la potenziale mancanza di prove in futuro»[119].

Altra importante novità introdotta nel nuovo assetto normativo è data dalla previsione esplicita del diritto dell'interessato di revocare in qualsiasi momento il proprio consenso, «con la stessa facilità» con cui esso è stato prestato[120].

base di scelte di politica legislativa (ad esempio, nell'ipotesi in cui il trattamento sia necessario per il perseguimento del legittimo interesse del titolare); in altri casi il bilanciamento medesimo è rimesso al legislatore (come nel caso in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico).

[117] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679,* WP259, 28 novembre 2017.

[118] In particolare, quelle informazioni individuate agli artt. 13 e 14 del Regolamento UE 2016/679.

[119] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679,* WP259, 28 novembre 2017.

[120] Art. 7, par. 3, del GDPR.

### 2.1.2. *(Segue):* Il riconoscimento facciale in presenza di "interessi pubblici rilevanti": i principi di proporzionalità e di necessità

Altra ipotesi particolarmente rilevante in cui è lecito il trattamento di dati biometrici, in deroga al divieto generale sancito dall'art. 9 del GDPR, si ha nel caso in cui il trattamento di tali dati avvenga per «motivi di interesse pubblico rilevante»[121].

Perché il divieto sia inoperante, tuttavia, il trattamento dei dati biometrici deve rispettare una serie di condizioni: quanto alla finalità, il trattamento deve essere *necessario* per motivi di interesse pubblico rilevante e deve essere *proporzionato* alla finalità perseguita; quanto al *fondamento giuridico*, esso deve essere individuato «sulla base del diritto dell'Unione o degli Stati membri»; quanto alle garanzie offerte, è richiesto che il trattamento rispetti «l'essenza del diritto alla protezione dei dati» e preveda «misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Dunque, ai fini di un accertamento circa la legittimità o meno del trattamento dei dati biometrici, due sono i profili principali di cui tenere conto: da un lato, è necessario che vi sia una chiara disciplina normativa che costituisca il fondamento giuridico del trattamento; dall'altro lato, è necessario che sia garantito il rispetto dei principi di proporzionalità e di necessità nelle limitazioni dei diritti che potrebbero essere lesi.

Quanto al primo aspetto, il ruolo da riconoscere alla previsione normativa è chiaramente messo in luce dalla Corte EDU, la quale più volte ha precisato che, affinchè le limitazioni al rispetto della vita privata di cui all'art. 8 CEDU siano «previste dalla legge», non è sufficiente un generico richiamo alle finalità da perseguire, dovendo piuttosto la legge consentire espressamente la raccolta e conservazione dei dati biometrici. Dunque, la riserva di legge richiede non soltanto l'esistenza di una base giuridica nel diritto interno, ma bisogna aver riguardo soprattutto alla "qualità della legge", che deve essere «chiara, con effetti prevedibili e accessibile all'interessato», e quindi sufficientemente precisa, in modo tale che i destinatari abbiano la concreta possibilità di conoscere la fonte normativa e ragionevolmente prevedere le conseguenze della sua applicazione[122].

---

[121] Ipotesi espressamente menzionata all'art. 9, par. 2, lett. g) del GDPR. Si veda anche l'art. 2-*sexies* del Codice *privacy,* come novellato dal d.lgs. 101/2018, per la cui trattazione si rinvia, *infra,* in questo Capitolo, al paragrafo §2.1.8.

[122] CORTE EDU, *Silver e altri c. Regno Unito,* 25 marzo 1983; CORTE EDU, *Khan c. Regno Unito,* 12 maggio 2000; CORTE EDU, *Buckley c. Regno Unito,* 29 settembre 1996.

Avendo riguardo al secondo aspetto, il canone di proporzionalità trae origine dalla Carta dei diritti fondamentali dell'Unione europea, è stato sviluppato a livello normativo dal GDPR e dalla LED e poi affinato dalla giurisprudenza della Corte di Giustizia dell'Unione e dalla Corte EDU, oltre che dal Garante europeo per la protezione dei dati personali e dal Garante della *privacy* italiano.

L'art. 52 della Carta di Nizza stabilisce che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciute dalla Carta medesima devono essere previste dalla legge, nonché rispettare il contenuto essenziale di tali diritti e il principio di proporzionalità e di necessità.

Il Regolamento precisa, d'altro canto, che il diritto alla protezione dei dati personali non è assoluto, ma va adeguatamente bilanciato con altri diritti fondamentali egualmente rilevanti, «in ossequio al principio di proporzionalità»[123]. In particolare, è possibile limitare gli obblighi e i diritti previsti agli articoli da 12 a 22 e 34 del GDPR, qualora sia necessario salvaguardare altri importanti diritti, tra i quali figurano «la sicurezza nazionale; la difesa; la sicurezza pubblica; la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali […]; altri importanti obiettivi […], anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; […]»[124].

In termini similari si esprime, in merito alla prevenzione e repressione dei reati, l'art. 10 della LED, il quale autorizza il trattamento dei dati biometrici solamente se «strettamente necessario»[125], «soggetto a garanzie adeguate per i diritti e le libertà dell'interessato» e «autorizzato dal diritto dell'Unione o dello Stato membro». In alternativa a tale ultimo requisito, la LED consente il trattamento di tali dati qualora l'interessato abbia *volontariamente* rinunciato all'anonimato[126]. Si tratta, questo, di un profilo al contempo interessante e delicato, in considerazione della massiccia presenza nella nostra società di telecamere e videocamere presenti in luoghi pubblici – installate

[123] Considerando n. 4 del GDPR.
[124] Art. 23, par. 1, lett. a), b), c), d), e), f), g) del GDPR. In aggiunta, par. 2 precisa i contenuti essenziali delle disposizioni legislative che limitano i diritti, tra i quali spiccano sicuramente «le finalità del trattamento» e «la portata delle limitazioni introdotte».
[125] Il requisito della "stretta necessità" è soddisfatto solamente qualora ci siano giustificazioni precise e solide; Cfr. GRUPPO DI LAVORO ARTICOLO 29*, Parere su alcune questioni fondamentali della direttiva (UE) 680 sulla protezione dei dati nelle attività di polizia e giustizia,* WP 258, 29 novembre 2017, 7 ss.
[126] L'art. 10, par. 1, lett. c) della LED fa riferimento a «dati resi manifestamente pubblici dall'interessato».

per i più svariati scopi – soprattutto nel caso in cui sia prevista una conservazione dei dati registrati. Come precisato più volte dalla Corte EDU[127], la volontà dell'individuo di rinunciare alla particolare protezione dei dati personali che gli è accordata dall'ordinamento deve essere esplicita, non potendo essere desunta dalla pubblicità del luogo. Allo stesso modo, con riferimento ai dati che circolano sui *social network,* restano comunque fermi tutti gli obblighi informativi a favore dell'interessato[128].

Il principio di proporzionalità è divenuto ormai una pietra miliare nella giurisprudenza della Corte di Giustizia dell'Unione, che lo richiama sovente per valutare se le limitazioni alla tutela del diritto alla protezione dei dati personali siano o meno legittime.

Secondo una definizione ormai divenuta classica, il test di proporzionalità si esplica «nella valutazione sulla *idoneità* degli atti dei pubblici poteri a realizzare gli obiettivi legittimi perseguiti dalla norma e che tali atti *non superino i limiti* di ciò che è idoneo al conseguimento degli obiettivi stessi o *eccedano* più di quanto necessario a raggiungerli»[129].

Perché possa dirsi rispettato il principio di proporzionalità, dunque, è essenziale che sia compiuta una valutazione fondata su tre criteri, da applicarsi in sequenza: idoneità, necessità e proporzionalità in senso stretto. L'idoneità mette in relazione il mezzo impiegato (*i.e.* lo strumento normativo) con gli obiettivi legittimi perseguiti dalla norma. In ossequio a tale criterio, non devono essere prese in considerazione quelle misure che non sono in grado di raggiungere il fine prescelto. La necessità mette a confronto tutte le varie soluzioni (ritenute idonee) e impone la scelta su quella che permette di sacrificare il minor sacrificio possibile di interessi e diritti. La proporzionalità in senso stretto implica la valutazione complessiva di vantaggi e degli svantaggi per gli interessi in gioco: nel

[127] Cfr. CORTE EDU, *P.G. and J.H. v. the United Kingdom,* 25 settembre 2001; CORTE EDU, *Peck v. The United Kingdom,* 28 gennaio 2003.
[128] G. MOBILIO, op. cit., 158.
[129] G. MOBILIO, op. cit., 162, che riprende la definizione di "principio di proporzionalità" tenendo conto di varie pronunce della Corte di Giustizia dell'Unione: CGUE, C-291, *Schwarz c. Stadt Bochum ,* 17 ottobre 2013, p. 45-46; CGUE, cause riunite C-293-12 e C-594, *Digital Rights Ireland Ltd,* 8 aprile 2014, p. 46-47. Del medesimo orientamento sono CGUE, *Afton Chemical,* C-343-09, 8 luglio 2010, §45; CGUE, *Volker und Markus Schecke e Eifert,* Cause riunite C-92-09 e C-93-09, 9 novembre 2010, §74; CGUE, *Nelson e a.,* cause riunite C-581-10 e C-629-10, 23 ottobre 2012, §71; CGUE, *Sky Österreich,* C-283-11, 22 gennaio 2013, §50; CGUE, *Schaible,* C-101-12, 17 ottobre 2013, §29; CORTE EDU, *Silver e altri c. Regno Unito,* 25 marzo 1983; CORTE EDU *Khan c. Regno Unito,* 12 maggio 2000; CORTE EDU *Buckley c. Regno Unito,* 29 settembre 1996.

caso in cui il pregiudizio per i diritti incisi siano eccessivi rispetto agli scopi perseguiti, allora la scelta deve essere rimessa in discussione.

Paradigmatica di questo orientamento è la nota sentenza *Digital Rights Ireland*[130], nella quale il giudice di Lussemburgo ha dichiarato l'illegittimità della c.d. direttiva *data retention* (direttiva 2006/24/CE) per violazione del principio di proporzionalità nel bilanciamento tra il diritto alla protezione dei dati personali e le esigenze di pubblica sicurezza. Secondo la Corte, tale direttiva, seppure idonea a raggiungere lo scopo per cui è stata emanata – vale a dire la lotta contro gravi reati, come quelli legati alla criminalità organizzata e al terrorismo – comporta una grave compressione nei diritti fondamentali dagli articoli 7 e 8 della Carta di Nizza, «senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario»[131]. Nel medesimo solco si pone la c.d. sentenza *Schrems*[132], nella quale la Corte – facendo sempre perno sull'art. 52 CDFUE – ribadisce che le limitazioni alla tutela dei dati personali devono essere adottate dal legislatore «nei limiti dello stretto necessario».[133]

Un analogo *standard* di validità viene adottato anche dalla Corte europea dei diritti dell'uomo, allo scopo di verificare se le limitazioni alla tutela della vita privata, e dunque anche dei dati personali, siano legittime.

Secondo i parametri utilizzati dal giudice di Strasburgo e in stretta connessione con la dottrina del "margine di apprezzamento statale"[134], la compressione di un diritto

---

[130] CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite n. C-293/12 e n. 594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural resouces et al.,* 8 aprile 2014.

[131] Come sottolineato da V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea,* in *Federalismi.it,* 2017, la direttiva in questione si inserisce nel quadro del difficile bilanciamento tra *privacy* e sicurezza, in quanto essa – in risposta degli attacchi terroristici di Madrid e Londra – disciplinava la conservazione dei dati di traffico telefonico e telematico da parte dei fornitori di servizi di comunicazioni elettroniche, al fine di accertamento e repressione di gravi reati, ma erano del tutto carenti «regole chiare e precise che disciplinino la portata della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati».

[132] CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite n. C-362-14, *Maximillian Schrems c. Data Protection Commissioner,* 6 ottobre 2015.

[133] Come osserva V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea,* in *Federalismi.it*, 17, è significativo che ancora una volta il vaglio di proporzionalità operato dalla Corte di Giustizia riguardi il difficile contemperamento tra esigenze investigative delle autorità svedesi e quindi, in ultima istanza, esigenze di sicurezza nazionale e dall'altro lato, tutela dei dati personali dei cittadini europei.

[134] I. ANRO', *Il margine di apprezzamento nella giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei Diritti dell'uomo* in F. COSTAMAGNA, A. ODDENINO, E. RUOZZI,

rilevante ai sensi della Convenzione deve essere prescritta dalla legge (presupposto formale); in secondo luogo, essa deve essere considerata «necessaria in una società democratica», requisito che si estrinseca nella ricerca di proporzionalità tra i mezzi adoperati e il fine perseguito[135]. Come precisato più volte dalla medesima Corte, l'aggettivo "necessario" non equivale a "utile", "ragionevole" o "auspicabile", ma implica la presenza di «una pressante esigenza sociale», la cui esistenza che deve essere valutata discrezionalmente da ciascuna autorità nazionali[136].

Le considerazioni appena svolte trovano riscontro nella giurisprudenza del Garante europeo per la protezione dei dati e del Gruppo di lavoro "Articolo 29" – oggi Comitato europeo per la protezione de dati – e negli orientamenti del Garante della *privacy* italiano, ove i principi di proporzionalità e di necessità orientano in maniera decisiva le decisioni di tali Autorità, per la cui trattazione si rinvia al Capitolo successivo.

### 2.1.3. *(Segue):* Il principio di limitazione delle finalità e i c.d. trattamenti secondari

Fermo il rispetto delle condizioni di liceità del trattamento[137], la raccolta dei dati personali è improntata all'ulteriore principio di limitazione delle finalità, in base al quale i dati personali devono essere trattati per scopi precisi, espliciti e legittimi, sia nella raccolta che nelle altre attività di cui si compone il trattamento[138]. Or dunque, è chiaro che il principio in parola si compone di due parti, che meritano di essere analizzate separatamente.

Innanzitutto – e questo rappresenta secondo l'opinione del Gruppo di lavoro Articolo 29 un "prerequisito" di ogni trattamento – i dati personali devono essere *raccolti* per finalità determinate (cioè sulla base di un'attenta e specifica indagine degli scopi per

A. VITERBO, L. MOLA, L. POLI (a cura di), *La funzione giurisdizionale nell'ordinamento dell'ordinamento internazionale e nell'ordinamento comunitario*, Editoriale Scientifica, Napoli, 2010, 7-28 (contributo in opera collettanea).

[135] CORTE EDU, *S. e Marper c. Regno Unito,* 4 dicembre 2008. In tale decisione, la Corte EDU – facendo esplicito riferimento all'art. 8 CEDU – sancisce che le modalità di conservazione dei profili genetici previste dal *Nation DNA Database* inglese integra una violazione del diritto alla *privacy,* in quanto non rispetta i criteri sopraelencati, quali il principio di legalità, di necessità e di proporzionalità.

[136] CORTE EDU, *Dudgeon c. Regno Unito*, §51-53; CORTE EDU, *Z. c. Finlandia*, 3 dicembre 1996, §94; CORTE EDU, *Piechowicz c. Polonia*, §212; CORTE EDU, *Paradiso e Campanelli c. Italia,* 24 gennaio 2017; CORTE EDU, *A.-M.V. c. Finlandia*, 14 novembre 2019.

[137] Art. 6 del Regolamento UE 2016/679.

[138] Art. 5, par. 1, lett. b) del GDPR e art. 4, par. 1, lett. b) della LED. Similmente, l'art. 5, par. 4 lett. b) della Convenzione 108+ dispone che i dati automatizzati devono essere registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini.

cui i dati personali saranno utilizzati, escludendo la raccolta di dati inutili o superflui[139]), esplicite (cioè chiaramente spiegate, evitando formulazioni vaghe e generiche, avendo anche riguardo alla formazione culturale e linguistica del destinatario[140]) e legittime (nel senso che devono rispettate tutte le norme in materia di protezione dati e tutte le normative applicabili al caso concreto[141]).

Una volta raccolti i dati, essi devono essere «successivamente *trattati* in modo che non sia incompatibile con tali finalità» (enfasi aggiunta): è richiesto che ogni successiva operazione rientri nel novero di quelle finalità che *ex ante* sono state individuate dal titolare stesso. Sembra, dunque, opportuno delimitare il requisito della "non incompatibilità", alla luce delle indicazioni fornite dal Gruppo di Lavoro Articolo 29. Innanzitutto, ai fini del giudizio di compatibilità, possono essere seguiti due diversi approcci: un approccio formale, in forza del quale il titolare deve raffrontare le finalità indicate dal titolare e qualsiasi ulteriore operazione, verificando che quest'ultima sia ricompresa nel senso letterale di quanto dichiarato; in alternativa, un approccio sostanziale, in forza del quale bisogna prescindere dalla formulazione letterale, valorizzando il contesto e le reali intenzioni del titolare del trattamento. È da preferire il secondo metodo, in quanto, nonostante il primo appaia più neutrale, la sua rigida applicazione potrebbe portare alla necessità di formulare informative eccessivamente lunghe e incomprensibili, mentre il secondo è più flessibile ed efficace[142].

Il fondamento logico del principio *de quo* – che si fonda sulla stretta relazione tra motivi della raccolta e l'effettivo impiego durante le operazioni di trattamento – è da rinvenire nella costante tensione tra la rapida evoluzione tecnologica, imperniata sui *Big Data* e *Open data,* con il diritto fondamentale dell'individuo alla protezione dei propri

[139] Le finalità devono essere identificate nello specifico dal titolare del trattamento nel momento in cui avviene la raccolta. Il titolare può anche raccogliere di dati personali per più finalità, purché rispetti tale principio. Come si ricava da un esempio tratto da GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2012 on purpose limitation del 2 aprile 2013*, 569/13/EN - WP 203, nel caso in cui l'imprenditore fornisce servizi differenti (ad esempio, *email*, *social*, caricamento foto e video), egli è tenuto ad indicare con un certo livello di dettaglio tutte le finalità, in modo conciso e facilmente comprensibile, eventualmente dividendo le varie finalità in sub-finalità – rispondendo tale *modus operandi* anche alla finalità di consentire al titolare del trattamento di verificare la correttezza delle operazioni delegate ad altri soggetti.

[140] Tale requisito deve essere rispettato non solo a beneficio dei possibili interessati, ma anche delle autorità di controllo, le quali devono poter valutare la corrispondenza tra lo scopo indicato al momento della raccolta e lo scopo effettivamente perseguito.

[141] STUDIO LEGALE MONDINI RUSCONI, *Big data: privacy, gestione, tutele: acquisizione e protezione dati, linee guida GDPR, concorrenza e mercato, proprietà intellettuale, valorizzazione,* Altalex Editore, Milano, 2018, 119 ss.

[142] *Ibidem.*

dati personali: in virtù del principio di autodeterminazione, l'interessato deve pur sempre mantenere una qualche forma di controllo sui propri dati[143].

Tuttavia, nonostante il titolare del trattamento debba prevedere *ex ante* e in modo chiaro le finalità da perseguire, il legislatore europeo si mostra consapevole che tali dati personali potranno essere sottoposti a trattamenti ulteriori (c.d. *trattamenti secondari*). Nello specifico, il GDPR dispone che il trattamento per una finalità diversa è compatibile con le finalità per cui i dati sono stati raccolti, se ricorrono una serie di condizioni, in assenza delle quali il titolare del trattamento potrà richiedere un nuovo consenso ovvero far riferimento alle ipotesi sopracitate nelle quali il consenso non è necessario[144]. Nel caso in cui ricorrano altre condizioni di liceità[145], non è richiesta una base giuridica separata.

Viceversa, la LED è più elastica nel disporre le condizioni in presenza delle quali le forze di polizia possono procedere al riutilizzo dei dati personali per finalità ulteriori, purché si tratti di finalità di prevenzione, indagine, accertamento e perseguimento di reati[146]. Resta fermo, tuttavia, il principio secondo il quale la generica finalità di indagare su reati diversi da quelli in relazione ai quali i dati sono raccolti non legittima *sic et simpliciter* il loro utilizzo secondario[147].

La Corte di Giustizia, nella famosa sentenza "*Digital Rights*" già citata, sostiene che il legislatore debba individuare le «condizioni sostanziali e procedurali» per il trattamento secondario dei dati e che debba dettare criteri oggettivi che permettano di individuare il numero di persone cui compete «il diritto di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito»[148].

Allo stesso modo, la Corte di Lussemburgo, nel celebre caso *S. e Marper c. Regno Unito* – nello statuire che la conservazione *sine die* di impronte digitali, campioni cellulari e profili genetici di persone assolte dai reati per i quali erano state indagate costituisce

---

[143] G. MOBILIO, op. cit., 170.
[144] Ai sensi dell'art. 6, par. 4, del GDPR occorre far riferimento, tra gli altri, al nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità ulteriori (lett. a), il contesto di proveniente dei dati personali (lett. b), la natura dei dati personali (lett. c), le possibili conseguenze del trattamento secondario (lett. d), l'esistenza di garanzie adeguate (lett. e).
[145] Quelle menzionate all'art. 6, par. 1 del Regolamento UE 2016/679.
[146] Ai sensi dell'art. 4, par. 2 della LED è necessario che il trattamento sia conforme al diritto dell'Unione o degli Stati membri e, congiuntamente, che il trattamento sia necessario e proporzionato.
[147] GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati,* WP233, 1° dicembre 2015, 6.
[148] CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite n. C-293/12 e n. 594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural resouces et al.,* 8 aprile 2014.

una violazione del diritto alla vita privata e familiare di cui all'art. 8 CEDU – ha precisato che la legge deve prevedere adeguate garanzie contro il rischio di abusi o di riutilizzi arbitrari dei dati personali, dettando regole sufficientemente precise e dettagliate in tema di durata, conservazione, utilizzo e accesso a terzi dei dati medesimi, nonché prevedendo le procedure volte a preservare l'integrità e la riservatezza dei dati e le modalità per la loro cancellazione. [149]

L'uso delle TRF, tuttavia, disvela problematiche difficilmente arginabili. Come accade con riferimento ai *big data*[150], che anche le TRF sfruttano, assieme al c.d. "uso primario" dei dati e delle immagini digitali generati dagli utenti, è frequente da parte dei titolari del trattamento il c.d. "uso secondario" dei dati, correlato al loro "valore opzionale", il quale non è neppure prevedibile al momento della raccolta dei dati medesimi[151].

Dal momento che i dati e le immagini generati durante il processo di acquisizione sono facilmente captabili e sono raccolti in *database* in grado di raccogliere grandi quantità di informazioni, le TRF – come fotografie sul *web,* sui *social media* o nelle applicazioni *online* adibite alla loro gestione – sono spesso utilizzate con la finalità, a volte non prevedibile dal titolare al momento della raccolta, di estrarre modelli biometrici o di riconoscimento del volto, in assenza di una specifica base giuridica per questa nuova finalità, nonostante il divieto generale del Gruppo di Lavoro Articolo 29[152].

Inoltre, l'uso delle TRF da parte delle forze di polizia pone il problema di arginare le c.d. *fishing expeditions,* vale a dire la raccolta indiscriminata di immagini e di dati, rispondente allo scopo generico di raccogliere informazioni su un grande numero di sospettati[153]. Al contrario, la raccolta di dati personali per scopi di polizia dovrebbe essere limitata – in ossequio ai principi di proporzionalità e di necessità – alla prevenzione, indagine e perseguimento di uno specifico reato, ragione per cui si dovrebbe individuare una stretta ed evidente correlazione tra i dati trattati e l'indagine specifica sul soggetto

[149] CORTE EDU, *S. e Marper c. Regno Unito,* 4 dicembre 2008.
[150] *Infra,* nel Capitolo Primo, §1.2.1.
[151] M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo,* Il Mulino, Bologna, 2019*,* 27.
[152] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche,* WP193, 27 aprile 2012, 2, il quale sottolinea che sia necessario per tale nuovo trattamento il consenso della persona interessata, dovendosi comunque rispettare il principio della limitazione della conservazione, di cui si dirà più avanti.
[153] G. MOBILIO, op. cit., 172.

che ha commesso il reato[154]. Tale principio deve essere rispettato in tutte le fasi del procedimento penale, con la conseguenza che nel caso in cui un soggetto venga assolto i suoi dati devono essere cancellati[155].

### 2.1.4. *(Segue):* Il principio di minimizzazione dei dati

La raccolta dei dati personali è informata al rispetto dell'ulteriore principio di minimizzazione dei dati, il quale impone che siano raccolti esclusivamente i dati personali necessari per raggiungere la finalità per la quale è stato prestato il consenso (o per la quale sussiste la base giuridica), procedendo alla cancellazione di quelli non necessari o non conformi a tale finalità[156].

Nonostante entrambe le normative a protezione dei dati personali impongano che i dati raccolti siano «adeguati» e «pertinenti»[157], il Regolamento e la LED si esprimono in termini parzialmente difformi: mentre il primo prevede che i medesimi siano «limitati a quanto necessario», il secondo attenua tale rigore prevedendo che essi siano «non eccedenti» rispetto alle finalità per le quali sono trattati, lasciando intendere un vincolo meno severo per le forze di polizia[158]. Il d.P.R. n. 15/2018 – attuativo della LED – recupera in parte il rigore del Regolamento, laddove prevede che gli organi di polizia debbano raccogliere – tramite sistemi di ripresa fotografica, video e audio – solamente i dati «strettamente necessari» per le finalità di polizia, registrando quelli «indispensabili»[159].

---

[154] Come sottolineato da F. CASCETTA, M. DE LUCCIA, *Sistemi di identificazione personale*, in *Mondo digitale n. 1*, marzo 2004, 54, si pensi, ad esempio, al caso in cui, sulla scena del crimine, polizia e *intelligence* catturino un'impronta digitale: inserendo quest'ultima sul *database* dei soggetti schedati, il sistema informatico è in grado di escludere dalla lista dei sospettati tutti gli individui presenti nel *database* che presentino un'impronta palesemente difforme da quella oggetto dell'indagine; viceversa, a tutte le impronte giudicate similari viene assegnato un punteggio percentuale *(score)* di similitudine con quella inserita, formando dei sottoinsiemi di similarità. Attraverso tale tecnica di identificazione (c.d. *negative recognition*), è possibile restringere il campo dei potenziali responsabili del reato, da milioni di individui a qualche centinaio ed eventualmente risalire al potenziale criminale.

[155] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Practical guide on the use of personal data in the police sector*, febbraio 2018, in https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

[156] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 173.

[157] Art. 5, par. 1, lett. c) del GDPR e art. 4, par. 1, lett. c) della LED.

[158] GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati,* WP233, 1° dicembre 2015, 7.

[159] Art. 23, c. 2 del d.P.R. n. 15/2018.

La *ratio* perseguita dal legislatore nell'enunciazione di tale principio è la medesima sottesa al principio di limitazione delle finalità: l'interessato deve essere messo nella condizione di mantenere un ampio potere di controllo e di intervento sui propri dati, cosicché possa eventualmente attivare gli ulteriori strumenti previsti a sua tutela dall'ordinamento giuridico.

Il rispetto di tale principio assume grande rilevanza con riguardo ai dati biometrici, e in particolare al riconoscimento facciale, specialmente nella fase di estrazione delle caratteristiche, durante la quale i dati biometrici grezzi sono convertiti in un'immagine vettoriale, ottenendo in tal modo il c.d. *template* o "modello biometrico", che sarà successivamente utilizzato per il confronto con altri *template*[160].

Difatti, da un lato, il titolare del trattamento è tenuto ad estrarre, trasmettere e conservare solamente le informazioni necessarie, evitando che le dimensioni del modello biometrico siano eccessive[161], così da scoraggiare ulteriori trattamenti aventi ad oggetto i medesimi dati personali[162]; dall'altro lato, la quantità di informazioni estratte per la realizzazione del *template* deve essere sufficientemente ampia, con la finalità di evitare il rischio di confusione o sostituzione di identità – come avverrebbe nel caso di modelli poco accurati. Inoltre, è necessario che le dimensioni del *template* siano sufficientemente ampie cosicché la costruzione del modello biometrico mantenga la sua univocità, per evitare che tramite diverse tecniche algoritmiche si possa risalire ai dati biometrici grezzi con cui esso è stato costruito[163].

Da ultimo, Le TRF ripropongono lo stesso problema paventato a proposito del principio di limitazione delle finalità: i *big data* utilizzati dalle TRF – soprattutto qualora impieghino algoritmi di *machine learning* – per la loro stessa natura, richiedono una grande quantità di dati da processare, in modo da poter sfruttare appieno la valenza economica dei dati[164], laddove il principio di minimizzazione vorrebbe limitare l'utilizzo

---

[160] G. MOBILIO, op. cit., 174.
[161] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche,* WP193, 27 aprile 2012, 2.
[162] Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020, 22; GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* WP192, 22 marzo 2012, 9.
[163] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche,* WP193, 27 aprile 2012, 2; Cfr. G. MOBILIO, op. cit., 174.
[164] M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo,* Il Mulino, Bologna, 2019*,* 27-30, i quali qualificano i dati personali come «bene economico» – così come sono stati definiti a suo tempo anche dall'economista Alessandro Acquisti – e fanno riferimento, a tal proposito, alla c.d. «catena del valore del dato».

dei dati personali a quanto necessario per raggiungere la finalità per la quale è stato prestato il consenso[165].

### 2.1.5. *(Segue):* La conservazione delle immagini: il principio di limitazione della conservazione

I principi sopra enucleati interagiscono con un altro principio generale posto a presidio della tutela dei dati biometrici, vale a dire il principio di limitazione della conservazione, il quale impone che i dati siano «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il raggiungimento delle finalità per le quali sono stati trattati»[166].

La *ratio* del principio va ricercata nell'esigenza di assicurare una gestione compartimentata dei dati, funzionale a garantire una tutela effettiva del diritto all'autodeterminazione informativa[167].

Tale principio è espressamente sancito dalla Convenzione n. 108 del 1981, ove si precisa che i dati personali debbano essere «adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati»[168]. Deroghe sono ammesse solamente ove previste dalla legge e se costituiscono una misura necessaria in una società democratica, in relazione a finalità specifiche, tra cui figura quella di assicurare la sicurezza pubblica e la repressione dei reati[169]. La Corte EDU, inoltre, ha espressamente chiarito che è necessario che tali deroghe siano proporzionate, precise e prevedibili, ai sensi dell'art. 8 CEDU[170].

In termini sostanzialmente analoghi si esprimono il Regolamento europeo[171] e la LED[172].

Dal principio in parola discende l'obbligo, posto a carico del titolare del trattamento, di procedere alla cancellazione dei dati, qualora venga meno il nesso tra la finalità che ha giustificato la raccolta dei dati e la conservazione dei medesimi.

---

[165] G. MOBILIO, op. cit., 175.
[166] Art. 5, par. 1, lett. e) del GDPR.
[167] S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 360.
[168] Art. 5, par. 1, lett. c) della Convenzione n. 108 del 1981.
[169] Art. 9 della Convenzione n. 108 del 1981.
[170] Cfr. CORTE EDU, *Rotaru c. Romania,* 4 maggio 2000.
[171] Art. 5, par. 1, lett. e) del GDPR.
[172] Art. 4, par. 1, lett. e) della LED.

Come si è avuto modo di accennare[173], nel caso delle TRF, tale obbligo vale sia per i dati grezzi d'origine, catturati durante la fase di acquisizione dell'immagine, sia per i *template* biometrici. In particolare, i campioni biometrici utilizzati per la realizzazione del modello biometrico possono essere trattati esclusivamente a fini di registrazione e acquisizione dell'immagine e possono essere memorizzati nel *database* solamente per il tempo strettamente necessario alla generazione del *template* stesso. Conclusa la fase di registrazione, il dato biometrico in questione deve essere cancellato sia delle aree di memoria volatile sia dai supporti di memorizzazione[174]. Si tratta di una questione fondamentale, se si pensa che – mentre è piuttosto complesso risalire dal *template* ai dati biometrici grezzi senza conoscere l'algoritmo con cui è stato generato – conoscendo i dati biometrici d'origine è sempre possibile riprodurre il modello biometrico utilizzando diverse tecniche algoritmiche[175].

Nondimeno, il tempo della cancellazione varia anche a seconda dell'esito del riconoscimento: mentre nel caso in cui il sistema non riconosca la corrispondenza tra le caratteristiche biometriche e *template* registrato nel *database,* la cancellazione dei dati deve avvenire immediatamente e automaticamente, viceversa, in caso di corrispondenza, la conservazione deve appunto avvenire per il tempo strettamente necessario per il raggiungimento delle finalità per le quali sono stati trattati[176].

L'osservanza del principio *de quo* è problematica in tutti i casi in cui, nei sistemi di *machine learning* o di apprendimento automatico, gli algoritmi di *matching* facciale siano "allenati" per imparare e ricavare da soli – partendo da enormi *dataset* di immagini ricavate da *Internet* (soprattutto dalle piattaforme *social*) – le caratteristiche dei volti più ricorrenti, spesso senza neanche preoccuparsi di acquisire il consenso dell'interessato o dell'applicazione medesima (c.d. *data scraping*)[177].

Tale tecnica di rastrellamento dei dati è stata messa a punto da *Clearview AI*, che ha venduto grandi quantità di immagini all'FBI, al Dipartimento della Sicurezza

[173] *Infra,* nel Capitolo Primo, §1.2.
[174] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 12 novembre 2014*, in *Gazzetta ufficiale della Repubblica Italiana*, Serie generale – n. 280*,* 25.
[175] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 29 gennaio 2020, 23; G. MOBILIO, op. cit., 177.
[176] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, CONVENTION 108, *Guidelines on Facial Recognition,* T-PD (2020)03rev4, 28 gennaio 2021.
[177] G. MOBILIO, op. cit., 178.

Nazionale, all'esercito e a numerose agenzie di polizia degli Stati Uniti, oltre che a varie società private operanti nei settori dell'intrattenimento, dello sport, del *fitness*, delle cripto-valute e nel settore bancario. Alla luce dello scalpore mediatico che tali pratiche hanno suscitato, *Facebook, Twitter* e *YouTube* hanno chiesto – per ora invano – a *Clearview* di non utilizzare le foto presenti nei loro siti e di cancellare quelle già utilizzate[178]. Il Garante della *privacy* ha sanzionato *Clearview* in Italia per 20 milioni di euro[179].

Analoghi problemi si pongono per la conservazione dei dati biometrici a fini di polizia. Mentre è pacifico che le immagini e i dati biometrici raccolti per una specifica indagine penale possano essere conservati per tutta la durata del procedimento medesimo, maggiori problemi si pongono per il caso in cui tali dati siano raccolti e conservati per una generica finalità di prevenzione in relazione a determinate tipologie di criminali: spesso sono costruite dalle forze dell'ordine enormi *database* di immagini e dati biometrici, usati stabilmente durante le attività investigative a fini di identificazione dei soggetti sospettati di aver commesso un reato. La LED cerca di arginare rischi potenziali per la tutela dei dati personali, prevedendo l'obbligo per gli Stati membri di fissare «termini adeguati» entro i quali procedere alla cancellazione dei dati o, quantomeno, per un «esame periodico» circa la necessità di conservare gli stessi[180].

Quanto al luogo e alle modalità della conservazione dei dati biometrici, va premesso che – se la conservazione del dato biometrico grezzo non è superflua una volta conclusa la fase di registrazione – è probabile che la conservazione del *template* sia richiesta a fini di l'autenticazione/verificazione. In questo caso, occorre stabilire se la conservazione debba avvenire presso il titolare dei dati ovvero presso il titolare del

---

[178] J. CONDEMI, *Clearnview AI: cos'è e come funziona il riconoscimento facciale,* in *AI4BUSINESS*, 2 maggio 2022, https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/. Cfr. G. PEREZ, H. COOK, *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app the helps law enforcement,* in *CBS News,* 20 febbraio 2020.

[179] Si veda, *amplius,* il Capitolo Terzo, §3.2.4 reso a commento dell'intera vicenda.

[180] Art. 5 LED. La disciplina sui termini di conservazione dei dati biometrica a fini di accertamento e repressione dei reati è contenuta nell'art. 10, d.P.R. n. 15/2018. Il principio 7 della Raccomandazione n. R(87) 15 prevede che i dati personali conservati a fini di polizia siano cancellati quando non più necessari per le finalità per le quali erano stati raccolti, tenendo conto di una serie di criteri, quali la necessità di conservare i medesimi dati con riguardo ad un altro procedimento penale; emanazione di una sentenza, specialmente se di assoluzione; riabilitazione; prescrizione; amnistia; età della persona dei cui dati si tratta; categoria particolare di dati.
Per una disamina più approfondita circa la conservazione dei dati telefonici e telematici e le procedure di accesso da parte delle forze dell'ordine si rimanda a M. TORRE, *Privacy e indagini penali,* Giuffrè Francis Lefebvre, Milano, 2020, 51.

trattamento. Nel primo caso, la conservazione potrebbe avvenire sui dispositivi di proprietà dell'interessato, come sui comuni *smartphone* o su carte d'identità. Nel secondo caso, il titolare del trattamento provvede alla conservazione in *database* centralizzati o sugli stessi dispositivi di acquisizione biometrica.

Con specifico riferimento alle TRF, nel caso di verificazione/autenticazione, la prima modalità sembrerebbe maggiormente in linea con i principi in materia di protezione dei dati personali, pur sussistendo il rischio che – in caso di furto o smarrimento del dispositivo da parte dell'interessato – questi sia temporaneamente impossibilitato ad accedere al sistema di riconoscimento facciale. Viceversa, la seconda soluzione, sarebbe l'unica strada percorribile nel caso in cui la comparazione perseguisse la finalità di identificazione, nel qual caso si renderebbe necessaria la costruzione di appropriate banche dati centralizzate in forma cifrata con una chiave segreta che si trovi nell'esclusiva disponibilità del titolare del trattamento, per impedire l'accesso ai non autorizzati[181].

Ad ogni modo, nel caso di conservazione del *template* presso il titolare del trattamento, sarà sua cura adottare tutte le precauzioni necessarie – che dovranno essere implementate con il progredire delle tecnologie – per l'integrità e la riservatezza dei dati biometrici, quali la trasmissione e conservazione dei dati in forma compartimentalizzata, la conservazione dei modelli biometrici e dei dati grezzi in *database* distinti, la cifratura, la predisposizione di misure organizzative e tecniche per il rilevamento delle frodi, la programmazione di un codice di integrità ai dati[182].

Tali principi di integrità e riservatezza – funzionali a garantire il più generale principio di sicurezza del trattamento – permeano l'intero procedimento di riconoscimento facciale, dalla fase di acquisizione dell'immagine sino all'archiviazione del *template* biometrico a fini di identificazione, verificazione/autenticazione ovvero categorizzazione.

---

[181] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* WP 80, 1° agosto 2003, 4 ss. e, in linea di continuità, COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020*,* 23, ove si specifica che il titolare del trattamento debba adottare tutte le opportune misure per garantire la sicurezza dei diti trattati, ad esempio ricorrendo ad un algoritmo di cifratura.

[182] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020*,* 23.

Complementare rispetto al principio di limitazione della conservazione è il diritto all'oblio, previsto sia come conseguenza dell'inesattezza dei dati sia come corollario del principio di limitazione della conservazione[183].

Il *right to be forgotten,* invero, deve essere inteso come il potere dell'interessato di decidere in ordine all'eliminazione dei dati che lo riguardano, risolvendosi – al pari del principio di limitazione della conservazione – in una sorta di diritto all'autodeterminazione informativa. Tale diritto costituisce una declinazione della tutela dell'identità personale, in quanto garantisce il diritto dell'interessato di potere "essere dimenticato"[184].

Nato come diritto di origine pretoria[185], in quanto inizialmente privo di una specifica base normativa, e poi introdotto nel Codice Privacy, oggi il diritto alla cancellazione dei propri dati personali è espressamente disciplinato dal Regolamento all'art. 17, il quale contempla le diverse circostanze che legittimano tale diritto[186].

---

[183] Invero, G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità,* in G. RESTA, V. Z. ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* RomaTre-Press, Roma, 2016, 34, precisa la distinzione tra cancellazione e oblio, consistendo il primo in un'operazione che esclude ogni ulteriore conservazione dei dati personali e rappresentando, piuttosto, il secondo una finalità perseguibile sia per il tramite della cancellazione sia per il tramite del blocco.

[184] R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 199.

[185] Il diritto all'oblio ha cominciato a interessato giudici e giuristi negli ultimi anni, in quanto strettamente connesso all'evoluzione tecnologia. Dopo i tanti e vani tentativi della giurisprudenza di merito di introdurre tale diritto nella cultura giuridica, la Corte di Cassazione, nella sentenza n. 3679 del 1998, lo ha inizialmente declinato quale espressione del più generico diritto alla riservatezza e, successivamente (nella sentenza n. 5525 del 2012), quale particolare forma del diritto dell'identità personale. Tuttavia, solamente all'indomani della celebre sentenza resa dalla Corte di Giustizia nel 2014 nel caso *Google Spain* (causa C-131/12), tale diritto ha cominciato ad animare più diffusamente il dibattito pubblico. In conclusione, oggi il diritto all'oblio è declinazione sia del diritto alla protezione dei dati personali sia del diritto all'identità personale. Per una approfondita ricostruzione del diritto all'oblio si rimanda, senza pretesa di esaustività, a R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 199-214; G. RESTA, V. Z. ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Romatre-press, Roma, 2016; M. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione,* in *Dir. Fam. Pers.,* 2015, 44, 2, 740-758; F. PIZZETTI, *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya",* in *Dir. Inform.,* 2014, 805-829.

[186] In particolare, l'art. 17, c. 1 del GDPR prevede che l'interessato ha diritto di ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali che lo riguardano da parte dei titolare del trattamento: a) qualora i dati non siano più necessari ai fini del trattamento per il quale sono stati raccolti o trattati (ipotesi che qui ci occupa); b) quando l'interessato revochi il consenso al trattamento dei dati, il periodo previsto per la conservazione sia spirato ovvero non vi siano altri motivi legittimi per proseguire il trattamento; c) quando vi sia opposizione da parte dell'interessato; d) quando i dati siano stati trattati illecitamente; e) qualora la cancellazione costituisca adempimento di un obbligo previsto dal diritto dell'Unione o dello Stato membro; f) quando i dati personali sono stati raccolti relativamente all'offerta di servizi di una società dell'informazione ai minori.

Qualora la richiesta sia legittima, nello svolgimento di tale operazione, il titolare del trattamento – e in ciò consiste la maggiore novità introdotta dal Regolamento rispetto alla disciplina previgente – deve tener conto «della tecnologia disponibile e dei costi di attuazione», adottando le «misure ragionevoli, anche tecniche» volte ad informare i terzi che si ritrovano a trattare i dati per altre finalità della richiesta dell'interessato di cancellare «qualsiasi link, copia o riproduzione dei suoi dati personali»[187], evidentemente allo scopo di bloccare la diffusone dei dati nei confronti di tutti i soggetti che stanno trattando i dati oggetto della richiesta di cancellazione. Peraltro, il GDPR bilancia il diritto all'oblio con altri diritti della società civile egualmente rilevanti, primi tra tutti il diritto alla libertà di espressione e di informazione[188].

### 2.1.6. *(Segue):* La vera novità del GDPR: il principio di *accountability*

Il Regolamento europeo ha segnato il passaggio da un approccio rimediale e riparatorio alla tutela dei dati personali ad un approccio anticipatorio e finalizzato a prevenire i possibili pregiudizi cagionati dal trattamento[189]. È stato, infatti, valorizzato il principio di "*accountability".* Tale principio – che rappresenta un'evidente novità rispetto all'impianto normativo precedentemente delineato nella Direttiva 95/46/CE – può essere definito come "il principio dei principi", in quanto la sua osservanza implica il rispetto di tutti principi e istituti ulteriori che sono richiamati nella presente trattazione[190].

Il trattamento dei dati personali, difatti, è stato *ab origine* considerato dall'ordinamento europeo come un'attività rischiosa, in grado, cioè, per la sua intrinseca natura, di cagionare danni maggiori rispetto a quelli derivanti dalla c.d. attività biologica[191], con la conseguente necessità di predisporre norme volte a tutelare gli interessi dei soggetti coinvolti sia sul piano preventivo che sul piano successivo e

[187] Art. 17, c. 2 del GDPR.
[188] Si veda, in particolare, l'art. 17, c. 3 del GDPR.
[189] G. MOBILIO, op. cit., 128; G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 55 ss.; G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence,* in *Panel for the future of Science and Technologies*, STOA, PE 641.5 30, giugno 2020, 12.
[190] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 211.
[191] Per una panoramica generale sull'evoluzione della nozione di "attività rischiosa" nel quadro della c.d. società industriale, si vedano, senza pretesa di esaustività, P. TRIMARCHI, *Rischio e responsabilità oggettiva,* Giuffrè, Milano, 1961, 43 ss.; S. RODOTA', *Il problema della responsabilità civile,* Giuffrè, Milano, 1964, 175 ss.; G. ALPA, *La responsabilità civile. Parte generale,* Utet, Torino, 2010, 293 ss.

riparatorio[192]. Or dunque, con la Direttiva 95/46/CE, il modello comunitario aveva inizialmente approntato una serie di rigidi obblighi nei confronti dei titolari e responsabili del trattamento – basti all'uopo ricordare le norme sugli obblighi e *standard* di sicurezza, recepiti nel Codice *privacy* secondo uno schema bipartito[193] –, al contempo riconoscendo il diritto all'autodeterminazione informativa[194] in favore dell'interessato. Sperimentata l'arretratezza di un modello normativo statico qual era quello che emergeva dalla c.d. Direttiva Madre, il nuovo Regolamento – recependo soluzioni da tempo discusse in ambito accademico e talvolta sperimentate nelle sedi istituzionali e di mercato[195] – ha adottato un mutamento di paradigma[196], apprestando strumenti e metodi di natura preventiva, proprio perché volti, *in modo proattivo,* ad evitare utilizzazioni dei dati suscettibili di recare nocumento ai diritti e alle libertà dell'interessato, e non diretti ad attivarsi a violazione già avvenuta. Proprio tale caratteristica, di intrinseca duttilità e di aderenza alla realtà economico-sociale, ha fatto sì che le regole previste nel GDPR costituissero un archetipo per gli atti ufficiali adottati da altri paesi del mondo, pur restando privi di un simile regime di protezione dei dati personali[197].

---

[192] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 57-58.

[193] Come sottolineato da G. CIACCI, *Il diritto dell'informatica: brevi note in tema di protezione dei dati personali,* in G. CIACCI, G. BUONOMO, *Profili di informatica giuridica,* Cedam, Padova, 2018, il Codice *privacy* aveva operato una prima distinzione tra le c.d. misure "idonee", disciplinate all'art. 31 del D.lgs. 196/2003, le quali, se adottate correttamente, erano tali da esonerare il titolare del trattamento da qualsiasi tipo di responsabilità (civile, penale e amministrativa) e le c.d. misure "minime" di protezione, disciplinate agli artt. 33 ss. e nell'Allegato B del d.lgs. 196/2003, le quali, se adottate correttamente, erano in grado di esonerare il titolare solamente dalla responsabilità penale e amministrativa. Seguendo un altro tipo di classificazione, a seconda delle modalità con cui avveniva il trattamento, se con strumenti elettronici o senza di essi, era possibile distinguere ulteriormente vari accorgimenti tecnici, con la conseguente applicabilità di queste o quelle norme (*id est,* rispettivamente, art. 34 del d.lgs. 196/2003 e artt. 1-26 dell'Allegato B e art. 35 del d.lgs. 196/2003 e artt. 27-29 dell'Allegato B).

[194] Il diritto all'autodeterminazione informativa o *recht auf informationelle selbstbestimmung* è stato coniato dalla giurisprudenza tedesca a seguito della celebre sentenza *Volkszahlungsurteil* (BVferG, 15 dicembre 1983).

[195] R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 79.

[196] In realtà, secondo A. MANTELERO, *La gestione del rischio,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 476 e 492, il cambiamento di paradigma è più apparente che reale, in quanto – sebbene il Codice *privacy* imponesse solamente l'adozione di misure minime – costituiva prassi affermata l'implementazione delle misure di sicurezza nei processi di sviluppo dei beni e servizi. Per alcuni versi, dunque, il Regolamento non fa altro che recepire le migliori prassi già esistenti. Ciononostante, si riconosce senz'altro che il Regolamento abbia spostato il *focus* normativo dalla legittimità del trattamento e autodeterminazione dell'interessato all'*accountability* e gestione del rischio.

[197] R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 104-105. Si pensi, negli Stati Uniti, alla FEDERAL TRADE COMMISSION, *Protecting consumer privacy in an era of rapid change; A proposed framework for business and policymakers. Technical report,* dicembre 2010.

In ossequio al principio di *accountability* – già espressamente richiamato dall'art. 5, par. 2, con riferimento all'osservanza dei principi generali sul trattamento dei dati personali – l'art. 24, par. 1 del Regolamento dispone che «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario».

Come risulta dalla lettera della norma, tale principio si sostanzia in due obblighi: da un lato, comporta l'obbligo per il titolare del trattamento dei dati personali di conformarsi alla normativa relativa alla protezione dei dati tramite l'adozione di procedure e misure tecniche e organizzative, dall'altro lato comporta l'obbligo, in capo al medesimo soggetto, di essere in grado di dimostrare la conformità delle attività di trattamento con le disposizioni dettate dal GDPR[198]. Viene, dunque, affidato ai titolari del trattamento il compito di considerazione la natura, il contesto, le finalità e i rischi ad esso sottesi e di calibrare autonomamente, sulla base di tale valutazione, le modalità, le garanzie e i limiti che devono essere applicati al trattamento dei dati personali[199]. A tal proposito, il Gruppo di Lavoro "Articolo 29" ha precisato che l'espressa previsione di tale principio contribuisca a favorire il passaggio *"from theory to practice"*[200]: l'effetto dovrebbe essere quello di trasformare i principi generali della protezione dei dati in politiche e procedure concrete definite dal titolare del trattamento[201].

La difficoltà di comprendere immediatamente il concetto di *"accountability"* dipende, in parte, dalla sua stessa origine, in quanto deriva dall'esperienza anglosassone[202]. Nella lingua italiana, è difficile rendere una traduzione esatta del termine in parola: *"accountability"* è qualcosa di più della semplice responsabilità, è consapevolezza della responsabilità di cui si è gravati e, al tempo stesso, affidabilità, senza trascurare una buona dose di autorevolezza. Non si tratta più solamente di

[198] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità,* WP 173, 13 luglio 2010.
[199] G. ALPA, *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pacini Editore, Pisa, 2020, 198 ss.
[200] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità,* WP 173, 13 luglio 2010.
[201] G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 20.
[202] *Ivi*, 19.

*compliance* alla normativa, ma il Regolamento richiede al titolare la capacità di aver ragionato e aver adottato in modo consapevole una scelta[203].

L'art. 24 prevede che le misure organizzative e tecniche che i titolari del trattamento adottano debbano essere adeguate, nel senso che devono adattarsi al contesto e alle circostanze in cui avviene il trattamento, attraverso una valutazione *ex ante.* La norma, infatti, non specifica quali siano le specifiche misure da adottare, richiedendo piuttosto una valutazione che deve essere effettuata caso per caso, in modo tale che sia garantita la c.d. scalabilità della protezione dei dati[204], vale a dire una modulazione delle misure al trattamento effettuato, tenendo conto della tipologia e delle finalità del trattamento, nonché della natura dei dati trattati e dei diritti e delle libertà che di volta in volta entrano in gioco.

Il principio di responsabilizzazione, inoltre, si articola su due livelli: il primo prevede un obbligo di base vincolante che comporta l'osservanza di una serie di misure adeguate, tecniche e organizzative, espressamente previste nel Regolamento; il secondo livello, invece, comporta l'adozione di misure volontarie volte a rafforzare il principio di *accountability,* costituendo un ulteriore baluardo a tutela dei dati personali.

Fatte le dovute premesse, pare opportuno passare in rassegna le varie misure, previste all'interno del Regolamento, volte a riempire di contenuto tale principio.

L'art. 32, par. 1 del Regolamento, che deve essere letto in combinato disposto con l'art. 24, prevede un elenco esemplificativo, e non esaustivo, delle misure di sicurezza che possono essere adottate dal titolare e dal responsabile del trattamento al fine di assicurare «un livello sicurezza adeguato al rischio» e, dunque, allo scopo di evitare i rischi connessi alla distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati[205]. In ogni caso, l'intervento

---

[203] R. PANETTA, *Privacy is not dead: it's hiring!,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 26. Come sottolineato in GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità,* WP 173, 13 luglio 2010, il termine "*accountability*" un termine complesso, in grado di compendiare nozioni differenti, quali "*reinforced responsibility*" (responsabilità rafforzata), "*assurance*" (assicurazione), *"reliability"* (affidabilità), *"trustworthiness"* (attendibilità), *"obligation de rendre des comptes"* (obbligo di rendere conto).

[204] Cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy Europeo,* Giuffrè, Milano, 2016.

[205] Art. 32, par. 2 del GDPR. Secondo la più ampia esplicazione contenuta nel considerando n. 75, i rischi connessi alle istanze di adeguatezza delle misure tecniche e organizzative possono derivare da «trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il

tecnico-organizzativo, che deve essere commisurato alla natura del trattamento, ai rischi ad esso sottesi, nonché all'evoluzione tecnologica e ai relativi costi di attuazione, è strutturato in modo uniforme nelle diverse fasi in cui i dati personali restano nella disponibilità del titolare.

Prenderemo in considerazione dapprima le misure organizzative e poi le misure tecniche.

Tra le misure organizzative di sicurezza risiede, innanzitutto, la designazione, e la consequenziale distribuzione di responsabilità, del titolare e del responsabile per la tutela dei dati personali[206] (conosciuto anche come *Data Protection Officer* o *DPO*)[207]. Tra le altre funzioni, il responsabile ha il compito di sorvegliare sull'applicazione del Regolamento da parte del titolare[208]. La nomina del responsabile per la protezione dei dati è obbligatoria nel caso di trattamento su larga scala di categorie particolari di dati, e dunque anche dei dati biometrici estratti dalle TRF[209].

---

trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati».

[206] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 214.

[207] Art. 28 del Regolamento UE 2016/679.

[208] R. PANETTA, *Privacy is not dead: it's hiring!*, in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, Giuffrè Francis Lefebvre, Milano, 2019, 38-39. È bene sottolineare come egli non sia in alcun modo responsabile nei confronti degli interessati in caso di mancata attuazione degli obblighi previsti dalla normativa in esame: tale responsabilità resta in capo al titolare del trattamento, non essendo per nessuna ragione delegabile. Qualora il responsabile contravvenga alle disposizioni del titolare, sarà quest'ultimo a dover dimostrare che l'evento dannoso non gli sia in alcun modo imputabile per evitare di incorrere nelle sanzioni prescritte dal Regolamento. Per un approfondimento sul singolarissimo riparto di responsabilità tra il titolare e il responsabile si veda anche L. FEROLA, *La "nuova figura" del responsabile della protezione dei dati personali e le sue caratteristiche*, in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, Giuffrè Francis Lefebvre, Milano, 2019, 360-365. Invece, sui requisiti soggettivi del DPO si veda F. PIZZETTI, *Modalità e requisiti necessari per la nomina a DPO in Intelligenza artificiale;* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei Dati Personali e regolazione*, G. Giappichelli Editore, Torino, 2018, 96 ss.

[209] Art. 37, par. 1, lett. c) del GDPR.

È prevista, altresì, la nomina di figure intermedie quali il c.d. contitolare del trattamento o del rappresentate del titolare o del responsabile del trattamento non stabilito nell'Unione[210].

Tra le misure organizzative figura anche l'adesione a codici di condotta[211] e l'ottenimento di certificazioni[212], che possono costituire strumenti utili al titolare per dimostrare la conformità delle regole aziendali al principio di *accountability*[213]. L'emissione di tali certificati "di qualità" avviene su base volontaria e presuppone l'attivazione di sistemi di *labelling* da parte delle imprese[214].

Costituiscono, altresì, misure organizzative l'adozione di *policy* interne, nonché la predisposizione di linee-guida e circolari.

Per ciò che concerne, invece, le misure tecniche di sicurezza, l'art. 32 del GDPR individua un modello di condotta basato sulla "spersonalizzazione" dei dati[215], attuato mediante le procedure di pseudonimizzazione e di cifratura dei dati personali, mentre l'art. 25 del Regolamento menziona la *privacy by default* e la *privacy by design.*

Invero, l'evoluzione tecnologica cui stiamo assistendo negli ultimi decenni, che porta con sé l'introduzione di macchine in grado di agire in modo autonomo rispetto alla volontà dell'uomo (c.d. *machine learning*), la massiccia diffusione dei *big personal data,* l'utilizzo di Internet come «tessuto connettivo» della società[216], ha reso evidente la non

---

[210] Rispettivamente art. 26 e art. 27 del GDPR. Il Regolamento pone specifici obblighi in capo a tali figure, nonché il relativo regime di imputabilità, per il cui approfondimento si veda G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 71 ss.; L. FEROLA, *La "nuova figura" del responsabile della protezione dei dati personali e le sue caratteristiche,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 348 ss.

[211] Art. 40 del GDPR, il quale contiene una sofisticata disciplina di tali strumenti, in cui sono evidenti elementi di continuità e di discontinuità rispetto al precedente impianto normativo. Per un approfondimento sui codici di condotta si veda D. POLETTI, M. C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione,* in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* Giuffrè Francis Lefebvre, Milano, 2019, 369 ss.

[212] Art. 25, par. 3 e art. 42 del GDPR

[213] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 215.

[214] R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 82.

[215] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 67.

[216] Questi sono i tre "macro-filoni" dell'innovazione tecnologica, secondo il pensiero di G. GIANNONE CODIGLIONE, *Internet of things e nuovo regolamento privacy*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 131.

più trascurabile interconnessione tra tecnologia e diritto, cioè quell'*inestricabile nodo gordiano* tra scienza e regola giuridica, che, nella società del rischio[217] e dell'incertezza[218], sono chiamate a concorrere al fine di conferire effettività al diritto alla protezione dei dati personali. Il Regolamento europeo – prendendo posizione in ordine al lungo dibattito sulle c.d. *privacy enhancing tecnhologies* – si fa portatore di questa istanza, affidando anche alla componente tecnologica la tutela dei dati personali nella fase prodromica al trattamento[219]. L'impostazione pragmatica che informa tali regole operative si risolve nella partizione binaria tra *privacy by design* e *privacy by default,* entrambe destinate ad operare *ex ante* per selezionare le sole informazioni rilevanti dell'interessato, in linea con la logica di tutela preventiva dei dati personali[220].

Un primo gruppo di misure[221] riguarda il momento preparatorio e progettuale delle attività di trattamento dei dati: secondo il principio della *privacy by design* (anche "PbD"), ogni sistema informatico e di comunicazione finalizzato al trattamento dei dati deve essere, sin dalla sua progettazione e distribuzione, preordinato ad operare nel rispetto dei diritti fondamentali degli utilizzatori e dei soggetti i cui dati sono trattati[222]. Il concetto di *privacy by design,* dunque, impone al titolare di verificare che, sin dalla progettazione, i sistemi di cui dispone siano conformi al dettato normativo, con la conseguenza che si finisce per coinvolgere anche i produttori e sviluppatori dell'Intelligenza Artificiale, i quali dovranno progettare i *software* in modo tale da consentire ai titolari del trattamento di adempiere agli obblighi imposti dal Regolamento[223].

---

[217] U. BECK, *La società del rischio. Verso una seconda modernità,* Carocci Editore, Roma, 2000.
[218] Z. BAUMAN, *La società dell'incertezza,* Il Mulino, Bologna, 1999.
[219] In realtà, la *privacy by design* ha suscitato reazioni contrastanti: da un lato, l'entusiasmo di chi la crede una vera e propria rivoluzione in campo normativo, dall'altro, il sospetto di chi la vede semplicemente come una costruzione teorica di un principio poco rigoroso, ancillare rispetto ad altri rocciosi principi contenuti nel Regolamento. Peraltro, non si tratta neppure di una novità assoluta, in quanto già la Direttiva 95/46/CE, all'art. 17, richiedeva che le misure tecniche e organizzative dovessero essere implementate considerando lo stato dell'arte, i costi e soprattutto i livelli di rischio connessi alla natura del trattamento considerato. Per un approfondimento circa la genesi del principio si veda F. SARTORE, *Privacy-by-design*, *l'introduzione del principio nel corpus del GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 295 ss.
[220] R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 80-109.
[221] A tali misure si riferisce il par. 1 dell'art. 25.
[222] F. SARTORE, *Privacy-by-design, l'introduzione del principio nel corpus del GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 295.
[223] G. ALPA, *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pacini Editore, Pisa, 2020, 200 ss.

In realtà, nonostante il pregevole intento, non si mancato di sottolineare, da un lato, l'approccio "ad ampio spettro" e quasi "olistico" adottato dal legislatore, che richiede l'implementazione di misure tecniche e organizzative esemplificate, in modo troppo semplicistico, con la pseudonimizzazione; dall'altro lato, la natura amorfa del principio, che ora viene declinato come una delle modalità con cui il titolare del trattamento dovrebbe dimostrare la *compliance* alle disposizioni dettate dal Regolamento[224], ora come un crocevia tra vari principi, ambiguità di fondo che tradisce l'assenza di chiara direzione verso cui orientare tale principio. In sostanza, il principio in questione non ha ancora trovato dei contorni ben definiti né una dimensione applicativa certa e, in termini più pratici, potrebbe risultare particolarmente difficile per i titolari del trattamento (unici diretti obbligati) capire come rispettare e accrescere le misure di PbD[225]. A tal proposito, si potrebbe far riferimento alle sette strategie elaborate da Hopman, che fungono da ponte tra le iperuraniche aspirazioni del principio e la prassi[226].

Non va, peraltro, trascurata la circostanza che l'inserimento di tale principio *in fieri* nel *corpus* del Regolamento appare un tentativo di rimettere l'Uomo al centro della società, restituendogli il controllo totale sulle macchine[227].

Come si è avuto modo di accennare, la pseudonimizzazione costituisce una delle misure di sicurezza più importanti tra le soluzioni di PbD. Il Regolamento propone una definizione di pseudonimizzazione, qualificata come «il trattamento dei dati personali in modo tale che i dati [essi] non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive», purché «tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzate intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o

[224] In particolare, il Considerando n. 78 prevede che il titolare del trattamento, per dimostrare la conformità del trattamento con il Regolamento, dovrebbe adottare politiche interne e attuare misure volte a soddisfare i principi della protezione dei dati sin dalla progettazione (*by design*) e di *default.*

[225] F. SARTORE, *Privacy-by-design, l'introduzione del principio nel corpus del GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 300 ss.

[226] Si veda, in particolare, EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), *Privacy anda Data protection by design – from policy to engineering,* 2014. Le sette strategie – minimizzazione, occultamento, separazione, aggregazione, informazione, controllo, *enforcement* e *accountability* – sono volte a garantire la c.d. *unlinkability* dei dati, che consiste nel garantire che i dati non possano essere collegati tra diversi ambienti, cui in teoria potrebbero essere ricollegati, facendo in modo che i *set* di dati siano mantenuti separati tra di loro.

[227] R. PANETTA, *Privacy is not dead: it's hiring!,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 29-30.

identificabile»[228]. Dunque, per mezzo delle tecniche di pseudonimizzazione, il titolare del trattamento può conservare i dati personali di un individuo[229], senza che questi siano riconducibili all'interessato, il quale potrà essere identificato solo indirettamente, cioè tramite l'utilizzo di apposite chiavi di reidentificazione, possedute in genere solo dal titolare o dal responsabile o da un loro delegato[230]. Da notare che l'intento perseguito dal legislatore è quello di predisporre incentivi adeguati perché i titolari del trattamento adottino tecniche di de-identificazione dei dati idonee a ridurre i rischi per i diritti e le libertà delle persone fisiche e, in ultima analisi, a garantire la sicurezza dei dati. L'adozione di tali tecniche, naturalmente, non costituisce automaticamente una prova del rispetto delle prescrizioni del Regolamento e, pertanto, non esonera il titolare del trattamento da eventuali responsabilità [231].

Il secondo gruppo di misure[232] riguarda le misure organizzative e tecniche adottate dal titolare per assicurare che, per impostazioni predefinite (*privacy by default*), il trattamento si limiti ai soli dati personali necessari per ogni specifica finalità di trattamento. Tale obbligo riguarda tutti gli aspetti e tutte le fasi del trattamento, dalla «quantità dei dati raccolti» alla «portata del trattamento» fino alla conservazione del trattamento, in modo tale che la configurazione predefinita dei *software* sia in grado di scongiurare il rischio una diffusione involontaria dei dati. Tale principio, dunque, costituisce la *summa* dei principi di minimizzazione dei dati e di limitazione delle finalità, in quanto implica che siano raccolti solo i dati personali necessari e che le finalità del trattamento siano quanto più limitate[233].

Con specifico riferimento ai dati biometrici estratti dalle tecniche di riconoscimento facciale, le misure tecniche e organizzative di sicurezza sono finalizzate soprattutto a prevenire i rischi di violazione e furto dei dati biometrici[234], i quali peraltro

---

[228] Art. 4, n. 5 del GDPR.
[229] I dati pseudonimizzati restano comunque "dati personali", dal momento che i soggetti interessati restano pur sempre identificabili.
[230] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 216.
[231] C. FOGLIA, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019, 320-322.
[232] A dette misure si riferisce il par. 2 dell'art. 25.
[233] E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali,* in EMILIO TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 86.
[234] Questo è quello che è accaduto con riferimento ai dati estratti dal riconoscimento facciale di più di un milione di persone, raccolti dalla UK Metropolitan police*,* da istituti di credito e aziende appaltatrici della

sono particolarmente vulnerabili perché non possono essere sostituiti dall'interessato. Altro pericolo che si vuole scongiurare mediante la predisposizione di adeguate misure di sicurezza è costituito dal furto di identità digitale[235], vale a dire i tentativi di sostituirsi ad un soggetto inducendo in errore un sistema di verificazione. Al fine di prevenire tali comportamenti fraudolenti, per evitare che il sistema possa essere ingannato dal ricorso a forme di alterazione o distorsione delle immagini digitali, possono essere apprestate varie contromisure e tecniche di protezione volte a verificare che l'immagine digitale acquisita provenga dall'uomo, quali l'analisi del movimento – mediante i quali i sistemi di riconoscimento facciale intercettano quei movimenti visibili o impercettibili nei volti reali – ovvero l'analisi della *texture* – mediante i quali l'uomo allena il sistema a distinguere la struttura della pelle naturale – ovvero il rilevamento dei segni di vita, come il battito di ciglia[236]. In aggiunta, sono stati implementati metodi multimodali di riconoscimento, basati su un algoritmo di *deep learning* per riconoscere gli esseri umani utilizzando l'iride, il volto e vene delle dita[237].

Come espressamente affermato dal Comitato europeo per la protezione dei dati[238], fra le soluzioni tecniche sviluppate con riferimento ai dati biometrici trattati dai sistemi di videosorveglianza, vanno annoverate misure quali trasmettere e conservare i dati in forma compartimentalizzata, conservare i dati grezzi e i modelli biometrici in *database* distinti, cifrare i dati biometrici (soprattutto i *template* biometrici), prevedere una politica per la cifratura e per la gestione delle chiavi di cifratura, associare un codice di integrità ai dati (come una firma o un codice *hash*) e vietare gli accessi ai dati biometrici a persone non autorizzate.

---

difesa, i quali sono stati pubblicati su *Internet* nell'agosto del 2019, come segnalato da G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 182 e J. TAYLOR, *Major breach found in biometrics system used by bank, UK police and defence firms,* in *The Guardian,* 14 agosto 2019. Allo stesso modo, nel 2021, si è verificata la violazione di centinaia e centinaia di milioni di profili Facebook, che indicavano nome, numero di telefono, attività professionale, relazione sentimentale, i quali sono stati messi in vendita su Internet, come segnalato da A. DI CORINTO, *Ecco i database rubati a Facebook. Che cosa possono farne gli hacker,* in *Repubblica,* 15 febbraio 2021.

[235] I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and tge Confidentality of Personal Identifiable Images,* Springer, Cham, 2020, 16 ss.

[236] A. ANJOS, S. MARCEL, *Counter-measures to photo attacks in face recognition: a public database and a baseline, International Joint Conference on Biometrics,* 2011, 1 ss.

[237] N. ALAY, H. H. AL-BAITY, *Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits,* 2020.

[238] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020, 23.

Parimenti, il Garante *privacy* italiano[239] ha chiarito che i campioni o *template* biometrici vadano conservati, laddove necessario per effettuare i confronti, in aree di *filesystem* protette con chiavi crittografiche che li rendano indecifrabili per i non autorizzati o in banche dati che permettano di utilizzare tecniche avanzate di cifratura.

Venendo al secondo obbligo di cui si compone il principio di *accountability,* va segnata l'introduzione, ad opera del Regolamento europeo, del c.d. registro dei trattamenti, che dovrebbe costituire lo strumento base di ogni titolare del trattamento, allo scopo di poter dimostrare di essere *accountable,* in quanto consente al titolare e al responsabile di effettuare la valutazione del rischio[240]. È chiara, dunque, la sua duplice natura di misura organizzativa e di documento probatorio, anche in considerazione del fatto che *accountability* equivale anche a «prova di aver adempiuto correttamente»[241]. Da notare che la tenuta del registro dei trattamenti è facoltativa in alcune ipotesi[242], ma è sempre obbligatoria qualora siano trattati dati biometrici (e le altre «categorie particolari di dati»)[243].

In qualche modo rilevante è, inoltre, l'art. 33 del Regolamento, il quale ha introdotto l'obbligo, posto a carico del titolare del trattamento, di notificare la violazione dei dati personali all'Autorità di controllo (c.d. *data breach*), indicando contestualmente la natura e tipologia di violazione, le possibili conseguenze e le misure adottate o di cui si propone l'adozione per rimediare alla violazione o attenuare i possibili effetti negativi[244]. La notifica deve avvenire senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne sia venuto a conoscenza, ma solamente nel caso in cui ritenga probabile che tale violazione sia tale da produrre nocumento ai diritti e libertà degli interessati[245]. Parimenti, qualora la violazione sia suscettibile di presentare

---

[239] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimento biometrico e firma grafometrica,* 12 novembre 2014, 26.
[240] Art. 30 del GDPR. Cfr. G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022, 26.
[241] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 218.
[242] La tenuta del registro non è obbligatoria nel caso di impresa o organizzazioni con meno di 250 dipendenti.
[243] Art. 30, par. 5 del Regolamento.
[244] Art. 33, par. 3, lett. a), c), d) del GDPR. L'art. 33, par. 4 specifica che, nel caso in cui non sia possibile fornire contestualmente tali informazioni, queste possono essere fornite nelle fasi successive, senza ingiustificato ritardo. Inoltre, ai sensi dell'art. 33, par. 5, il titolare del trattamento ha l'onere di documentare qualsiasi violazione dei dati personali, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è fondamentale per consentire all'Autorità Garante per la protezione dei dati personali che siano state rispettate tali norme.
[245] Art. 33, par. 1 del GDPR.

un rischio elevato per i diritti e le liberà delle persone fisiche, il titolare deve comunicare la violazione anche all'interessato, senza indebito ritardo[246], formulando eventualmente raccomandazioni alla persona fisica interessata intese ad attenuare i potenziali effetti negativi[247]. In tali ipotesi, dunque, il titolare del trattamento è chiamato a giudicare il diverso grado di rischio (elevato o basso-improbabile) a posteriori, poiché appunto dipendente dalle potenziali o attuali conseguenze che la violazione ha prodotto[248].

Tra gli strumenti che garantiscono l'*accountability* del titolare del trattamento, particolarmente rilevante è la nuova disciplina sulla valutazione d'impatto sulla protezione dei dati (c.d. *Data Protection Impact Assessment* o DPIA) e la consultazione preventiva, che si sostituisce all'obbligo, precedentemente previsto, di notificare alle autorità di controllo il trattamento dei dati personali[249] ed egualmente ispirata al principio di trattamento dei dati personali in maniera non rischiosa[250].

In particolare, la valutazione d'impatto, che implica una stima a monte dei rischi sottesi ai trattamenti di dati personali e il continuo aggiornamento dei parametri, costituisce una delle principali soluzioni con cui il titolare può rispettare il principio della *privacy by design* e della *privacy by default*.

A norma dell'art. 35 del Regolamento, qualora un trattamento, nel contesto di attività di sfruttamento delle nuove tecnologie – considerati la natura, l'oggetto e le finalità del trattamento – presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare è tenuto ad effettuare una valutazione circa l'impatto sortito da tali trattamenti sulla protezione dei dati personali. Inoltre, la valutazione d'impatto costituisce un passaggio obbligatorio per quelle forme particolarmente rischiose di trattamento, tra le quali figurano il trattamento di «categorie particolari di dati» di cui all'art. 9 del GDPR

[246] Art. 34, par. 1 del GDPR. La medesima norma, al par. 3, specifica che non è necessaria la comunicazione all'interessato qualora sia soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha adottato, anche con riferimento ai dati personali oggetto della violazione, tutte le misure tecniche e organizzative adeguate, soprattutto quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare ha successivamente adottato tutte le misure tecniche e organizzative adeguate per evitare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; c) detta comunicazione sarebbe proporzionata, caso nel quale il titolare procede a una comunicazione pubblica o simili.

[247] Considerando n. 86, che precisa che tali comunicazioni agli interessati dovrebbero essere effettuate «non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo».

[248] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 75-76.

[249] Tale obbligo era originariamente previsto all'art. 18 della Direttiva 95/46/CE.

[250] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 68.

– di cui fanno parte i dati biometrici estratti dalle tecniche di riconoscimento facciale –, nonché la sorveglianza sistematica su larga scala di una zona aperta al pubblico[251].

Qualora, all'esito della valutazione d'impatto, il titolare ritenga che il trattamento presenti un rischio elevato in mancanza di misure in grado di attenuare il rischio, egli ha la facoltà di consultare preventivamente l'autorità di controllo, per chiedere indicazioni su come gestire il rischio (c.d. consultazione preventiva o *prior consultation)*[252]. In ogni caso, l'Autorità Garante non ha il potere di *autorizzare* il trattamento, ma semplicemente – qualora ritenga che il titolare del trattamento non abbia adeguatamente e sufficientemente individuato e minimizzato i rischi ad esso connessi – ha l'onere di fornire un parere scritto al titolare o al responsabile del trattamento, indicando le misure di sicurezza da implementare, esercitando altresì i poteri investigativi, autorizzativi e consultivi di cui dispone[253]. Si tratta, dunque, di un intervento *ex post,* successivo alle misure già intraprese dal titolare, avendo il Regolamento europeo abolito la verifica preliminare (c.d. *prior checking*) originariamente prevista dal Codice *privacy*[254].

La lettura sistematica delle disposizioni in commento porta a ritenere che la disciplina sulla protezione dei dati personali incentiva i prestatori di beni e servizi ad adottare procedure tecniche e organizzative informate alla minimizzazione, se non eliminazione, del rischio, dovendosi essi adeguare allo *standard* di diligenza atteso: i maggiori costi sostenuti per conformarsi al dettato normativo sono più che compensati

[251] Art. 35, par. 3, lett. b) e c) del Regolamento. L'art. 35 del GDPR, inoltre, pone in capo all'Autorità di controllo l'obbligo di redigere periodicamente un elenco aggiornato di quelle tipologie di trattamento che necessariamente devono essere sottoposte alla valutazione preventiva o, alternativamente, di indicare quali trattamenti non sono sottoposti a tale obbligo (par. da 4 a 6).
[252] Art. 36 del GDPR.
[253] Art. 36, par. 2 del GDPR, il quale scandisce anche i termini, e le relative proroghe, entro i quali deve avvenire il "dialogo" tra l'Autorità Garante per la protezione dei dati personali e il titolare del trattamento. Nella consultazione preventiva, ai sensi dell'art. 36, par. 3, il titolare deve comunicare all'Autorità di controllo, tra le altre, le eventuali responsabilità dei titolari, dei contitolari e dei responsabili del trattamento, le finalità del trattamento, le misure adottate per proteggere i diritti e le libertà degli interessati, nonché l'esito della valutazione d'impatto.
[254] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 218. In senso maggiormente critico sulla valutazione preventiva, si veda A. MANTELERO, *La gestione del rischio,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 513, ove si sottolinea che – essendo la valutazione d'impatto un filtro preventivo basato però sull'autovalutazione del titolare del trattamento – si potrebbe sottostimare il livello di rischio, nel qual caso l'autorità di controllo non verrebbe a conoscenza del trattamento se non a violazione già avvenuta.

dalla minimizzazione dei costi sociali conseguenti alle violazioni dei dati personali e dei costi esterni in termini di responsabilità[255].

In conclusione, il principio di *accountability* enucleato nel Regolamento europeo esige una valutazione dei *compliance plans* aziendali rispetto ai rischi di perdita e distruzione dei di dati o accessi non autorizzati, sia sul piano tecnologico – attraverso l'adozione di misure tecniche di sicurezza, quali pseudonimizzazione e cifratura – sia sul piano organizzativo – attraverso la predisposizione di figure intermedie che vigilino sulla corretta applicazione del Regolamento e delle misure tecniche stesse – imponendo anche una revisione della propria organizzazione interna[256].

Sulla scorta di queste osservazioni, risulta chiaro che il Regolamento europeo accoglie un approccio dinamico al rischio, incentrato sul caso concreto e sull'evoluzione degli elementi di rischio, cui far fronte tramite una costante e periodica revisione delle soluzioni adottate[257]: a differenza della normativa precedente, che indicava per ogni tipologia di trattamento le specifiche misure di sicurezza da adottare, il GDPR rimette al titolare la scelta delle misure organizzative e tecniche che ritiene più adeguate a prevenire il rischio di impatti negativi sulle libertà e sui diritti degli interessati. L'individuazione delle misure tecniche e di organizzazione interna è intimamente legata alla natura e tipologia di trattamento e, conseguentemente, ai rischi che si vogliono scongiurare: si tratta, dunque, di una valutazione che deve essere effettuata caso per caso, preliminare al trattamento stesso. Peraltro, tali disposizioni non tassative e che, in qualche misura, si affidano alla valutazione, all'esperienza e al buon senso del titolare del trattamento non devono essere qualificate come un vuoto normativo, fonte di incertezza applicativa, quanto piuttosto come una sfida consapevole lanciata dal legislatore europeo: prevedere, come nella precedente *impasse* normativa, regole rigide e dettagliate in una società sempre più *smart* avrebbe significato produrre un testo normativo obsoleto prima ancora di essere applicato[258].

---

[255] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, 76-77.

[256] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 218.

[257] A. MANTELERO, *La gestione del rischio,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 476.

[258] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 217-221.

Sotto questo profilo, non è più il legislatore europeo a dover stare al passo con le evoluzioni tecnologiche, ma sono i titolari del trattamento a dover aggiornare caso per caso, periodicamente, le misure tecniche e organizzative da adottare per salvaguardare i dati personali degli interessati[259]. È questo il motivo principale per cui il principio di *accountability* rappresenta il cuore del Regolamento, "la chiave di volta su cui poggia l'intero sistema"[260].

### 2.1.7. *(Segue):* Ulteriori principi applicabili alle TRF

In definitiva, è corretto affermare che i principi applicabili alle tecniche di riconoscimento facciale sono quelli enucleati all'art. 5 del Regolamento.

Tali principi – che costituiscono l'architrave della disciplina in tema di protezione dei dati personali – rivelano una duplice natura: da un lato, stabiliscono la regola applicabile al caso concreto, dall'altro rappresentano dei principi-guida per l'interpretazione e applicazione di tutte le norme contenute nel Regolamento. In ossequio al carattere di neutralità tecnologica accolta dalla normativa[261], essi sono soggetti ad un'interpretazione evolutiva, che tenga conto del contesto storico e delle evoluzioni tecnologiche[262].

Nel corso della presente trattazione abbiamo già dato conto del principio di liceità, del principio di limitazione delle finalità, nonché dei principi di minimizzazione e di limitazione della conservazione dei dati.

A completare il quadro dei principi generali, pare opportuno richiamare gli ulteriori principi applicabili alle TRF.

Come si è detto, ogni trattamento di dati personali deve essere informato a criteri di liceità, correttezza e trasparenza[263]. In generale, un trattamento è lecito solamente se si fonda sul consenso dell'interessato ovvero su un'altra base giuridica legittima[264]. Ove

---

[259] G. ALPA, *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pacini Editore, Pisa, 2020, 200.
[260] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018), 217-221.
[261] Considerando n. 15 del Regolamento.
[262] G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022, 16.
[263] Art. 5, par. 1 del GDPR.
[264] Costituiscono basi giuridiche idonee a giustificare il trattamento dei dati personali le «condizioni» contemplate all'art. 6, par. 1 del GDPR.

venga meno la base giuridica che aveva fondato il trattamento, il trattamento deve cessare, a meno che non sia possibile per il titolare continuare il trattamento dei dati personali individuando altra base giuridica.

Peraltro, come chiarito dal Garante per la protezione dei dati personali, è possibile affermare la liceità del trattamento solamente qualora siano, al contempo, rispettati i principi di necessità, proporzionalità, finalità e correttezza, nonché di qualità dei quali[265].

Abbiamo poi messo in luce come il trattamento di «categorie particolari di dati personali» – di cui fanno parte i dati biometrici utilizzati dalle TRF – è, in linea generale, vietato[266], salvi i casi espressamente menzionati all'art. 9, par. 2 del Regolamento.

La liceità va letta congiuntamente alla correttezza e trasparenza del trattamento.

La correttezza attiene essenzialmente alle concrete modalità con cui si svolge il rapporto tra titolare e interessato: i dati personali non devono essere trattati in modo pregiudizievole, illegittimamente discriminatorio o fuorviante per l'interessato[267]. Corollari di tale principio sono alcuni diritti riconosciuti dal Regolamento agli interessati, quali il diritto all'informazione, il diritto di intervenire sul trattamento (accesso, cancellazione, rettifica, portabilità dei dati) e il diritto di non essere soggetti a processi decisionali individuali automatizzati.

La trasparenza attiene, piuttosto, all'accessibilità e comprensibilità delle informazioni e comunicazioni relative al trattamento che sono fornite all'interessato[268]. Nondimeno, la trasparenza costituisce un *obbligo trasversale* a tutta la disciplina in materia di protezione dei dati personali, in quanto comporta non solo che il titolare fornisca agli interessati le informazioni cui hanno diritto, ma attiene anche al modo in cui il titolare *comunica* tali informazioni (deve essere, a tal fine, utilizzato un linguaggio semplice e chiaro) e al modo con cui il titolare *agevola l'esercizio dei diritti* degli interessati[269].

---

[265] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante – Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro,* 21 luglio 2005.
[266] Art. 9, par. 1 del GDPR.
[267] G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022, 17.
[268] Art. 12 e Considerando n. 39 del Regolamento.
[269] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del Regolamento (UE) 2016/679,* 29 novembre 2017, 3.

Il principio di trasparenza va osservato lungo tutto il processo di trattamento dei dati, dalla fase di raccolta fino alla fase di cancellazione dei dati. Tutte le attività svolte dal titolare devono essere svolte in virtù di tale principio, il quale si riflette anche sul rapporto con il Garante *privacy* e con le altre autorità di controllo[270].

Il trattamento dei dati conformemente al principio di trasparenza è strettamente connesso al principio di *accountability:* quanto più il titolare svolge le proprie attività in modo trasparente, quanto più sarà in grado di dimostrare la conformità del trattamento alle prescrizioni del Regolamento[271].

A differenza del Regolamento, tuttavia, la LED non enuclea un generico principio di trasparenza, in ragione delle finalità che persegue, ma piuttosto distingue tra informazioni da «mettere a disposizione» del pubblico in modo generalizzato e le informazioni da trasmettere ad un determinato soggetto «in casi specifici»[272], con la conseguenza che – ove le forze dell'ordine volessero installare un sistema di riconoscimento facciale in uno spazio pubblico – dovrebbero distinguere tra informazioni da tramettere alla generalità dei consociati e informazioni da fornire alle persone soggette al rilevamento[273].

Ebbene, il principio di trasparenza appare ancora più decisivo con riferimento alle tecniche di riconoscimento facciale, la cui natura e le cui funzionalità non sempre risultano comprensibili all'uomo[274].

In tale contesto, risulta speculare al principio di trasparenza il diritto alla c.d. *explainability* o comprensibilità del sistema di riconoscimento facciale, vale a dire il diritto di venire a conoscenza non solo dell'architettura e delle caratteristiche del processo

---

[270] G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022, 20.
[271] G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022, 19. Anche il Comitato europeo per la protezione dei dati personali, nelle *Linee guida 4/2019 sull'articolo 25 GDPR – Protezione dei dati fin dalla progettazione e per impostazione predefinita*, versione 2.0., 20 ottobre 2020 ha individuato degli elementi centrali volti all'attuazione del principio di trasparenza, quali la chiarezza, la semantica, l'accessibilità, la rilevanza, il *design* universale, la comprensione, la multicanalità, la stratificazione.
[272] Rispettivamente art. 13, par. 1 e art. 13, par 2 della LED.
[273] G. MOBILIO, op. cit., 186, il quale osserva, peraltro, come vi siano delle sostanziali differenze tra il GDPR e la LED, sia con riferimento alla quantità di informazioni da fornire agli interessati, come precisate dal d.lgs. n. 51/2018 attuativo della LED, sia con riguardo ai contenuti e ai limiti di tali informazioni.
[274] Come specificato in GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* 3 ottobre 2017, WP 251.rev.01, 10, esistono diversi livelli di comprensione, per cui per alcune persone potrebbe risultare particolarmente complesso comprendere le tecniche utilizzate nella profilazione e nei processi decisionali automatizzati.

decisionale utilizzato, ma anche dei criteri utilizzati e dei motivi posti alla base delle singole decisioni assunte dal sistema di intelligenza artificiale[275].

Peraltro, tale diritto – reso necessario dalla discrepanza tra la logica sottesa al pensiero umano e il linguaggio degli algoritmi – non è contenuto né nel Regolamento né tantomeno nella LED, risultando appena accennato solo al Considerando n. 71 del GDPR, che però non ha valenza precettiva, ma solo interpretativa. Non è possibile, dunque, parlare di un vero e proprio diritto ad ottenere una spiegazione *ex post* sulla decisione assunta dall'algoritmo, essendo riconosciuto semplicemente un generico diritto di informazione *ex ante* sull'esistenza del processo decisionale automatizzato e sulle sue caratteristiche[276].

Ciononostante, in dottrina sono state avanzate tesi di segno contrario, secondo le quali – seguendo un'interpretazione sistematica – il Regolamento garantirebbe il diritto alla comprensibilità e trasparenza sia dell'architettura che dei criteri adoperati durante il processo decisionale automatizzato seguito dall'algoritmo[277].

A riprova di tale orientamento, è possibile rintracciare nell'ordinamento euro-unitario atti volti ad enfatizzare tale principio, come la risoluzione del Parlamento europeo del 2017[278], secondo la quale dovrebbe essere sempre possibile «indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale che possa avere un impatto rilevante sulla vita di una o più persone». Similmente, il Gruppo di Lavoro "Articolo 29" ha chiarito che il titolare del trattamento dovrebbe essere in grado di indicare all'interessato, tramite un linguaggio semplice e chiaro, i criteri su cui si basa la decisione automatizzata, e dunque la logica seguita, senza dover necessariamente fornire complesse spiegazioni sugli algoritmi impiegati[279].

---

[275] G. MOBILIO, op. cit., 209, il quale ritiene opportuno utilizzare il termine «comprensibilità» in luogo di altri termini utilizzati in documenti ufficiali, quali «spiegabilità» o «spiegabilità», in quanto quest'ultimi sono poco utilizzati nella lingua italiana.

[276] G. MOBILIO, op. cit., 213. Per un approfondimento si veda, in particolare, S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explaination of Automated Decision-Making Does Not Exists in the General Data Protection Regulation,* in *International Data Privacy Law,* 7, 2, 2016, 76 ss.

[277] G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists* in *in the General Data Protection Regulation,* in *International Data Privacy Law,*7, 4, 2017, 245 ss., che parla di «*legibility* di *data* e *analytic algorithms».*

[278] PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica,* 2015/2103 (INL), 2018/C 252/25, 16 febbraio 2017.

[279] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679* del 3 ottobre 2017, WP 251 rev.01, 28.

Anche il Consiglio di Stato italiano, in una sentenza piuttosto recente [280], ha declinato il principio di trasparenza quale «piena conoscibilità» di tutte le fasi dell'algoritmo, dai suoi autori al funzionamento del procedimento seguito, dal meccanismo di decisione agli aspetti cui si è data priorità durante la procedura decisionale, sino ai dati utilizzati dal procedimento automatizzato, al fine di discernere i casi in cui il potere autoritativo resti imputabile alla persona fisica.

Passando in rassegna il principio di esattezza, tale criterio richiede che i dati personali siano «esatti e, se necessario, aggiornati»[281]. Da qui discende, da un lato, l'obbligo, posto a carico del titolare, di procedere alla cancellazione o rettifica tempestiva di tutti i dati inesatti rispetto alle finalità per le quali sono trattati, dall'altro, il diritto di cui godono gli interessati di ottenere la rettifica dei dati personali inesatti e l'integrazione dei dati incompleti.

Da ultimo, occorre precisare che il principio di integrità e riservatezza risulta strettamente connesso non solo al principio di sicurezza dei dati, ma anche al principio di *accountability.* Come abbiamo avuto modo di precisare, infatti, a differenza del previgente regime giuridico, l'attuale plesso normativo in materia di protezione dei dati personali non prevede più un elenco delle misure "minime" e misure "idonee" di sicurezza che i titolari devono rispettare per essere *compliance,* ma spetta a ogni titolare le misure di sicurezza tecniche e organizzative che ritiene più adeguate al fine di prevenire il rischio di impatti negativi sulle libertà e sui diritti degli interessati[282].

### 2.1.8. *(Segue):* Spazi di discrezionalità riguardanti il trattamento dei dati biometrici: le scelte del legislatore italiano

Tenendo conto della natura direttamente applicabile del Regolamento, nella presente analisi, abbiamo finora considerato le «particolari categorie di dati», tra cui figurano anche i dati biometrici, di cui si occupa l'art. 9 del GDPR. Pare ora opportuno esaminare la (ulteriore) disciplina prevista per le stesse categorie di dati nel nostro ordinamento giuridico.

[280] Cons. St. Sez. VI, sent. 8 aprile 2019, n. 2270.
[281] Art. 5, par. 1, lett. d) del GDPR.
[282] *Infra,* in questo Capitolo, §2.1.6.

Come si è detto, il Regolamento riconosce, in più punti, spazi di discrezionalità agli Stati membri[283] sia in via generale, sia con specifico riferimento alle particolari categorie di dati, con la conseguenza che il legislatore nazionale conserva la facoltà di «mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute»[284] e, dunque, di introdurre delle deroghe al divieto generale di trattare categorie particolari di dati personali, «fatte salve adeguate garanzie» per salvaguardare i dati personali e i diritti fondamentali[285].

Sfruttando il margine di autonomia che gli è riconosciuto, dunque, il legislatore italiano – operate, mediante il d.lgs. 101/2018, delle modifiche al Codice *privacy* – ha scelto di puntualizzare la disciplina delle particolari categorie di dati, dettando una regolamentazione specifica con riferimento a trattamenti specifici svolti, nella sfera pubblicistica, principalmente, in materia sanitaria, in materia scolastica, a fini di archiviazione o di ricerca o a fini statistici, per finalità giornalistiche o riguardanti altre manifestazioni del pensiero[286].

Ad opera della riforma del 2018, sono stati altresì introdotti nel *corpus* del Codice *privacy* l'art. 2-sexies e l'art. 2-septies.

---

[283] In senso critico si esprime F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 121, ove si paventa il rischio di vanificare – per il tramite degli ampi margini di discrezionalità lasciati ai singoli Stati membri – il livello di armonizzazione in materia di protezione dei dati personali, che costituisce peraltro il motivo principale per cui si è scelto di adottare un Regolamento e non una Direttiva.

[284] Così dispone il Considerando n. 53 del Regolamento.

[285] Così dispone il Considerando n. 52 del Regolamento. Similmente, il Considerando n. 51 dispone che le categorie particolari di dati non dovrebbero, in linea generale, essere oggetto di trattamento, salvo il caso in cui il trattamento sia consentito nei casi specifici previsti dal Regolamento o dal diritto degli Stati membri. Si precisa, poi, che dovrebbero comunque osservarsi i principi generali e le altre norme previste nel Regolamento, in particolare le condizioni per il trattamento lecito. Il tema è affrontato anche nel Considerando n. 8.

[286] A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 222 ss. Si vedano, tra gli altri, l'art. 2-*novies* (Trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte Costituzionale), l'art. 60 (Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale), l'art. 61 (Utilizzazione di dati pubblici e regole deontologiche), l'art. 100 (Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici), l'art. 110 (Ricerca medica, biomedica ed epidemiologica). La medesima Autrice segnala che l'adeguamento alle novità introdotte dal Regolamento ha richiesto anche la revisione del regime precedentemente vigente riguardante le autorizzazioni individuali – cui dovevano essere sottoposti i dati sensibili, tra cui i dati biometrici, per poter essere oggetto di trattamento – e le autorizzazioni di carattere generale. In particolare, le prime sono state eliminate, mentre alle seconde è toccata diversa sorte: il Garante *privacy* italiano ha sottoposto le autorizzazioni generali ad una verifica di compatibilità con il GDPR, all'esito della quale alcune sono state ritenute compatibili, altre non compatibili con il nuovo assetto dei diritti delineato dal Regolamento.

In particolare, l'art. 2-*sexies*, sulla scorta di quanto previsto all'art. 9, par. 1, lett. g) del GDPR, detta le condizioni necessarie per il trattamento di «categorie particolari di dati personali»[287] (tra cui, val la pena ricordare, i dati biometrici) necessario per «motivi di interesse pubblico rilevante». Per ragioni di razionalizzazione e semplificazione, tale norma – specificato il contenuto della base giuridica, che necessariamente deve essere costituita da una norma di natura legislativa o regolamentare – riunisce in un elenco non esaustivo i trattamenti da ritenersi effettuati per motivi di interesse pubblico. A titolo esemplificativo, figurano in tale elenco i trattamenti in materia di cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato del rifugiato; le attività di controllo e ispettive; la materia riguardante l'obiezione di coscienza; i compiti del servizio sanitario nazionale e dei soggetti che operano in ambito sanitario, l'istruzione e la formazione scolastica, professionale, superiore o universitaria[288].

Significative sono poi le disposizioni dettate dall'art. 2-septies, dedicato alle «misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute», ove si prevede che il Garante della *privacy* italiano possa assumere un provvedimento generale con cui individuare le misure di garanzia[289] e le eventuali altre condizioni necessarie per garantire i diritti degli interessati. Invero, tale provvedimento potrebbe prestare il fianco alla reintroduzione di quei meccanismi formali e procedurali previsti nel precedente quadro normativo (l. 675 e d.lgs. 196/2003), tra cui l'autorizzazione al trattamento di dati sensibili, che invece il Regolamento ha voluto eliminare e sostituire con altri istituti[290].

Senonché, al momento, pare che nessun provvedimento generale di tal guisa sia stato adottato dal Garante della *privacy* italiano.

Alla luce di tali disposizioni, la dottrina più avveduta ha sottolineato il nuovo atteggiamento del legislatore europeo, il quale sempre più, nel complesso bilanciamento tra il diritto alla protezione dei dati personali e gli altri interessi in gioco, sta spostando il

[287] Per mezzo dell'adeguamento apportato dal d.lgs. n. 101/2018, il legislatore italiano ha chiarito che l'espressione «dati sensibili» cui si riferiva l'originario Codice *privacy* si intende riferita alle «categorie particolari di dati» cui fa riferimento l'art. 9 del GDPR (art. 22 del d.lgs. n. 101/2018).
[288] G. MALAZZANI, *Il trattamento di categorie particolari di dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 231.
[289] In particolare, le misure di garanzia possono individuare le misure di sicurezza, quali la cifratura, la pseudonomizzazione, le tecniche di minimizzazione e altre misure volte a proteggere i diritti degli interessati (art. 2-*septies*, c. 5 del Codice *privacy*).
[290] F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 121.

baricentro verso l'interesse collettivo e pubblico. Da ciò discende un importante aspetto che permea la materia *de qua:* anche in virtù degli effetti prodotti sul diritto dall'innovazione tecnologica, dall'evoluzione sociale e dalla globalizzazione, si sta progressivamente superando la dimensione "proprietaria" e "dominicale" dei dati personali, figlia del diritto alla *privacy* come elaborato da Warren e Brandeies[291], a favore di logiche basate sulla condivisione dei dati personali. La materia del trattamento dei dati, dunque, sembra abbandonare la rigida dimensione individuale (propugnata con forza sino ai giorni nostri) e cerca di accogliere e modulare spinte all'apparenza antagoniste. Nel nuovo assetto delineato nel Regolamento, dimensione individuale e dimensione pubblica sembrano intrecciarsi tra loro, nella consapevolezza che la libera circolazione dei dati non può che contribuire alla costruzione di un ordinamento democratico[292].

Tale ottica di (parziale) sacrificio dell'interesse individuale in nome di superiori esigenze di carattere collettivo o sociale sembra essere confermata all'art. 23 del Regolamento, il quale individua quegli ambiti – quali sicurezza nazionale, sicurezza pubblica, difesa, prevenzione e contrasto dei reati, salvaguardia dell'indipendenza della magistratura – con riferimento ai quali il legislatore europeo o nazionale possono prevedere limitazioni alla portata degli obblighi e dei diritti previsti in materia di protezione dei dati personali, purchè la limitazione «rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica»[293].

### 2.1.9. *(Segue):* La funzione nomofilattica del Comitato europeo per la protezione dei dati personali

Uno degli elementi di maggiore novità introdotti con il GDPR è stata l'istituzione del Comitato europeo per la protezione dei dati (anche *European Data Protection Board* o EDPB), strumento introdotto nella prospettiva di promuovere l'applicazione uniforme

[291] S. D. WARREN, L. BRANDEIES, *The right to privacy,* in *Harward Law Review,* 1890, n. 5, 193 ss.
[292] F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 122-126.
[293] *Ivi*, 123.

del Regolamento e di assicurare un efficace coordinamento delle attività delle Autorità di controllo dei singoli Stati membri e della Commissione[294].

Il Comitato europeo – organismo indipendente dell'Unione[295] dotato di personalità giuridica[296] – ha sostituito il "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (generalmente indicato fra gli "addetti ai lavori" come Gruppo di Lavoro "Articolo 29" o, anche, *Article 29, Data Protection Working Party* o WP29), il quale sotto la vigenza della Direttiva 95/46/CE costituiva l'organo di «raccordo permanente» tra le singole Autorità nazionali[297]. A differenza dell'attuale Gruppo dei garanti europei, tuttavia, il WP29 non aveva il potere di emanare decisioni vincolanti, essendogli demandate esclusivamente funzioni consultive, tra cui il compito di elaborare, anche su indicazione della Commissione, pareri e opinioni in ordine alla corretta interpretazione delle disposizioni contenute nella Direttiva[298].

Seppure l'attività svolta dal Gruppo di Lavoro "Articolo 29" ha assunto notevole rilevanza nel consentire di governare il «tumultuoso sviluppo delle nuove tecnologie»[299], il nuovo assetto delineato dal Regolamento ha suggerito al legislatore la necessità di istituire un organismo dotato di compiti e poteri più ampi, nonché di un maggiore grado di vincolatività nelle decisioni adottate[300].

Il Comitato europeo per la protezione dei dati è composto dalla figura di vertice delle Autorità di controllo di ciascuno Stato membro e dal Garante europeo per la protezione dei dati[301] (anche *European Data Protecton Supervisor* o EDPS o GEPD), o

---

294 C. IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 725-729.

295 Considerando n. 139 del Regolamento UE 2016/679.

296 Art. 68, par. 1 del Regolamento, ove si precisa che il Comitato europeo è rappresentato dal suo Presidente.

297 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016, 113.

298 C. IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 725-729; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016, 113-114.

299 *Ivi*, 114.

300 C. IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 728.

301 Il Garante europeo per la protezione dei dati non era previsto dalla Direttiva 95/46/CE e, dunque, non era annoverato fra le Autorità di controllo, sebbene sin dalla sua istituzione partecipasse alle attività del gruppo "Articolo 29". Con il passaggio al nuovo Regolamento europeo, è espressamente previsto che il GEPD (EDPS, in inglese) partecipi alla struttura dell'EDPB. Tuttavia, il Garante europeo conserva una posizione specialmente consultiva, essendogli demandati diritti di voto limitati. Si veda, per un approfondimento, F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016, 115 ss.

dai relativi rappresentanti. Inoltre, ha diritto di partecipare alle attività e alle riunioni del Comitato, ma senza diritto di voto, anche la Commissione, mentre il Garante europeo della protezione dei dati dispone di diritti di voto limitati a casi specifici[302].

Il Regolamento, nell'istituire e disciplinare la figura del Comitato europeo, si preoccupa anzitutto di precisare che opera «con indipendenza» e che «nell'esecuzione dei suoi compiti e nell'esercizio dei suoi poteri non sollecita né accetta istruzioni da alcuno[303]». Si tratta di un profilo particolarmente rilevante, in quanto garantisce l'indipendenza dell'organo da ogni Istituzione europea.

Al Comitato europeo è demandata una molteplicità di compiti[304], da attività di controllo e «sorveglianza» sulla corretta e uniforme applicazione del Regolamento, a funzioni consultive e, ancora, da attività di pubblicazione di linee guida, raccomandazioni e migliori prassi ad attività di elaborazione dei codici di condotta uniformi, nonché, infine, la funzione di individuazione dei requisiti necessari per l'accreditamento degli organismi di certificazione.

Come anticipato, il Comitato europeo è stato istituito con il dichiarato intento di garantire l'applicazione uniforme del Regolamento[305]: esso, infatti, assume un ruolo centrale ai fini della piena realizzazione del c.d. meccanismo di coerenza[306] finalizzato a realizzare la cooperazione tra le autorità di controllo degli Stati membri, in quanto tale organo vigila sulle attività svolte dalle Autorità di controllo e dalla Commissione, nonché assicura il coordinamento delle azioni intraprese dagli Stati membri e dalle loro *Data Protection Authorities* (c.d. DPA). Alla luce di tali osservazioni, il Comitato europeo può essere considerato un vero e proprio «organo di chiusura del sistema» per ciò che concerne l'applicazione e l'attuazione delle norme contenute nel Regolamento[307].

L'attuazione del meccanismo di coerenza è assicurata, anzitutto, dal compito, attribuito al Comitato europeo, di formulare pareri sui progetti di decisione delle Autorità

[302] Rispettivamente, art. 68, par. 3, par. 5 e par. 6 del Regolamento. Il Garante europeo della protezione dei dati, in dettaglio, gode di diritti di voto solamente con riferimento alle decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione.
[303] Sono, tuttavia, fatte salve per espressa previsione normativa le richieste della Commissione di cui all'art. 70, par. 1 e 2 del Regolamento.
[304] Detti compiti sono dettagliatamente enucleati all'art. 70 del GDPR.
[305] Art. 70, par. 1, lett. a) del Regolamento, ove sono fatti comunque salvi i compiti attribuiti alle Autorità nazionali di controllo.
[306] Si vedano, in particolare, l'art. 63 e il Considerando n. 135 del Regolamento.
[307] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 2, *Il Regolamento europeo 2016/679,* Torino, 2016, 105.

di controllo, nonché di emettere pareri relativi a questioni determinate[308]. Esso, inoltre, ha la facoltà di intervenire, emettendo decisioni vincolanti, nella composizione di controversie che insorgano tra le diverse Autorità di controllo[309] e nelle circostanze eccezionali in cui emerga un'urgente necessità di tutelare i diritti e le libertà dei cittadini[310].

Allo scopo di realizzare la sua funzione nomofilattica, il Comitato europeo, inoltre, incoraggia la cooperazione e lo scambio di informazioni e prassi tra le Autorità di controllo sia a livello bilaterale che multilaterale e promuove programmi comuni di formazione tra le Autorità di controllo, nonché lo scambio di conoscenze e documentazioni in materia di protezione dei dati personali tra le Autorità di controllo di tutti quei Paesi in grado di influenzare direttamente o indirettamente l'implementazione del Regolamento[311].

Quale organo consultivo, il Comitato europeo fornisce indicazioni e pareri alla Commissione con riferimento a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese le eventuali proposte di modifica del Regolamento medesimo[312]; parimenti, fornisce consulenza alla Commissione sul formato e sulle procedure inerenti allo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e Autorità di controllo in ordine alle norme vincolanti d'impresa[313].

L'attività consultiva del Comitato europeo si estende, inoltre, anche alla emanazione di pareri, sempre destinati alla Commissione, in merito all'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così da valutare se questi ultimi siano in grado di assicurare un livello adeguato di protezione[314].

Il Comitato europeo si occupa, altresì, di predisporre e pubblicare linee guida, raccomandazioni e migliori prassi, occupandosi anche del periodico controllo ed aggiornamento delle medesime[315].

---

[308] Art. 70, par. 1, lett. t) del GDPR. Il riferimento, qui, è alle questioni presentate a norma dell'art. 64 del GDPR.
[309] Art. 65 del Regolamento.
[310] Art. 66 del Regolamento.
[311] Rispettivamente, art. 70, par. 1, lett. u), v) e w) del Regolamento. Si veda anche C. IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 737.
[312] Art. 70, par. 1, lett. b) del GDPR.
[313] Art. 70, par. 1, lett. c) del Regolamento.
[314] Art. 70, par. 1, lett. s) del GDPR.
[315] Il Comitato europeo pubblica linee guida, raccomandazioni e migliori prassi in merito a numerose materie enucleate in maniera certosina all'art. 70 del Regolamento, tra cui: procedure per la cancellazione

A detto organo compete, inoltre, la predisposizione dei codici di condotta e dei meccanismi di certificazione della protezione dei dati, nonché dei sigilli e marchi di protezione[316], allo scopo di garantire la migliore attuazione della nuova normativa. La finalità di garantire l'applicazione coerente del Regolamento si concretizza, inoltre, nel compito di formulare pareri sui codici di condotta redatti nell'ambito dell'Unione europea[317].

Da ultimo, egualmente significativa è la funzione demandata al Comitato europeo di individuare i requisiti necessari per l'accreditamento degli organismi di certificazione[318]. Sulla scorta di tali criteri, ciascuno Stato membro ha la facoltà di scegliere se attribuire il potere di accreditamento al Garante nazionale o ad altro organismo nazionale[319].

## 2.2. La Proposta di Regolamento (UE) sull'Intelligenza Artificiale avanzata dalla Commissione europea

### 2.2.1. *(Segue):* Il sostrato giuridico della Proposta di Regolamento (UE) sull'Intelligenza Artificiale

di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico (lett. d); qualsiasi questione relativa all'applicazione del Regolamento, proprio allo scopo di garantire l'applicazione uniforme della normativa (lett. e); allo scopo di specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione (lett. f); in materia di accertamento, violazione di dati personali e determinazione dell'ingiustificato ritardo di cui all'articolo 33, paragrafi 1 e 2, oltre alle circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali (lett. g); relativamente alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (lett. h); in materia di procedure per le segnalazioni da parte di persone fisiche di violazioni dei dati personali (lett. m).

[316] Art. 70, par. 1, lett. n) del Regolamento. A tal proposito, al Comitato europeo è demandato anche il compito di accreditare gli organismi di certificazione, nonché di tenere un registro pubblico dei maccanismi di certificazione e dei titolari o responsabili del trattamento (lett. o). Sotto tale profilo, F. PIZZETTI, *Gdpr e linee guida per pmi, che c'è da attendersi dal Garante privacy,* in *Agenda digitale,* editoriale del 2 ottobre 2018, osserva che tale funzione del Comitato europeo non si pone in contrasto con quella che riserva l'adozione di «linee guida di indirizzo» al Garante nazionale (art. 154-*bis* del d.lgs. 101/2018), in quanto il Gruppo dei Garanti europei ha il potere di emanare linee guida, mentre al Garante nazionale è attribuito il potere di emanare mere «linee di indirizzo». Resta comunque aperta la questione relativa all'effettivo valore giuridico di tali strumenti di *soft law,* come sottolineato in F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016, 111.

[317] Art. 70, lett. x) del GDPR.

[318] Art. 70, lett. p) del Regolamento.

[319] Esercitando tale facoltà, il legislatore italiano ha individuato, quale organismo nazionale di accreditamento, l'Ente unico nazionale di accreditamento, fatto salvo il potere del Garante di assumere l'esercizio di tali funzioni, in caso di grave inadempimento dell'Ente (art. 2-septiesdecies del d.lgs. 101/2018). Sul punto si veda F. PIZZETTI, *Decreto Gdpr, le urgenze dopo l'entrata in vigore (19 settembre),* in *Agenda digitale,* editoriale del 5 settembre 2018, il quale mette in luce, pur sottolineandone la complessità, il merito della norma di aver «procedimentalizzato» il tema.

Come accennato, nonostante siano state date moltissime definizioni di Intelligenza Artificiale, ad oggi non esiste ancora una nozione, normativa o scientifica, di Intelligenza Artificiale condivisa in seno agli studiosi di tutto il mondo. Le stesse istituzioni, peraltro, da sempre si misurano con il problema definitorio. Per ovviare a tale lacuna, il Parlamento europeo, nel febbraio 2017, nell'ambito della Risoluzione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica[320], ha invitato la Commissione a proporre una definizione normativa comune, mettendo in luce l'esigenza di una nozione flessibile, non troppo analitica e che non ostacolasse l'innovazione[321].

Tale richiesta rappresenta un importante tassello nell'attuazione dell'Agenda Digitale europea[322], lanciata dalla Commissione europea nel 2010, che conferma la grande attenzione posta dalle istituzioni europee in tema di Intelligenza Artificiale[323].

Lungo tale direttrice, si sono collocate, dapprima, la richiesta avanzata dai parlamentari europei di introdurre norme in materia di robotica e Intelligenza

---

[320] PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica,* 2015/2103(INL), 2018/C 252/25, 16 febbraio 2017. Peraltro, il Parlamento europeo ha individuato anche alcune caratteristiche distintive del fenomeno: «l'ottenimento di autonomia grazie a sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività) e lo scambio e l'analisi di tali dati; l'autoapprendimento dall'esperienza e attraverso l'interazione (criterio facoltativo); un supporto fisico minore; l'adattamento del proprio comportamento e delle proprie azione all'ambiente; l'assenza di vita in termini biologici». Nondimeno, U. RUFFOLO, *Prefazione,* in A. F. AURICCHIO, G. RICCIO, U. RUFFOLO, *Intelligenza artificiale tra etica e diritti: prime riflessioni a seguiti del Libro Bianco dell'Unione europea,* Cacucci, Bari, 2020, 25, mette in luce che tale iniziativa proponeva un approccio all'Intelligenza Artificiale ormai superato, in quanto proclamava la necessità di regolare ogni aspetto del fenomeno.

[321] R. ANGELINI, *Intelligenza Artificiale e* governance. *Alcune riflessioni di sistema,* in F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, 294.

[322] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un'agenda digitale europea*, (COM(2010)245 definitivo), 19 maggio 2010.

[323] L'Agenda Digitale europea, lanciata nel 2010 per un periodo di 10 anni (periodo 2010-2020), costituisce un piano strategico-programmatico mediante il quale ciascuno Stato membro si è impegnato a favorire la crescita economica e occupazionale, sfruttando le grandi potenzialità dell'innovazione tecnologica. In sintesi, essa si poneva quale scopo principale quello di creare all'interno del Vecchio Continente un mercato digitale unico e competitivo, in grado di trainare l'economia verso una «crescita intelligente, sostenibile e inclusiva». In particolare, si veda POLITECNICO DI MILANO 1863, SCHOOL OF MANAGEMENT [2023], *Il digitale chiama: l'Italia risponde?* in *Osservatorio agenda digitale, Agenda digitale: la strada per digitalizzare la PA,* consultabile in https://blog.osservatori.net/it_it/agenda-digitale-come-digitalizzare-pa#:~:text=In%20sostanza%2C%20l'Agenda%20Digitale,sul%20potenziale%20delle%20tecnologie%20digitali; M. TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia Digitale,* 24 ottobre 2018, che costituisce una rielaborazione della relazione su *Il libro Bianco dell'AGID sull'intelligenza artificiale,* presentata in occasione del *III Colloquio italo-francese sul Diritto del Web,* svoltosi presso l'Università LUISS Guido Carli il 21 giugno 2018, in collaborazione con l'Università di Parigi Panthèon-Sorbonne. Val la pena sottolineare che proprio in attuazione dell'Agenda Digitale europea, allo scopo di porre le basi per lo sviluppo di un'economia basata sui dati, sono stati adottati i quadri normativi sulla protezione dei dati personali (Regolamento (UE) 2016/679 e Direttiva (UE) 2016/680) che costituiscono il sostrato giuridico del riconoscimento facciale esaminato nella presente trattazione.

Artificiale[324] (16 febbraio 2017), sopra richiamata, seguita dall'idea di istituire un *High-Level Expert Group on Artificial Intelligence*[325] (9 marzo 2018), e successivamente, la Dichiarazione sull'IA da parte dei Gruppo europeo per l'etica delle scienze e delle nuove tecnologie[326] (9 marzo 2018) e le Linee Guida etiche per un'Intelligenza Artificiale affidabile[327] (8 aprile 2019). In questo quadro, si colloca anche la firma, da parte di 24 Stati membri dell'Unione europea e della Norvegia, dell'Accordo di cooperazione per accelerare lo sviluppo dell'IA[328] (10 aprile 2018), cui hanno fatto seguito la Comunicazione della Commissione europea sull'Intelligenza Artificiale[329] (25 aprile 2018) e la Comunicazione della Commissione europea sul piano coordinato per l'Intelligenza Artificiale[330] (7 dicembre 2018), in cui la Commissione elabora – delineando gli obiettivi legislativi, etici e di investimento – un piano di ampio respiro finalizzato allo sviluppo delle nuove tecnologie, con il dichiarato intento di colmare lo svantaggio competitivo dell'Unione rispetto ad altri Stati del mondo.

---

[324] PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)) (2018/C 252/25), 16 febbraio 2017, Considerando C e §1.

[325] COMMISSIONE EUROPEA, *Call for a High-Level Expert Group on Artificial Intelligence,* 9 marzo 2018. *L'High-Level Expert Group on Artificial Intelligence (AI HLEG)* – che raccoglie ben cinquantadue esperti nel campo dell'Intelligenza Artificiale provenienti dal mondo della Pubblica Amministrazione, delle imprese, dell'Università e della ricerca – ha posto la definizione di Intelligenza Artificiale richiamata nella presente trattazione (in particolare, *infra,* in §1.2.1).

[326] COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA RICERCA E INNOVAZIONE, GRUPPO EUROPEO PER L'ETICA DELLE SCIENZE E DELLE NUOVE TECNOLOGIE, *Statement on artificial intelligence, robotics and "autonomous" systems,* 9 marzo 2018. Il Gruppo europeo per l'etica delle scienze e delle nuove tecnologie (EGE) è un organo indipendente con funzioni consultive, istituito dalla Commissione europea per la prima volta nel 1991, con lo scopo di portare alla luce e dare risposta ai problemi etici sollevati dalle nuove tecnologie, come sottolineato in CORDIS, *Il Gruppo europeo di etica delle scienze e delle nuove tecnologie si rinnova e guarda al futuro,* consultabile in https://cordis.europa.eu/article/id/16849-a-revitalised-european-group-on-ethics-and-new-technologies-eyes-the-future/it. Nella relazione, la Commissione europea, nel delineare le problematiche connesse agli sviluppi tecnologici, sottolinea le implicazioni etiche e morali poste dall'Intelligenza Artificiale.

[327] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e social europeo e al Comitato delle Regioni, Creare fiducia nell'Intelligenza Artificiale antropocentrica,* (COM(2019) 168 final), 8 aprile 2019.

[328] COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa,* (COM(2018) 237 final), 25 aprile 2018.

[329] COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa,* (COM(2018) 237 final), 25 aprile 2018.

[330] COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, Piano coordinato sull'Intelligenza Artificiale,* (COM(2018) 795 final), 7 dicembre 2018, ove viene fornita, né per la prima volta né per l'ultima, un'esplicita definizione di "Intelligenza Artificiale", qualificata come «quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici».

In sede nazionale, l'Agenzia per l'Italia Digitale (AgID) ha presentato il Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino[331] (21 marzo 2018), curato da un Gruppo di esperti italiani, allo scopo di studiare opportunità e rischi dell'AI nel rapporto tra la Pubblica Amministrazione e i cittadini[332].

In aggiunta, esprimendo profonde preoccupazioni in merito all'impiego di alcuni *software,* tra i quali il riconoscimento facciale e vocale, quando inseriti in programmi di «sorveglianza emotiva», vale a dire di monitoraggio dello stato mentale e psicologico dei cittadini con lo scopo di aumentare la produttività sul luogo di lavoro, il Parlamento europeo – nella Risoluzione su una politica industriale europea globale in materia di robotica e intelligenza artificiale[333] (12 febbraio 2019) – ha posto in luce che tali sistemi di Intelligenza Artificiale contraddicono *in re ipsa* quei diritti fondamentali che costituiscono i capisaldi su cui si fonda l'Unione europea.

Inoltre, in data 19 febbraio 2020, dando seguito all'invito del Parlamento, la Commissione europea ha presentato il Libro Bianco sull'Intelligenza Artificiale[334], che costituisce il preludio all'adozione della Proposta di Regolamento di cui si dirà nel proseguo della trattazione.

Tale atto di *soft law* mette in luce le ambivalenze dell'evoluzione tecnologica *in fieri*: da un lato, sottolinea che «l'intelligenza artificiale si sta sviluppando rapidamente» e consentirà un maggiore efficienza dei sistemi di produzione; dall'altro lato, tuttavia, rileva che l'utilizzo degli algoritmi e delle decisioni automatizzate cela «una serie di rischi

---

[331] AGENZIA PER L'ITALIA DIGITALE, *Libro Bianco sull'intelligenza Artificiale al servizio del cittadino,* 21 marzo 2018. Il Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino ha contribuito a porre al centro del dibattito pubblico prospettive e rischi del ricorso agli algoritmi e alle decisioni automatizzate da parte della Pubblica Amministrazione italiana. A tale scopo, la parte centrale del Libro Bianco individua le nove sfide poste dall'Intelligenza Artificiale: Etica, Tecnologia, Competenza, Ruolo dei dati, Contesto legale, Accompagnare la trasformazione, Prevenire le diseguaglianze, Misurare l'impatto, L'essere umano. Seguono una lista di raccomandazioni finalizzate all'implementazione degli strumenti di IA e un elenco di suggerimenti – evidentemente dotati di solo valore esortativo nei confronti delle amministrazioni, essendo privi di qualsivoglia valore precettivo. Si veda, per un maggiore approfondimento, M. TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia Digitale,* 24 ottobre 2018.

[332] Come sottolineato da M. TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia Digitale,* cit., tale gruppo di lavoro è composto da trenta esperti provenienti dal mondo accademico, dalle organizzazioni internazionali, del mercato e delle *start-up*.

[333] PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale, Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale*, 2018/2088(INI), 2020/C 449/06, 12 febbraio 2019.

[334] COMMISSIONE EUROPEA, *Libro Bianco sull'Intelligenza Artificiale – Un approccio europeo all'eccellenza e alla fiducia,* (COM/2020/65 final), 19 febbraio 2020.

potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali»[335]. Beninteso, il mercato unico europeo trae la sua forza, sempre di più, dal valore economico dei dati e sulla loro circolazione e le istituzioni europee puntano a creare «un clima di fiducia» nei confronti dell'Intelligenza Artificiale, ma non si deve trascurare di considerare i rischi potenziali ad essa connessi[336].

Accogliendo tali ambivalenze, il progetto promosso dal Libro Bianco – che punta a rendere l'Unione Europea «*leader* mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni»[337] – si fonda su due linee strategiche complementari: da un lato, dare vita ad un "ecosistema di eccellenza" in ricerca e innovazione, allo scopo di accelerare soluzioni basate sull'IA[338]; dall'altro lato, in una spiccata vocazione antropocentrica[339], creare un "ecosistema di fiducia" nei confronti dell'IA, rassicurando gli Stati Membri e i cittadini che lo sviluppo dell'IA avverrà comunque nel rispetto delle norme dell'UE, comprese le norme a tutela dei diritti fondamentali[340].

In particolare, il Libro Bianco prevede che, nei "settori ad alto rischio", i sistemi di IA debbano essere sviluppati responsabilmente, in quanto gli addetti ai lavori devono valutare *ex ante* i rischi connessi allo sviluppo di tali tecnologie e, conseguentemente, adottare tutte le misure ragionevoli per ridurre al minimo il rischio di danni, garantendo comunque un adeguato coinvolgimento dell'essere umano[341]. Tra i settori ad alto rischio, il Libro Bianco menziona anche i sistemi di riconoscimento facciale impiegati in luoghi pubblici, ribadendo – senza soluzione di continuità con le prescrizioni contenute nel GDPR – che la raccolta e l'uso dei dati biometrici a scopo di identificazione sono in linea generale vietati, a meno che tale uso non sia giustificato, proporzionato e soggetto a una serie di condizioni. Ad ogni modo, il Libro Bianco propone l'avvio di un dibattito europeo sulle circostanze specifiche che potrebbero giustificare il ricorso al riconoscimento facciale e sulle garanzie necessarie[342].

---

[335] *Ivi,* 1.
[336] *Ivi,* 2 ss.
[337] *Ibidem.*
[338] *Ivi,* 5 ss.
[339] Il Libro Bianco sull'Intelligenza artificiale sostiene che è l'Intelligenza Artificiale a dover essere messa al servizio dell'uomo, e non viceversa, e palesa la necessità che i sistemi di IA rispettino sempre il principio generale dell'equità, nonché i diritti e le libertà dei cittadini.
[340] *Ivi*, 10 ss.
[341] *Ivi*, 25 ss.
[342] *Ivi*, 24.

Viceversa, nei settori a basso rischio (*rectius,* settori non considerati "ad alto rischio"), il Libro Bianco propone il c.d. sistema di etichettatura su base volontaria, in base al quale, cioè, gli operatori economici – a cui sarebbe in tal caso assegnato uno speciale marchio di qualità – possano decidere volontariamente di conformarsi alle prescrizioni previste per i settori ad alto rischio, dimodoché i consumatori siano messi nella condizione di riconoscere prodotti e servizi conformi a determinati parametri di riferimento[343].

Ulteriori sollecitazioni per un intervento normativo del fenomeno *de quo* sono pervenuti ancora una volta dal Parlamento europeo, il quale – nella Proposta di Risoluzione recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'Intelligenza Artificiale, della robotica e delle tecnologie correlate[344] (8 ottobre 2020) – ha chiaramente sottolineato l'esigenza di regolamentare Intelligenza Artificiale, robotica e tecnologie correlate, prendendo posizione a favore di un approccio normativo basato sul rischio e orientato al futuro; d'altra parte, il Parlamento si è pronunciato a favore di un elenco esaustivo e cumulativo di settori ad alto rischio subordinato ad una revisione periodica, considerata la natura evolutiva di tali tecnologie[345].

Dando seguito ai copiosi interventi delle Istituzioni europee, e a fronte dell'ormai ineludibile esigenza di sviluppare un "ecosistema di fiducia" promossa dal Libro Bianco, il 21 aprile 2021 – nell'ambito della Strategia europea sull'innovazione – la Commissione europea ha pubblicato la "Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione" (di seguito anche Proposta sull'Intelligenza Artificiale o Proposta o Legge sull'IA o *AI Act*), che ambisce a porre il primo quadro giuridico al mondo in tale materia.

Nel proseguo della presente analisi – senza pretesa di essere esaustivi sull'intera disciplina normativa proposta dalla Legge sull'IA – prenderemo dapprima in considerazione la classificazione dei sistemi di IA come operata dalla Proposta, soffermandoci maggiormente sulle norme che si riferiscono ai sistemi di identificazione

[343] *Ivi*, 27 ss.
[344] PARLAMENTO EUROPEO, *Proposta di risoluzione del parlamento europeo, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate,* 2020/2012(INL), 8 ottobre 2020.
[345] *Ivi*, par. 12.

biometrica; esamineremo in un successivo momento il Parere congiunto formulato dall'EDPB e dall'EDPS, nonché il parere reso dall'Garante italiano – considerando in entrambi i casi soprattutto le raccomandazioni espresse dalle Autorità rientranti nell'ambito di interesse della presente trattazione.

### 2.2.2. *(Segue):* La disciplina giuridica sull'IA contenuta nel *draft* di Regolamento

Va preliminarmente osservato che, similmente al Libro Bianco, la Proposta, da un lato, mette in luce che l'Intelligenza Artificiale è in grado di apportare benefici sociali ed ambientali, oltre a fornire vantaggi competitivi all'economia europea in settori strategici[346]; dall'altro lato – nella consapevolezza dei nuovi rischi posti per le persone fisiche e per la società – si propone la finalità di salvaguardare i valori e i diritti fondamentali dell'UE, nonché la sicurezza degli utenti[347].

In tale contesto, la il *draft* di Regolamento si pone, quale obiettivo principale, quello di assicurare il buon funzionamento del mercato interno, fissando regole di immediata applicabilità relative allo sviluppo, all'immissione sul mercato dell'Unione e all'utilizzo di prodotti che servizi che utilizzano componenti di Intelligenza Artificiale o forniti come sistemi indipendenti di IA (c.d. prodotti *stand-alone*)[348].

Difatti, la natura transnazionale del fenomeno richiede che le norme siano poste a livello di UE, in modo da evitare che in futuro – come pure è stato paventato – singoli Stati membri prendano l'iniziativa legislativa per disciplinare l'IA nel rispetto dei diritti fondamentali. Detto in diversi termini, la Proposta mira – in virtù della fonte adottata – ad evitare che l'adozione di tante regole nazionali comporti: i) una frammentazione del mercato interno; ii) una conseguente riduzione sostanziale della certezza del diritto[349]. Tale risultato può essere conseguito soltanto mediante una fonte normativa di immediata applicabilità negli ordinamenti giuridici di tutti gli Stati Membri: il formarsi di un mosaico di regole nazionali potenzialmente differenti creerebbe ostacoli alla circolazione dei

[346] Sono compresi il settore dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico e della finanza, nonché il settore primario.
[347] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, Relazione,* (COM(2021) 206 final), 21 aprile 2021, 1-3.
[348] *Ivi,* 6. Che l'obiettivo principale della Legge sull'IA sia quello di istituire un quadro giuridico uniforme in grado di migliorare il funzionamento del mercato interno – tutelando al contempo imperativi interessi pubblici e diritti fondamentali delle persone – lo si ricava già dal Considerando n. 1.
[349] *Ibidem*.

negozi giuridici, diminuendo senz'altro la competitività dei produttori e dei fornitori dei sistemi di IA stabiliti nel territorio dell'UE[350].

Non stupisce, dunque, che la base giuridica su cui si fonda la Legge sull'IA è innanzitutto costituita dall'art. 114 del TFUE, che impone che siano adottate una serie di misure destinate all'instaurazione o al funzionamento del mercato interno[351].

Senonché, ciò che qui preme sottolineare è lo stretto rapporto intercorrente tra la Proposta in esame e il trattamento dei dati personali: dal momento che essa prende in esame anche sistemi di AI che comportano il trattamento di dati biometrici (*i.e.* personali), che costituiscono la maggior parte di sistemi di IA, ulteriore base giuridica è costituita dall'art. 16 TFUE[352], cioè la stessa base giuridica su cui si fonda il GDPR.

Venendo alla disciplina normativa, la Proposta pone innanzitutto – avvalendosi anche della tecnica dell'elencazione – un'esplicita definizione di sistema di Intelligenza Artificiale, qualificata come «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I[353], che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Ebbene, il legislatore europeo – nella difficoltà di rintracciare una caratteristica unica suscettibile di essere impiegata in vista di una nozione strutturale unitaria – non dà una definizione per caratteri, ponendo piuttosto la regola della legalità e della tipicità, affermando che è Intelligenza Artificiale soltanto quel *software* sviluppato con una o più delle tecniche e degli approcci elencati dal legislatore europeo, in grado di generare un determinato risultato. Dunque, la nozione strutturale di Intelligenza Artificiale è del tutto relativa, rimessa all'apprezzamento discrezionale della Commissione europea, che può

[350] *Ivi*, 7. Da tale obiettivo principale derivano, a cascata, una serie di obiettivi specifici: oltre ad assicurare la certezza del diritto con lo scopo di attrarre investimenti nazionali e internazionali, la Proposta vuole garantire che i sistemi di IA immessi e impiegati sul mercato europeo siano leciti, sicuri e affidabili; conseguentemente, essa si propone l'ulteriore finalità di migliorare la governance esistente in materia di diritti fondamentali e requisiti di sicurezza dei sistemi di IA.
[351] *Ivi*, 6.
[352] *Ivi*, 7. In particolare, l'art. 16 del TFUE stabilisce che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
[353] Allo stato attuale, le tecniche e gli approcci nominati nell'Allegato I sono i seguenti: a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (c.d. *deep learning*); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima *bayesiana*, metodi di ricerca e ottimizzazione.

peraltro aggiornare l'elenco contenuto nell'Allegato I, così da tener conto del progresso tecnologico e degli sviluppi del mercato[354].

All'esito di un'ampia consultazione di tutti i principali portatori di interessi[355], il *draft* di Regolamento adotta un approccio normativo proporzionato basato sul rischio[356]. Detto in diversi termini, esso opera una classificazione dei sistemi di IA in virtù del rischio di impatto negativo che potrebbero comportare sui diritti fondamentali dell'uomo, quali la dignità umana, la vita privata, la protezione dei dati personali, la non discriminazione, la parità tra uomo e donna, la salute e la sicurezza[357]: maggiore è il rischio che il prodotto (che utilizza parzialmente o totalmente componenti di IA) incida in maniera negativa su tali diritti, maggiore è la severità della soluzione adottata[358]. In particolare, il rischio viene ripartito su quattro differenti livelli: il rischio inaccettabile, l'alto rischio, il rischio limitato e il rischio minimo[359].

Partendo dal rischio inaccettabile, l'art. 5 della Proposta vieta le pratiche di intelligenza artificiale che prevedano: a) «l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali» che operano senza la consapevolezza della persona «al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico»; b) «l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone», causate dall'età o dalla disabilità fisica o mentale, «al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico»; c)

---

[354] Art. 4 della Proposta.
[355] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, Relazione,* (COM(2021) 206 final), 21 aprile 2021, 8-11.
[356] *Ivi,* 7.
[357] Tale catalogo di diritti fondamentali che potrebbero essere pregiudicati dall'Intelligenza Artificiale è contenuto in COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio* cit., 12.
[358] C. PALMIERI, *Intelligenza Artificiale, il nuovo quadro normativo europeo,* in *Altalex,* 17 agosto 2021, consultabile in https://www.altalex.com/documents/news/2021/05/20/intelligenza-artificiale-nuovo-quadro-normativo-europeo.
[359] G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021, consultabile in https://www.dirittobancario.it/art/intelligenza-artificiale-una-prima-analisi-della-proposta-di-regolamento/#:~:text=Intelligenza%20artificiale%3A%20una%20prima%20analisi%20della%20proposta%20di%20regolamento%20europeo,-27%20Maggio%202021&text=Nel%20corso%20degli%20ultimi%20anni,(di%20seguito%20anche%20IA).

«l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto» allo scopo di valutare o classificare l'affidabilità delle persone fisiche per un determinato periodo di tempo «sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste», in modo tale che il punteggio sociale (c.d. *social scoring*) ottenuto comporti una o entrambe le seguenti conseguenze: i) «un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche» in contesti sociali diversi da quello in cui i dati sono stati originariamente raccolti; ii) «un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità»[360].

Orbene, la lettera d) del medesimo articolo menziona espressamente i sistemi di identificazione biometrica remota "in tempo reale", vietando in linea generale il loro uso «in spazi accessibili al pubblico a fini di attività di contrasto»[361].

Ai fini della normativa in questione, sono considerati sistemi di identificazione biometrica remota quei sistemi di IA finalizzati *all'identificazione a distanza* di persone fisiche mediante il confronto tra i dati biometrici di una persona e i dati biometrici contenuti in un *database,* senza che l'utente del sistema di IA sia a conoscenza se la persona sia presente o meno nel *database* medesimo[362]. I sistemi di identificazione biometrica remota possono essere ulteriormente suddivisi in sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori": nel primo caso, il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, includendo sia le identificazioni istantanee sia quelle che avvengono con brevi ritardi, allo scopo di evitare elusioni della normativa[363]. In tutti gli altri casi – in cui il rilevamento, il confronto e l'identificazione avvengono con un ritardo significativo – si parla di sistema di identificazione biometrica remota "a posteriori"[364]. Si tratta di materiale – immagini o filmati – che è stato generato prima che il sistema fosse usato per l'identificazione delle persone fisica[365].

[360] Art. 5, par. 1, lett. a), b) e c) della Proposta.
[361] Art. 5, par. 1, lett. d) della Proposta.
[362] Tale definizione di "sistema di identificazione biometrica remota" è contenuta all'art. 3, n. 36 della Proposta di Regolamento; enfasi aggiunta. Una simile definizione è contenuta al Considerando n. 8, il quale precisa che è irrilevante, ai fini di classificazione, la tecnologia o i processi utilizzati, nonché i dati biometrici estratti.
[363] Art. 3, n. 37 della Proposta.
[364] Art. 3, n. 38 della Proposta.
[365] Considerando n. 8 della Proposta.

Sebbene in linea generale vietato, l'uso dei sistemi *de quo* è consentito qualora sia «strettamente necessario» per una delle finalità ivi indicate: i) la ricerca mirata di potenziali vittime di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia «specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico»; iii) «il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato» di determinati reati (a titolo esemplificativo, partecipazione ad un'organizzazione criminale, terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia infantile, corruzione, omicidio volontario, traffico illecito di organi e tessuti umani), punibili nello Stato membro in cui il reato è stato commesso «con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni»[366].

Ebbene, la Proposta richiede allo Stato membro di realizzare una sorta di analisi costi-benefici – dovendo stimare comparativamente i possibili vantaggi e i relativi costi – allo scopo di valutare l'utilità e l'opportunità di introdurre i sistemi di cui in discorso: le autorità competenti possono introdurre i sistemi di identificazione biometrica *de quibus*, tenendo conto da un lato, della «natura della situazione» e dall'altro lato, delle «conseguenze» che potrebbero derivarne «per i diritti e le libertà di tutte le persone interessate». Nel primo caso, bisogna avere particolare riguardo alla «gravità», «probabilità» e «entità del danno» che ne deriverebbe qualora, all'opposto, il sistema non venisse utilizzato. Nel secondo caso, bisogna avere riguardo alla «gravità», «probabilità» e «entità» delle sopracitate conseguenze[367].

In ogni caso, l'utilizzo di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di *law enforcement* è subordinato al rilascio di un'autorizzazione preventiva da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, la quale accerti la sussistenza dei requisiti richiesti dalla presente Proposta, al contempo verificando che l'uso del sistema biometrico sia «necessario e proporzionato» al raggiungimento delle finalità indicate nell'art. 5, par. 1, lett. d) della Proposta[368].

---

[366] Art. 5, lett. d) della Proposta.

[367] Art. 5, par. 2 della Proposta, il quale, in aggiunta, opera un esplicito riferimento alla necessità, per lo Stato membro che intenda introdurre i sistemi biometrici *de quibus*, di prevedere limitazioni temporali, geografiche e personali all'introduzione di siffatti sistemi.

[368] Art. 5, par. 3 della Proposta. A tal fine, la medesima norma prevede l'obbligo per ogni Stato membro di introdurre nel proprio tessuto normativo regole chiare e dettagliate che disciplinino la richiesta e il rilascio dell'autorizzazione summenzionata, le attività di controllo ad esse relative, nonché le finalità – sempre

Or dunque, mentre la Proposta vieta *in toto* quei sistemi di IA che sono suscettibili di causare pregiudizi fisici o psicologici alla persona, manipolandone il comportamento (ipotesi *sub* a e *sub* b) e quei sistemi di IA che implicano il c.d. *social scoring* da parte delle autorità pubbliche o per loro conto da cui deriverebbe un trattamento pregiudizievole o sfavorevole per la persona (ipotesi *sub* c), l'uso dei sistemi di identificazione biometrica "in tempo reale" in spazi aperti al pubblico per finalità di *law enforcement* – quantunque vietato in linea generale – è ammesso sussistendo tutte le condizioni menzionate, in quanto giustificato da prevalenti ragioni di pubblica sicurezza. In tal caso, il sistema di identificazione biometrica *de quo* è soggetto alle stesse norme dettate per i sistemi di AI qualificati "ad alto rischio"[369].

L'art. 6 della Proposta pone le regole per la classificazione dei sistemi di IA come "ad alto rischio". In particolare, prescindendo dalla sua immissione sul mercato o dalla sua messa in servizio in modo indipendente rispetto ai prodotti di cui alle lett. a) e b), un sistema di IA è considerato "ad alto rischio" qualora siano congiuntamente soddisfatte due condizioni: a) il sistema di IA, il quale è destinato ad essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un prodotto, è già disciplinato dalla normativa europea di cui all'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di IA o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione di conformità da parte di terzi in vista dell'immissione sul mercato o della messa in servizio in virtù della normativa europea di cui all'allegato II.

In aggiunta, indipendentemente che siano soddisfatte o meno le condizioni summenzionate, sono considerati "ad alto rischio" anche i sistemi di IA elencati nell'allegato III, tra i quali figurano, a titolo esemplificativo, i seguenti settori: l'identificazione e la categorizzazione biometrica delle persone fisiche (sia "in tempo reale" sia "a posteriori"); la gestione e il funzionamento delle infrastrutture critiche;

rientranti nel novero di quelle indicate nell'art. 5, par. 1, lett. d) – e gli specifici reati, in relazione ai quali le autorità competenti sono autorizzate ad utilizzare tali sistemi a fini di attività di contrasto (art. 5, par. 4).
[369] G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021.

l'occupazione, gestione dei lavoratori e l'accesso al lavoro autonomo; attività di contrasto[370]; amministrazione della giustizia e processi democratici[371].

Or dunque, in definitiva, sono considerati sistemi di IA ad alto rischio quei prodotti: i) già contenuti nella regolamentazione settoriale di cui all'Allegato II della Proposta[372] ovvero sottoposti alla valutazione di conformità da parte di terzi in vista dell'immissione sul mercato o della messa in servizio del prodotto stesso; ii) elencati nell'Allegato III della Proposta, tra i quali sono annoverate l'identificazione e la categorizzazione biometrica delle persone fisiche (sia "in tempo reale" sia "a posteriori")[373].

Difatti, i sistemi di IA *de quo,* soprattutto quando sono trattati dati riguardanti l'età, l'etnia, il sesso la disabilità, presentano un alto rischio di produrre risultati distorti, comportando conseguentemente effetti discriminatori. Alla luce di tali rischi, tutti i sistemi di identificazione biometrica remota sono qualificati come "ad alto rischio", dovendo conseguentemente essere sottoposti a requisiti specifici di registrazione e sorveglianza umana[374].

---

[370] Il n. 6 dell'Allegato III individua meticolosamente i sistemi di IA impiegati nelle attività di contrasto che devono essere qualificati come "ad alto rischio". In particolare, si riferisce ai sistema di IA destinati ad essere impiegati dalle autorità di contrasto con le seguenti finalità: a) effettuare valutazioni individuali dei rischi delle persone fisiche con lo scopo di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati; b) rilevare lo stato emotivo di una persona fisica, come ad esempio i poligrafi; c) individuare i c.d. *deep fake* menzionati all'art. 52, par. 3 della Proposta medesima; d) valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati; e) prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche ai sensi dell'art. 3, par. 4, della LED o valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi; f) la profilazione delle persone fisiche ai sensi dell'art. 3, par. 4, della LED nel corso dell'indagine, dell'accertamento e del perseguimento di reati; g) compiere l'analisi criminale riguardo alle persone fisiche. Tale elenco può essere periodicamente aggiornato dalla Commissione (art. 7 della Proposta).

[371] COMMISSIONE EUROPEA, *Allegati della Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione,* {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, 21 aprile 2021, 4-5.

[372] In questo modo si garantisce la copertura sia del mercato orizzontale che verticale dell'IA, come sottolineato in C. PALMIERI, *Intelligenza Artificiale, il nuovo quadro normativo europeo,* in *Altalex,* 17 agosto 2021.

[373] G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021. Come precisato al Considerando n. 41, la circostanza che un sistema di IA sia espressamente qualificato dalla Proposta in esame come "ad alto rischio" non implica necessariamente che sia considerato come lecito dalla normativa dell'Unione; parimenti, le disposizioni contenute nella Proposta non costituiscono un fondamento giuridico per il trattamento dei dati personali (compresi i dati biometrici). Restano, infatti, impregiudicati le norme contenute nelle Carta, il diritto derivato dell'Unione e il diritto nazionale di ciascuno Stato membro.

[374] Considerando n. 33 della Proposta.

Con la finalità di bilanciare l'alto rischio, il nucleo centrale dell'intera Proposta prevede un mosaico di regole che i sistemi di IA "ad alto rischio" devono rispettare.

Innanzitutto, la Legge sull'IA prevede una serie di condizioni che tali prodotti devono osservare precedentemente alla loro immissione sul mercato[375].

Conseguentemente, sono posti in capo a fornitori, distributori e utenti dei sistemi di IA considerati "ad alto rischio" una serie di obblighi connessi precedenti alla loro immissione sul mercato[376]. Senza pretese di esaustività, sono qui di seguito elencati i principali.

Iniziando dagli obblighi dei fornitori, condizione necessaria ai fini dell'immissione sul mercato o della messa in servizio dei sistemi "ad alto rischio" è l'istituzione, l'attuazione, il mantenimento e la documentazione di un sistema di gestione del rischio, mediante un processo continuo e sistematico, che duri per tutto il ciclo di vita del sistema di IA, che sia in grado di identificare e analizzare i rischi noti e prevedibili, stimare e valutare i rischi derivanti da un uso del *software* conforme alla finalità e i pericoli connessi ad un uso improprio, nonchè di valutare altri eventuali rischi derivanti dai dati analizzati successivamente alla immissione sul mercato e di adottare tutte le misure di gestione dei rischi in base allo stato dell'arte predisposte dalla Proposta stessa[377].

La Legge sull'IA, inoltre, obbliga i fornitori ad istituire un sistema di *governance* dei dati: i dati impiegati per l'addestramento di modelli, l'apprendimento, la convalida e la prova devono soddisfare precisi requisiti di qualità; i *set* di dati di addestramento, convalida e prova devono possedere le caratteristiche di pertinenza, rappresentatività, compiutezza e completezza. A tal proposito, la Proposta autorizza i fornitori di sistemi di IA a trattare i dati biometrici – e tutte le particolari categorie di dati di cui all'art. 9, par. 1 del Regolamento europeo e all'art. 10 della LED – qualora sia strettamente necessario ai fini del monitoraggio, rilevamento e correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, purché che siano adottate tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche[378].

[375] Capo 2 del Titolo III, artt. 8-15 della Proposta.
[376] Capo 3 del Titolo III, artt. 16-29 della Proposta.
[377] Art. 9 della Proposta.
[378] Art. 10 della Proposta.

Nel prosieguo, il legislatore europeo prevede che i fornitori dei sistemi di IA "ad alto rischio" siano tenuti ad adottare la documentazione tecnica – contenente almeno gli elementi richiesti dall'Allegato IV – in grado di dimostrare la conformità del sistema ai requisiti richiesti dalla Proposta e di consentire alle autorità di valutare tale conformità[379]. La norma individua nel dettaglio i dati che devono essere registrati nei sistemi di IA che consentano l'identificazione e la categorizzazione biometrica delle persone fisiche[380].

Inoltre, i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo tale da consentire la registrazione automatica degli eventi (c.d. *file* di *log*) idonea a garantire la tracciabilità dei risultati[381], nonché la trasparenza nelle informazioni da fornire agli utenti (in formato digitale o non digitale) in modo da consentire all'utente di impiegare in modo corretto tali prodotti[382]. Nella medesima ottica, è previsto che siano fornite all'utente tutta una serie di informazioni, che rispondono, tra gli altri, allo scopo di consentire all'utente di procedere alla valutazione d'impatto sulla protezione dei dati in virtù dell'art. 35 del GDPR[383]. In particolare, i fornitori devono assicurare un adeguato livello di robustezza, accuratezza e cibersicurezza durante l'intero arco di vita del sistema, nonché capacità di resilienza in merito a errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui opera[384].

Oltre a ciò, i fornitori – prosegue la Proposta – devono garantire la supervisione umana da parte di persone fisiche durante il ciclo di vita del sistema di IA, in modo da prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che si potrebbero verificare sia in caso di uso adeguato sia in caso di uso improprio del prodotto[385]. A tale scopo, avendo riguardo ai sistemi di IA che consentono l'identificazione e la categorizzazione biometrica delle persone fisiche, i fornitori devono garantire che l'utente non compia azioni o adotti decisioni basandosi esclusivamente sull'identificazione operata dal sistema, salvo il caso in cui l'azione o la decisione sia

[379] Art. 11 della Proposta.
[380] I dati che devono essere registrati nei sistemi di IA che consentano l'identificazione e la categorizzazione biometrica delle persone fisiche sono i seguenti: a) la registrazione del periodo in cui il sistema è stato utilizzato (data e ora di inizio e di fine di ogni utilizzo); b) la banca dati utilizzata per verificare i dati di *input*; c) i dati di *input* con riferimento ai quali la ricerca ha dato esito positivo; d) l'identificativo delle persone fisiche che hanno verificato la situazione di cui all'art. 14, par. 5.
[381] Art. 12 della Proposta.
[382] Art. 13 della Proposta.
[383] Si veda, *amplius*, il paragrafo §2.1.6, che tratta in modo approfondito il principio di *accountability,* per garantire il quale il titolare del trattamento è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati (c.d. *Data Protection Impact Assessment* o DPIA), ricorrendo determinate condizioni enucleate nell'art. 35 del GDPR.
[384] Art. 15 della Proposta.
[385] Art. 14 della Proposta.

verificata da almeno due persone fisiche[386], i cui dati identificativi devono essere registrati e conservati nel sistema[387].

Oltre agli obblighi summenzionati, i fornitori devono predisporre un sistema di gestione della qualità, proporzionato alle dimensioni dell'impresa, rispondendo a determinati requisiti in dettaglio individuati[388], nonché a svolgere la procedura di valutazione della conformità di cui all'art. 43 della Proposta, da svolgersi in un momento anteriore alla sua immissione sul mercato o alla sua messa in servizio.

La Proposta, difatti, predispone un sistema *standard* di valutazione della conformità, di certificazione e registrazione del sistema di IA ad alto rischio, che sia in grado di verificare e certificare l'adozione delle condizioni previste dalla normativa *de qua* e degli obblighi gravanti in capo ai fornitori[389].

In caso di esito positivo della procedura, i fornitori hanno l'onere di redigere una dichiarazione di conformità UE e di apporre la marcatura CE di conformità[390]. In una logica di cooperazione, i fornitori devono – su richiesta delle autorità nazionali competenti designate o istituite da ciascuno Stato membro[391] – rendersi disponibili a dimostrare la conformità del sistema di IA ad alto rischio ai requisiti richiesti dalla normativa in esame[392]. Viceversa, in caso di esito negativo della procedura di conformità, e in particolare nel caso in cui il sistema di IA presenti il rischio di produrre un incidente grave o un malfunzionamento che integri una violazione dei diritti fondamentali dell'Unione[393], il fornitore deve informare immediatamente le autorità nazionali competenti dello Stato membro in cui ha messo a disposizione il prodotto ed eventualmente l'organismo notificato che ha rilasciato un certificato di conformità per il sistema di IA[394].

Inoltre, qualora vi sia motivo di ritenere che un sistema di IA "ad alto rischio" immesso sul mercato o messo in servizio non sia conforme alla normativa in esame, grava

[386] Art. 14, par. 5 della Proposta.
[387] Art. 12, par. 4 della Proposta.
[388] Art. 17 della Proposta.
[389] Capo 5 del Titolo III, artt. 40-51 della Proposta.
[390] Art. 19 della Proposta, il quale rinvia agli artt. 48 e 49 per ciò che concerne, rispettivamente, la dichiarazione di conformità UE e la marcatura CE di conformità.
[391] Artt. 30 ss. della Proposta.
[392] Art. 48 della Proposta.
[393] Art. 62 della Proposta.
[394] Art. 22 della Proposta.

sul fornitore l'obbligo di adottare tutte le necessarie misure correttive ovvero ritirare o richiamare il prodotto, a seconda della gravità del caso.

Dopo aver enucleato gli obblighi gravanti sugli importatori[395] e sui distributori[396], il *draft* di Regolamento enuclea obblighi specifici in capo agli utenti dei sistemi di IA. In particolare, salvi gli ulteriori obblighi previsti dal diritto dell'Unione o degli Stati membri e la discrezionalità dell'utente nell'organizzazione della propria attività, gli utenti di sistemi di IA sono tenuti a usare tali prodotti e a monitorare il loro funzionamento conformemente alle istruzioni per l'uso predisposte dal fornitore, garantendo che i dati di *input* siano pertinenti alla finalità per cui è stato concepito il sistema di IA[397]. Sempre in una logica di cooperazione, qualora l'utente ritenga che l'uso del sistema conforme alle istruzioni sia in grado di produrre un incidente grave o un malfunzionamento che integri una violazione dei diritti fondamentali dell'Unione[398], deve informarne il fornitore o il distributore, sospendendone l'uso[399].

Sono, infine, dettate per tutti i sistemi di IA – e, dunque, anche per i sistemi di IA "ad alto rischio" – specifiche norme relative al monitoraggio dei prodotti medesimi da effettuarsi successivamente all'immissione sul mercato o messa in servizio[400].

Tornando alla classificazione dei sistemi di IA operata dalla Legge sull'IA, l'art. 52 si occupa dei sistemi di IA considerati a rischio limitato, con riferimento ai quali la Proposta si limita a stabilire specifici obblighi di trasparenza.

Innanzitutto, è previsto che i sistemi di IA destinati a interagire con le persone fisiche – ad eccezione di quelli il cui uso sia autorizzato dalla legge ai fini di attività di prevenzione e contrasto dei reati – devono essere progettati e sviluppati in modo tale che le persone fisiche siano informate della circostanza che stanno interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo[401].

Simile obbligo di trasparenza è previsto dalla norma con riferimento ai sistemi di riconoscimento delle emozioni e ai sistemi di categorizzazione biometrica, che rientrano maggiormente nel nostro ambito di interesse: in questo caso, le persone fisiche devono

[395] Art. 26 della Proposta.
[396] Art. 27 della Proposta.
[397] Art. 29 della Proposta.
[398] Art. 62 della Proposta.
[399] Art. 29 della Proposta.
[400] Titolo VIII della Proposta. Si veda, *amplius,* nota n. 86.
[401] Art. 52, par. 1 della Proposta.

essere informate della circostanza che sono esposte a un sistema di riconoscimento delle emozioni o di categorizzazione biometrica e del funzionamento del sistema, a meno che tali sistemi siano autorizzati dalla legge ad essere utilizzati ai fini di attività di prevenzione e contrasto dei reati[402].

Similmente, con riferimento ai c.d. *deep fake,* vale a dire quei sistemi di IA che generano o manipolano immagini o contenuti audio o video in modo tale che assomiglino notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona, , i fornitori sono tenuti a rendere noto agli utenti che il contenuto è stato generato o manipolato artificialmente, salvo il caso in cui il loro uso sia autorizzato dalla legge ai fini di attività di prevenzione e contrasto dei reati[403].

La norma precisa che restano impregiudicate le norme previste nel Titolo III della Proposta. Ciò implica che i sistemi di IA impiegati per la categorizzazione biometrica delle persone fisiche devono comunque rispettare le norme dettate dalla Proposta sui sistemi di IA considerati "ad alto rischio" di cui agli artt. 8-51.

Infine, quantunque non espressamente menzionati, dall'architettura della Proposta si può dedurre che residui un'ultima categoria di sistemi di IA, cioè quelli che presentano un rischio minimo per le libertà e i diritti fondamentali: è consentito il libero utilizzo di tali prodotti, giustificato proprio in virtù della circostanza che presentano un rischio minimo o nullo per i diritti o la sicurezza dei cittadini (si pensi ai videogiochi che sfruttano componenti di IA)[404].

Come accennato, la Legge sull'IA prevede per tutti i sistemi di IA regole sul monitoraggio successivo all'immissione sul mercato o messa in servizio[405]: in particolare, i fornitori sono tenuti ad istituire e documentare un sistema di monitoraggio successivo, proporzionato alla natura e ai rischi della tecnologia fornita, il quale raccolga, documenti e analizzi per l'intero ciclo di vita del sistema di IA i dati pertinenti forniti dagli utenti[406].

[402] Art. 52, par. 2 della Proposta.
[403] Art. 52, par. 3 della Proposta.
[404] G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021.
[405] Titolo VIII della Proposta.
[406] Art. 61, par. 1 e 2 della Proposta.

Tale sistema di monitoraggio si fonda su un piano di monitoraggio successivo all'immissione sul mercato[407].

A livello di *governance,* è previsto che l'applicazione della normativa in esame sia affidata ad un Comitato europeo per l'Intelligenza Artificiale (*European Artificial Intelligence Board*)[408], composto dalle autorità nazionali di controllo designate dagli Stati membri e dal Garante europeo per la protezione dei dati[409]. In particolare, ciascuno Stato membro è tenuto a istituire o designare tra le autorità nazionali competenti le autorità nazionali di controllo al fine di garantire l'applicazione e l'attuazione del (futuro) Regolamento[410].

### 2.2.3. *(Segue):* I rilievi critici formulati dall'EDPB e EDPS e dal Garante per la protezione dei dati personali

Si comprende bene come il vasto perimetro applicativo dell'IA, il suo dinamismo e la sua multidisciplinarietà rendono difficile rintracciare un equilibrio tra tutti gli elementi e gli interessi che vengono di volta in volta in considerazione[411]. In siffatto contesto, non stupisce che l'iniziativa legislativa abbia prestato il fianco a inevitabili rilievi critici, formulati tanto in un Parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo per la protezione dei dati[412] quanto dal Garante della *privacy* italiano[413].

In linea generale, il Garante della *privacy,* seppure con qualche riserva, valuta positivamente la scelta della Commissione europea in favore della regolazione del settore dell'Intelligenza Artificiale e, *a fortiori*, in favore della fonte regolamentare, che si

[407] Art. 61, par. 3 della Proposta.
[408] Art. 56 della Proposta.
[409] Art. 57 della Proposta.
[410] Art. 59 della Proposta.
[411] G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021.
[412] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021.
[413] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187); GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di Regolamento (UE) sull'Intelligenza Artificiale, Camera dei Deputati – Commissioni IX e X riunite,* 9 marzo 2022 (doc. web. 9751565).

conferma ancora una volta la fonte normativa prediletta nella costruzione della disciplina europea del digitale: la Proposta costituisce, infatti, un ulteriore tassello nella realizzazione di quell'aspirazione della politica europea a presentarsi come un unico continente ("*one continent one law*"), su cui l'Unione investe la propria identità[414].

Il Garante italiano, anzitutto, sottolinea la profonda interrelazione tra Intelligenza Artificiale e protezione dei dati personali: il punto di intersezione tra le due normative risiede nella circostanza, certamente non marginale, che la grande quantità di dati personali trattati è funzionale ad alimentare i sistemi di IA, soprattutto nei sistemi di *machine learning* o di apprendimento automatico. Ciò implica che eventuali anomalie, errori o scorrettezze nel trattamento dei dati personali che saranno utilizzati in vista dell'apprendimento automatico del *software* si riverbereranno sul processo algoritmico. Difatti, come precedentemente accennato, la Proposta si fonda, oltre che sull'art. 114 TFUE, anche sull'art. 16 TFUE – la stessa base giuridica su cui si fonda il GDPR – nella misura in cui la protezione dei dati personali costituisce una delle componenti essenziali dell'IA. Non a caso, il Regolamento europeo sulla protezione dei dati personali continuerà a disciplinare il nucleo dell'IA, vale a dire il trattamento dei dati personali funzionale ai processi decisionali automatizzati[415].

Invero, l'approccio seguito dalla Commissione nel *draft* di Regolamento riecheggia quello già sperimentato in materia di protezione dei dati personali, condividendo le due normative «un patrimonio cromosomico comune», sotteso «all'esigenza che l'Intelligenza Artificiale sia antropocentrica e che i diritti fondamentali […] rappresentino uno steccato chiamato a orientare la corsa del progresso tecnologico»[416].

Non a caso, molti degli strumenti di regolazione adottati dalla Legge sull'IA – i quali sono valutati nel complesso in modo positivo dal Garante italiano – sono mutuati dalla

---

[414] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di Regolamento (UE) sull'Intelligenza Artificiale, Camera dei Deputati – Commissioni IX e X riunite,* 9 marzo 2022 (doc. web. 9751565).

[415] *Ibidem*. Sotto tale profilo, il Garante *privacy* rileva che già il Regolamento sulla protezione dei dati contiene, già all'art. 22, una disciplina sui processi decisionali automatizzati relativo alle persone fisiche – aspetto fondamentale dell'IA – sancendo che la persona fisica ha diritto di non essere sottoposta ad una decisione basata unicamente sul trattamento automatizzato, nonché il diritto di ottenere la revisione umana, di esprimere la propria opinione e di contestare la decisione del *software.* Similmente dispone l'art. 11 della LED, proprio allo scopo di contrastare il rischio di discriminazioni, fondate sulle caratteristiche fisiche (prima tra tutte l'etnia) in un settore delicato quale quello relativo alla giustizia penale e polizia.

[416] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187).

normativa sulla *privacy:* utilizzando un metodo induttivo, si passa dal governo dei "soli" dati personali al governo degli algoritmi[417].

Ci si riferisce, in particolare, all'approccio fondato sul rischio (ripartito secondo una «piramide di gravità ascendente»), che costituisce la cornice strutturale su cui si fonda l'intera Proposta; alla valutazione di impatto; agli obblighi di trasparenza (sebbene in merito sia il Garante italiano sia il Parare congiunto formulato da EDPB e EDPS abbiano richiesto qualche miglioria, come vedremo); al sistema delle certificazioni e dei codici di condotta, chiamati a svolgere una funzione di *co-regulation*; alla comunicazione obbligatoria in caso di incidente grave o malfunzionamento che integri una violazione dei diritti fondamentali dell'Unione; al meccanismo di regolazione secondaria affidata ad autorità amministrative indipendenti; il coordinamento tra le autorità nazionali che partecipano al Comitato europeo per l'IA (nonostante, in merito alla *governance,* siano stata formulata più di una riserva sia da parte del Garante italiano sia parte dell'EDPB e EDPS); alla tassonomia dei divieti, che riecheggia i parametri previsti dalla normativa sulla protezione dei dati personali e che positivizza gli orientamenti consolidati delle Autorità di protezione di dati (nonostante qualche perplessità, come vedremo nel proseguo)[418].

Parimenti, nel Parere congiunto n. 5/2021, l'EDPB e l'EDPS valutano positivamente la scelta della Commissione europea, ritenendo che un Regolamento di tal genere costituisca un baluardo necessario a favore dei diritti fondamentali dei cittadini dell'Unione, nonostante rilevino che – alla luce della complessità della materia – la Proposta presenti soluzioni perfettibili sotto diversi punti di vista, per garantire efficienza e maggiore coordinamento con il GDPR[419].

Va innanzitutto rilevato che nel Parere congiunto, l'EDPB e l'EDPS ricordano che i sistemi di IA comportano il trattamento dei dati personali. Pertanto, riveste fondamentale importanza chiarire il rapporto con il quadro giuridico vigente in materia di protezione dei dati personali, in modo da evitare qualsiasi incongruenza con il GDPR e con la LED,

---

[417] *Ibidem*.

[418] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di Regolamento (UE) sull'Intelligenza Artificiale, Camera dei Deputati – Commissioni IX e X riunite,* 9 marzo 2022 (doc. web. 9751565).

[419] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 25.

non solo per garantire certezza del diritto, ma anche per evitare di pregiudicare il diritto fondamentale alla protezione dei dati personali[420].

A tal proposito, l'EDPB e l'EDPS raccomandano con forza di precisare, già all'art. 1 della Proposta, che la legislazione europea in materia di protezione dei dati personali[421] si applica in tutti i casi in cui i sistemi di IA che rientrano nel perimetro applicativo della Proposta trattino dati personali; parimenti, dovrebbe essere precisato che la Proposta non pregiudica l'applicazione della disciplina in materia *privacy,* compresi i poteri attribuiti alle autorità di controllo indipendenti.

Inoltre, se per un verso va valutata positivamente l'introduzione di specifici obblighi di trasparenza, per altro verso qualche perplessità suscitano le lacune in merito alla c.d. trasparenza degli algoritmi[422]. Difatti, considerato che l'apprendimento automatico può ingenerare distorsioni ed errori, il sistema di IA dovrebbe essere idoneo a garantire la protezione dei dati personali sin dalla sua progettazione; dovrebbe essere precisato, poi, che l'utente ha la possibilità di avvalersi dei diritti di cui all'art. 22 del GDPR sul processo decisionale automatizzato, compresa la profilazione (in particolare, il diritto all'intervento umano), nonché il diritto di chiedere la cancellazione e la rettifica dei propri dati personali, indipendentemente dalla classificazione del sistema di IA; l'utente, inoltre, dovrebbe essere sempre informato che il *software* utilizzerà in futuro i propri dati a fini di "allenamento", oltre che ha il diritto di ricevere una spiegazione generale della procedura e dell'ambito applicativo del sistema di IA. Infine, con riferimento ai sistemi di IA usati per finalità di *law enforcement* – in merito ai quali allo stato attuale non sono previsti obblighi di trasparenza – bisognerebbe operare una distinzione: per i sistemi di IA usati a fini di accertamento e di prevenzione dovrebbero essere previsti obblighi di trasparenza, in virtù della presunzione di innocenza, laddove i sistemi finalizzati all'indagine e al perseguimento di reati possano prevedere minori tutele, in virtù della loro finalità[423]. In tale quadro, il Garante italiano fa un passo in avanti. Egli rileva, infatti, che le disposizioni contenute nella Legge sull'IA adottano l'approccio – ormai superato

[420] *Ivi,* 9 e 19.
[421] Ci si riferisce, in particolare al GDPR, all'EUDPR, alla Direttiva 2002/58/CE (c.d. Direttiva *privacy*) e alla LED.
[422] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187).
[423] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 19-20 e 22.

– tipico della disciplina *privacy* e, prima ancora, della disciplina consumeristica: imporre al fornitore (la parte "forte" del rapporto) specifici obblighi di trasparenza; tuttavia, nella "società dell'accetta e continua", è difficile credere davvero che l'utente legga le chilometriche condizioni di contratto e informative *privacy.* Di conseguenza, bisognerebbe ripensare un metodo nuovo, passando da una dimensione formale a una logica di sostanziale consapevolezza dell'utente[424].

L'approccio sul rischio adottato dalla Proposta – accolto con particolare favore sia dal Garante italiano[425] che dall'EDPB e EDPS[426] – non esclude, peraltro, alcune soluzioni perfettibili, che si auspica possano essere accolte prima che la normativa entri in vigore.

Innanzitutto, la scelta di fornire un elenco esaustivo, per quanto modificabile e aggiornabile ad opera della Commissione, di sistemi di IA qualificati "ad alto rischio" – tra i quali sono annoverati l'identificazione e la categorizzazione biometrica delle persone fisiche sia "in tempo reale" sia "a posteriori" – cela il rischio di produrre «effetti polarizzanti», ostacolando un'introduzione più rapida di ulteriori prodotti rischiosi. Inoltre, l'elenco contenuto negli Allegati II e III della Proposta non fa riferimento ad alcuni sistemi di IA comunque invasivi e rischiosi, quali i sistemi di IA che calcolano i premi assicurativi ovvero che valutano i trattamenti medici o la ricerca in campo medico[427]. Detto in altri termini, la scelta di introdurre un elenco compiuto di applicazioni "ad alto rischio" – che pure costituisce l'architrave della struttura della Legge sull'IA – appare troppo ambiziosa e per certi versi ingenua, specie in un contesto tecnologico e di mercato, quale quello dell'Intelligenza Artificiale, in vertiginoso sviluppo. Si potrebbe allora pensare – consiglia il Garante italiano – di estendere ai *software de quibus* il sistema relativo alla valutazione d'impatto (e, ritengo, quello relativo alla consultazione preventiva), mutuato dalla disciplina *privacy*, prevedendo che il fornitore debba effettuare una valutazione circa l'impatto sortito da tali trattamenti sulla protezione dei dati personali; qualora, all'esito della valutazione, il fornitore non sia in grado di adottare

[424] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187).
[425] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di Regolamento (UE) sull'Intelligenza Artificiale, Camera dei Deputati – Commissioni IX e X riunite,* 9 marzo 2022 ( doc. web. 9751565).
[426] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 9 ss.
[427] *Ibidem*.

misure idonee ad attenuare il rischio «fino ad una soglia di sostenibilità sociale e democratica», egli dovrebbe essere tenuto a consultare la competente autorità di regolamentazione e vigilanza, la quale potrebbe fornire indicazioni su come gestire il rischio e, solo eventualmente, inibire la prosecuzione dell'attività[428].

Nel Parere reso congiuntamente, poi, l'EDPB e l'EDPS – quantunque valutino positivamente la precisazione, fatta propria dalla Legge sull'IA, secondo la quale la classificazione di un certo sistema come sistema di IA "ad alto rischio" non comporta la presunzione circa la sua liceità – raccomandano di inserire, tra i prerequisiti essenziali ai fini della dichiarazione di conformità UE e della marcatura CE di conformità, l'obbligo di assolvere puntualmente a tutti obblighi enucleati dalla disciplina europea in materia di protezione dei dati personali[429].

È oggetto di pesanti critiche, invece, l'art. 5 della Proposta, per una molteplicità di ragioni.

Anzitutto, i criteri richiesti dall'art. 5 restringono oltremodo la portata del divieto in esso contenuto: difatti, le lett. a) e b) dell'art. 5, par. 1 richiedono che il sistema di IA (che utilizza tecniche subliminali ovvero che sfrutta le vulnerabilità di uno specifico gruppo di persone) provochi l'effetto di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare alla persona o a

---

[428] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187). Nondimeno, in COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 10-11, sono avanzati dubbi anche in merito all'efficacia della valutazione d'impatto: la Proposta, infatti, richiede che la valutazione del rischio sia esperita dal *fornitore* di un sistema di IA "ad alto rischio", seppure nella maggior parte dei casi la qualifica di "titolare del trattamento" sia rivestita poi in concreto dall'*utente* del sistema di IA, che pure non è destinatario dell'obbligo: ad esempio, un utente di un sistema di riconoscimento facciale è titolare del trattamento ai sensi del GDPR, ma non è tenuto a rispettare i gravosi obblighi previsti dalla Legge sull'IA. Di conseguenza, rilevano l'EDPB e l'EDPS nel Parere congiunto, la valutazione d'impatto cui è tenuto il fornitore (più generale) non esclude, anzi richiede, una valutazione d'impatto sulla protezione dei dati più granulare (art. 35 del GDPR), che dovrebbe essere esperita dall'utente-titolare del trattamento. Per contro, la circostanza che un sistema sia qualificato "ad alto rischio" dalla Legge sull'IA comporta la presunzione (relativa) che i dati personali trattati dal medesimo presentano un rischio elevato. Alla luce di tali considerazioni, le Autorità raccomandano di specificare nella Proposta, soprattutto con riferimento ai dati biometrici, la necessità della doppia valutazione d'impatto cui sono sottoposti i sistemi di IA "ad alto rischio", tenendo conto vuoi del caso d'uso vuoi del contesto specifico cui è destinato ad operare il sistema. Inoltre, si osserva che sarebbe opportuno prevedere che la valutazione di conformità all'art. 43 sia operata *ex ante* da terzi, affinché sia garantita indipendenza di valutazione.

[429] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 11.

terzi un danno fisico o psicologico. Parimenti, restringono la portata del divieto i limiti previsti dalla lett. c), che vietano la pratica di IA solamente qualora impiegata «per un determinato periodo di tempo» da parte di autorità pubbliche o per loro conto e a condizione che il punteggio sociale comporti il verificarsi di uno o di entrambi gli scenari previsti, con una formulazione peraltro vaga, ai punti i) e ii). Per quanto concerne, in particolare, quest'ultimo divieto, le Autorità ritengono che la Proposta dovrebbe vietare qualsiasi pratica di *social scoring,* senza limitazioni di sorta, sia nel caso in cui sia impiegata da autorità pubbliche sia che sia impiegata da imprese private[430].

Quanto all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di *law enforcement,* è stato richiesto un trattamento più severo: i gravi rischi di intrusione nella vita privata delle persone che tali pratiche paventano potrebbero comportare la frustrazione (del tutto ragionevole) dell'aspettativa dei cittadini di restare anonimi negli spazi accessibili al pubblico; di conseguenza, sarebbero (potenzialmente) limitati diritti e libertà fondamentali, quali la libertà di espressione, di riunione e di associazione e, in generale, diritti che informano la nostra democrazia. Similmente, le eccezioni al divieto di cui all'art. 5, par. 1, lett. d) non sono esenti da vizi: innanzitutto, non è chiaro cosa si debba intendere per "ritardi significativi", con pesanti ricadute circa la definizione dei sistemi *de quo*; inoltre, quantunque tali pratiche siano impiegate per uno degli obiettivi elencati – la cui formulazione è in ogni caso vaga – si omette di considerare che essi richiedono il trattamento di dati di un numero indiscriminato di interessati al fine di identificare poche persone sospette. Alla luce di tali considerazioni, nel Parere congiunto, l'EDPB e l'EDPS richiedono di introdurre all'art. 5 un divieto generale di utilizzo dei sistemi di IA impiegati a fini di riconoscimento automatico delle caratteristiche umane (prime fra tutte il volto) in spazi accessibili al pubblico, compresi, per coerenza, i sistemi *de quo* impiegati in spazi *online*[431].

Oltre a tale divieto riguardante i sistemi di identificazione biometrica remota "in tempo reale", l'EDPB e l'EDPS raccomandano di vietare: a) i sistemi di IA finalizzati alla «categorizzazione biometrica», vale a dire i sistemi di IA che, trattando dati

[430] Si pensi ai *social media* ovvero ai fornitori di *cloud,* che trattano notevoli quantità di dati personali. Si veda COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 12-13.
[431] *Ibidem.*

biometrici (come ad esempio il volto), categorizzano le persone in insiemi (*clusters*), in base all'etnia, al genere, all'orientamento politico o sessuale ovvero altri motivi di discriminazione vietati dalla CDFUE, quando impiegati sia da autorità pubbliche che da società private (allo stato attuale, qualificati come sistemi di IA "ad alto rischio")[432]; b) i sistemi di IA che violano i principi fondanti dell'Unione (come ad esempio i poligrafi, oggi qualificati come sistemi di IA "ad alto rischio"); c) i sistemi di IA impiegati per il riconoscimento delle emozioni (allo stato attuale, qualificati come «determinati sistemi di IA» dall'art. 52 della Proposta), sia pur prevedendo delle eccezioni[433].

Quanto alla *governance,* sia il Garante italiano che l'EDPB e EDPS valutano complessivamente come positiva l'istituzione di un Comitato europeo per l'Intelligenza Artificiale (CEIA), così come la designazione dell'EDPS quale autorità competente e autorità di vigilanza del mercato. D'altro canto, senza pretesa di esaustività sulla questione, che ha particolarmente interessato le Autorità, il Titolo VI ha attratto numerosi rilievi critici[434]. In particolare, costituisce un nodo cruciale il ruolo da attribuire alle Autorità nazionali di protezione dei dati (tra cui il Garante *privacy* italiano): anziché lasciare agli Stati membri la libertà di istituire o designare le Autorità nazionali competenti, che agiscano quali autorità nazionali di controllo[435] – considerando la sinergia tra la disciplina sull'IA e sulla protezione dei dati personali e le competenze trasversali e le caratteristiche di indipendenza già acquisite dalle Autorità in parola – si propone che le stesse Autorità per la protezione dei dati siano designate quali autorità nazionali di controllo direttamente ai sensi dell'art. 59 della Proposta. Da tale soluzione deriverebbero due ordini di vantaggi: sarebbe anzitutto assicurata un'interpretazione coerente e uniforme, nonché «un'applicazione lungimirante» delle due discipline nei diversi Stati membri; ne deriverebbe, inoltre, una notevole semplificazione per gli utenti,

[432] Si ritiene che essi violino la dignità umana.
[433] Si pensi, ad esempio, al riconoscimento delle emozioni per finalità sanitarie o di ricerca – quali pazienti per cui la deduzione delle emozioni è rilevante – sempre prevedendo accurate garanzie. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 13.
[434] In particolare, in COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio* cit., 16-18, si rileva che Il ruolo e le funzioni dell'EDPS dovrebbero essere maggiormente precisati; dovrebbero essere garantiti maggiori poteri e maggiore autonomia al CEIA, con conseguente ridimensionamento del ruolo attribuito alla Commissione; risultano particolarmente confusionarie molte disposizioni relative ai compiti ai poteri assegnati alle varie autorità competenti, nonché i rapporti reciproci e la loro natura; dovrebbe essere specificato che le autorità di controllo sono completamente indipendenti.
[435] Art. 59 della Proposta.

che dovrebbero rivolgersi ad un'unica Autorità peri i sistemi di IA che trattino dati personali, in un'ottica di notevole semplificazione degli oneri amministrativi e finanziari riguardanti l'applicazione del (futuro) Regolamento[436].

Non rimane esente da critiche neppure la definizione di IA fornita dalla Commissione: come rilevato dal Garante *privacy,* la definizione formulata nella Proposta è «inevitabilmente ampia, generica, sfuggente», né tantomeno l'elenco delle tecniche e degli approcci riescono a restringerne in modo significativo l'ambito di applicazione. Tale rilievo rende il *draft* di Regolamento ancora più centrale e ambizioso, in quanto la maggioranza di applicazioni e dispositivi tecnologici oggi esistenti rientrerà nel suo ambito di applicazione[437].

Ulteriori rilievi critici, seppure non centrali ai fini della presente trattazione, riguardano l'ambito territoriale di applicazione della Proposta, i meccanismi di conformità, tra cui la certificazione[438] e i codici di condotta, nonché lo spazio di sperimentazione e innovazione[439].

### 2.2.4. *(Segue):* Aggiornamento: approvati gli emendamenti alla Proposta di Regolamento (ove finalmente compare il riconoscimento facciale)

Recentemente, l'11 maggio 2023, sono stati approvati da parte di due delle principali Commissioni parlamentari europee – Commissione IMCO[440] e Commissione LIBE[441] – numerosi emendamenti al *draft* di Regolamento (UE) sull'Intelligenza Artificiale. Ne risulta che – accogliendo una parte dei rilievi critici formulati dall'EDPB

[436] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio* cit., 17; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali* cit.
[437] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187).
[438] Per ciò che concerne il sistema di certificazione, nel *draft* di Regolamento non si rinviene un efficace collegamento con la disciplina europea in materia di protezione dei dati personali e con altre discipline europee richiamate nell'Allegato III; inoltre, l'EDPB e l'EDPS raccomandano di includere nella Proposta l'obbligo per i fornitori di rispettare i principi di minimizzazione dei dati e della *privacy by design,* quali requisiti essenziali ai fini della marcatura CE e, dunque, ai fini dell'immissione sul mercato europeo.
[439] Si veda, in particolare, COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021, 5-8; 20-24.
[440] Commissione per il mercato interno e la protezione dei consumatori
[441] Commissione per le libertà civili, la giustizia e gli affari interni

e EDPS e dagli *AI moralist* più ferventi – l'*AI Act,* la cui prima stesura risale all'Aprile 2021, è stato sostanzialmente modificato in un'ottica restrittiva[442]. In ogni caso, bisognerà attendere il 12-15 giugno 2023 per il voto in plenaria[443].

Per ciò che qui maggiormente interessa, è opportuno segnalare che – mantenuti immutati l'approccio normativo proporzionato basato sul rischio e lo schema piramidale originario fondato sulla distinzione tra rischio inaccettabile, alto rischio, rischio limitato e rischio minimo – numerose sono le modifiche riguardanti la biometria e il riconoscimento facciale[444].

Innanzitutto, all'art. 5 della Proposta è stato aggiunto il divieto di immissione sul mercato, messa in servizio o uso dei sistemi di categorizzazione biometrica che classificano le persone in base a caratteristiche sensibili o protette o in base alla deduzione di tali caratteristiche, salvi i casi in cui i sistemi siano utilizzati per scopi terapeutici a cui è stato prestato specifico consenso informato[445]. Dunque, mentre nella precedente bozza di Regolamento tali tecnologie erano qualificate, all'art. 52, come "determinati sistemi di IA" semplicemente sottoposti a obblighi di trasparenza ovvero tra le applicazioni di cui all'Allegato III, sottoposte alle medesime regole dettate per i sistemi di AI "ad alto rischio", oggi tali applicazioni sono vietate (salvi gli scopi terapeutici).

In secondo luogo, è stato finalmente aggiunto il divieto di immissione sul mercato, messa in servizio o uso di sistemi di Intelligenza Artificiale che creano o implementano *database* fondati sul riconoscimento facciale tramite il c.d. *data scraping*[446] non mirato di immagini da Internet o da telecamere a circuito chiuso[447]. Dunque, il riconoscimento

---

[442] S. SALMERI, L. LUCANI, *AI Act: approvati gli emendamenti del Parlamento europeo alla Proposta di Regolamento,* in *Studio Previti Associazione Professionale,* 17 maggio 2023, consultabile su https://www.previti.it/ai-act-approvati-gli-emendamenti-del-parlamento-europeo-alla-proposta-di-regolamento.

[443] F. META, *Artificial Intelligence Act, accordo politico al Parlamento Ue sulle nuove norme,* in *Network Digital 360,* 28 aprile 2023, consultabile su https://www.corrierecomunicazioni.it/digital-economy/artificial-intelligence-act-accordo-politico-al-parlamento-ue-sulle-nuove-norme/.

[444] Si invita a prendere visione delle modifiche alla Proposta al seguente link: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf.

[445] Art. 5, par. 1, lett. ba).

[446] Come già accennato, in questo Capitolo, al paragrafo §2.1.5., per *data scraping* si intende il processo automatizzato di estrazione di dati e informazioni dall'*output* generato da un altro *software;* spesso il c.d. *web scraping* consiste nel prelevare, tramite processi automatizzati, dati da *Internet,* classificarli in base a determinati requisiti, dividerli per categorie e inserirli all'interno di un *database:* si veda, per tutti, TAG TALENT GARDEN, *Cos'è il Data Scraping e quali sono le sue applicazioni per l'Analisi Dati,* in *Tag Talent Garden,* 4 maggio 2022, consultabile su https://talentgarden.org/it/data/web-scraping-cosa-applicazioni/.

[447] Art. 5, par. 1, lett. db).

facciale è stato finalmente riconosciuto tra le tecnologie che maggiormente comportano notevoli rischi per le libertà e i diritti fondamentali dei cittadini degli Stati membri.

Sono parimenti vietati l'immissione sul mercato, la messa in servizio o l'uso di sistemi di deduzione delle emozioni degli individui per finalità di *law enforcement,* di gestione delle frontiere, negli ambienti lavorativi e negli istituti di istruzione[448] (qualificati, nel *draft* di Regolamento dell'Aprile 2021, all'art. 52, come "determinati sistemi di IA" sottoposti soltanto a obblighi informativi).

Sono altresì vietati *tout cour* l'immissione sul mercato, la messa in servizio o l'uso dei sistemi di identificazione biometrica in *real time* in spazi aperti al pubblico, senza limitazioni di sorta[449]. Dunque, mentre nella precedente bozza i sistemi *de quibus,* quando impiegati per finalità di *law enforcement,* erano ammessi in presenza di una serie di condizioni[450], oggi sono integralmente vietati.

Inoltre, il Parlamento europeo ha esteso il divieto – e questa è la novità maggiormente illuminata – di immissione sul mercato, messa in servizio o uso ai sistemi di identificazione biometrica a posteriori in spazi accessibili al pubblico[451], salvo il caso in cui siano stati preventivamente autorizzati in base al diritto dell'Unione e siano «strettamente necessari» per la persecuzione di gravi e specifici reati, che siano stati già commessi[452]. Dunque, nell'attuale *draft* di Regolamento, il divieto comprende non solo i sistemi di identificazione biometrica in *real time,* ma anche quelli impiegati *ex post,* i quali possono essere utilizzati solo se preventivamente autorizzati per finalità di repressione di gravi (e determinati) reati già commessi.

Infine, sono finalmente vietati i c.d. sistemi di polizia predittiva, vale a dire quei sistemi di Intelligenza Artificiale che si dichiarano capaci di valutare, e dunque prevedere, il rischio di commissione di un reato o di recidiva o di commissione di un illecito amministrativo da parte di una persona fisica, basandosi sulla profilazione dell'individuo o sulla valutazione dei tratti e delle caratteristiche inerenti alla sua personalità[453].

---

[448] Art. 5, par. 1, lett. dc).
[449] Art. 5, par. 1, lett. d).
[450] Tali condizioni erano enucleate all'art. 5, par. 1, lett. d) e art. 5, par. 2 e 3 (precedente bozza).
[451] Sostanzialmente, l'analisi *ex post* di videoregistrazioni in spazi accessibili al pubblico.
[452] Art. 5, par. 1, lett. e).
[453] Art. 5, par. 1, lett. da). Come rilevato da F. META, *Artificial Intelligence Act, accordo politico al Parlamento Ue sulle nuove norme,* in *Network Digital 360,* 28 aprile 2023, probabilmente il Parlamento europeo si è reso conto dei gravi rischi per i diritti fondamentali sottesi ai c.d. sistemi di polizia predittiva a seguito dello scandalo olandese degli assegni familiari, a seguito del quale migliaia di famiglie olandesi sono state erroneamente accusate di frode a causa di un algoritmo.

Ebbene, sicuramente va valutata positivamente la scelta delle Commissioni parlamentari europee di inserire tra i sistemi di AI a rischio inaccettabile i sistemi biometrici (*in real time, ex post,* di categorizzazione biometrica in base a dati sensibili o protetti, il *data scraping*), nonché i sistemi di riconoscimento delle emozioni e di polizia predittiva, nella precedente bozza variamente qualificati, essendo stati accolti i rilievi critici espressi nel Parere congiunto n. 5/2021 dal Comitato europeo per la protezione dei dati e del Garante europeo per la protezione dei dati.

Ciononostante, non si può evitare di sottolineare che la sussunzione dei sistemi *de quibus* a sistemi a rischio inaccettabile appare una modifica dell'ultim'ora, forse dettata più dalla suggestione generata dal clamore attorno a ChatGPT – divenuto in poco tempo uno dei *software* di Intelligenza Artificiale più famosi al mondo – che da una reale comprensione delle dimensioni del problema.

In particolare, il Prof. Filiberto Brozzetti ha rilevato che tali integrazioni non presentano «la minima profondità di dettaglio», in quanto questo modo di legiferare sembra ridursi «ad una catalogazione sporadica ed estemporanea che potrà quindi essere integrata anche in futuro disorganicamente ed asistematicamente sulla base delle contingenze (per non dire delle mode o delle nevrosi)», finendo per risultare una modifica «velleitaria ed estetica più che etica».

Dunque, seppure pregevole l'intenzione del legislatore europeo di legiferare su una materia tanto complessa, l'idea globale che se ne ricava è che l'ordinamento giuridico europeo stia faticosamente rincorrendo le innovazioni tecnologiche e, in particolare, la biometria: come già rilevato, sembra che il legislatore europeo – nella (comprensibile) difficoltà di rintracciare quelle caratteristiche generali che sono lesive dei diritti e delle libertà dei cittadini – preferisca non porre un divieto per caratteri, suscettibile di coprire anche le future evoluzioni tecnologiche, ma procedere per elencazione, ponendo la regola della legalità e della tipicità delle applicazioni vietate. Si tratta di una scelta legislativa quantomeno discutibile, specie in un settore in rapidissimo sviluppo quale quello dell'Intelligenza Artificiale.

Venendo poi al contenuto del catalogo, seppure i sistemi di deduzione delle emozioni degli individui per finalità di *law enforcement,* di gestione delle frontiere, negli ambienti lavorativi e negli istituti di istruzione siano stati inclusi tra i sistemi di AI a rischio inaccettabile, sembra che non sia stato ancora ben compreso l'elevato rischio di intrusività nella vita quotidiana che tali sistemi presentano. Infatti, in base ad

un'interpretazione letterale della disposizione, il divieto riguarderebbe soltanto i sistemi di deduzione delle emozioni impiegati per le finalità descritte, restando così escluse le società private che usufruiscono di tali applicazioni per finalità diverse da quelle elencate. Sarebbe, pertanto, auspicabile un ulteriore aggiornamento della disposizione, in modo da vietare del tutto i sistemi in commento, quali che siano le finalità perseguite.

Ordunque, le altre modalità di utilizzo da parte di società private – diverse dalle finalità ivi elencate – sono state volutamente tenute da parte, perché considerate meno intrusive per le libertà e i diritti fondamentali dei cittadini, oppure costituiscono non ragionate vie di fuga che le società digitali private – una volta adempiuto l'obbligo di trasparenza (minimo e indispensabile) di cui all'art. 52 della Proposta (che resta impregiudicato) – potranno facilmente percorrere?

In quest'ultimo caso, allora, ci si può lecitamente domandare se la soluzione normativa adottata relativamente ai sistemi di deduzione delle emozioni, anche dopo gli emendamenti, sia sufficiente a tutelare la persona digitale nel momento in cui questa entra a contatto con sistemi capaci di rilevare le sue emozioni e di guidare i suoi comportamenti anche nel mondo *offline*: il rischio è che – una volta assolto l'obbligo informativo, spesso in un linguaggio e in una forma non facilmente comprensibili per l'utente – gli operatori economici si sentano liberi di portare a compimento il processo di profilazione degli utenti sulla base delle emozioni, di cui la persona non è pienamente consapevole[454]. Difatti, l'inconsapevolezza dell'utente è uno degli elementi da non trascurare per forgiare una soluzione normativa che sia realmente, e non solo esteriormente, *human-centric*[455].

In conclusione, la tensione insita nella dialettica tra l'esigenza di sviluppo di un settore in vertiginosa ascesa – che richiederebbe l'adozione di meccanismi giuridici flessibili che possano adattarsi dinamicamente all'evoluzione tecnologica – e la necessità di salvaguardare i valori e i diritti fondamentali dell'UE, nonché la sicurezza degli utenti – che invece richiederebbe soluzioni normative più rigide e coraggiose – sembra ancora

[454] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 532.

[455] *Ibidem.* Non a caso, a proposito dei principi generali applicabili a tutti i sistemi di Intelligenza Artificiale, è stato aggiunto alla Proposta l'art. 4a, che prescrive a tutti gli operatori che rientrano nell'ambito di applicazione del (futuro) Regolamento di sviluppare e utilizzare i sistemi di IA in modo conforme ad un approccio antropocentrico, per l'utilizzo e lo sviluppo di un'IA etica e affidabile. A tale scopo, devono essere rispettati i principi di supervisione umana (*"human agency and oversight"*), di robustezza tecnica e sicurezza (*"technical robustness and safety"*), di *privacy* e *governance dei dati* (nel senso che i sistemi di IA devono essere sviluppati e utilizzati nel rispetto delle norme vigenti in materia di protezione dei dati personali), di trasparenza (*"transparency"*), di diversità, non discriminazione ed equità (*"diversity, non-discrimination and fairness*), di benessere sociale e ambientale (*"social and environmental well-being"*).

reggersi su equilibri instabili, tuttora sbilanciati verso la necessità di fornire un vantaggio competitivo per il mercato interno europeo.

### 2.2.5. *(Segue):* La richiesta di moratoria del Parlamento europeo e il d.l. n. 139/2021, convertito con modificazioni dalla L. n. 205/2021

In tale quadro, con la Risoluzione sull'Intelligenza Artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziaria in ambito penale[456] (6 ottobre 2021), il Parlamento europeo ha invitato la Commissione a valutare l'introduzione di una moratoria sulla diffusione dei sistemi di riconoscimento facciale impiegati per finalità identificative nell'ambito delle attività di contrasto, salvo il caso in cui siano utilizzate a fini identificativi delle vittime di un reato, almeno fino a quando «le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie»[457].

Parimenti, in sede nazionale, soprattutto dopo il parere del Garante (non favorevole) sull'utilizzo del sistema S.A.R.I. *Real Time*[458], è stato presentato il decreto legge n. 139/2021 (c.d. Decreto Capienze), poi convertito con modificazioni dalla L. n. 205/2021, il quale dispone che l'installazione di impianti di videosorveglianza dotati di sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, sia quando utilizzati da autorità pubbliche che da soggetti privati, è sospesa «fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023»[459]. Ciononostante, la moratoria non riguarda i trattamenti di dati biometrici «effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione delle sanzioni penali» previste al d.lgs. n. 51/2018, a condizione che sia espresso parere favorevole da parte del Garante per la protezione dei dati personali. La moratoria non riguarda neppure i trattamenti effettuati «dall'autorità giudiziaria nell'esercizio delle

[456] PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), 6 ottobre 2021.
[457] *Ivi*, §27.
[458] Si veda, *amplius,* nel Capitolo Terzo, il paragrafo §3.2.2., reso a commento dell'intera vicenda.
[459] Art. 1, c. 9 del Decreto Capienze.

funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero», le quali peraltro non devono sottostare ad alcun controllo preventivo da parte del Garante[460].

A ben vedere, l'intervento normativo sembra porsi – forse inconsapevolmente – in antitesi rispetto alle preoccupazioni espresse, in ambito sovranazionale, dal Parlamento europeo.

Innanzitutto – mentre il Parlamento europeo ha chiesto di inibire il riconoscimento facciale impiegato a fini identificativi nell'ambito delle attività di contrasto, con la sola eccezione relativa alle TRF utilizzate a fini identificativi delle vittime di un reato – il Decreto Capienze autorizza ciascun ente pubblico che eserciti poteri a fini di prevenzione e indagine ad installare e attivare impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, a seguito del parere favorevole rilasciato dal Garante. Viene così frustrata la *ratio legis,* che era tesa proprio a inibire i sistemi *de quo* fino all'introduzione di un chiaro quadro normativo[461].

In secondo luogo, la sospensione non riguarda neppure i *software* di riconoscimento facciale impiegati dall'autorità giudiziaria e dal pubblico ministero (senza neppure la necessità di un parere favorevole da parte del Garante) – non distinguendo peraltro il testo normativo tra identificazione e categorizzazione, tra sistemi di riconoscimento facciale "in tempo reale" e "a posteriori". Ne deriva che l'autorità giudiziaria e il pubblico ministero possono utilizzare i sistemi *de quo* senza limitazioni, peraltro in assenza di una disciplina contenuta nel codice di procedura penale sul valore assunto da tali elementi di prova nel procedimento penale[462].

Ad ogni modo, la moratoria relativa all'installazione di impianti di videosorveglianza muniti di sistemi di riconoscimento facciale ha vita breve: mancano

---

[460] Art. 1, c. 12 del Decreto Capienze.

[461] Si veda, in particolare il d.d.l. A.C. 3009, *Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico,* 12 aprile 2021, consultabile in http://documenti.camera.it/leg18/dossier/pdf/AC0497.pdf?_1677679502061. Per un approfondimento sul tema si consiglia E. SACCHETTO, *Riconoscimento facciale, l'approccio italiano è in antitesi alla Ue: i nodi,* in *Network Digital 360, Agenda Digitale,* 7 dicembre 2022, consultabile in https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-lapproccio-italiano-e-in-antitesi-alla-ue-i-nodi/.

[462] E. SACCHETTO, *Riconoscimento facciale, l'approccio italiano è in antitesi alla Ue: i nodi,* in *Network Digital 360, Agenda Digitale,* 7 dicembre 2022, la quale si interroga sul sistema o istituto contenuto nel codice di procedura penale attraverso il quale gli elementi di prova, costituiti dalle videoregistrazioni che impiegano sistemi di riconoscimento facciale ottenute in luoghi pubblici o aperti al pubblico, possano trovare ingresso nel processo penale, in quanto i sistemi di riconoscimento "in tempo reale" non possono essere annoverati né tra gli accertamenti tecnici ripetibili né tra gli accertamenti tecnici irripetibili.

solo pochi mesi al 31 dicembre 2023 e non sembra che il mondo politico sia giunto ad una soluzione condivisa ed unanime.

A complicare il quadro fattuale e giuridico, sono intervenute le dichiarazioni del Ministro dell'Interno Matteo Piantedosi, il quale, a fine aprile 2023, a seguito dei deplorevoli fatti criminosi avvenuti nelle stazioni ferroviarie di Roma e Milano, ha ventilato l'ipotesi di introdurre videocamere di sorveglianza dotate di sistemi di riconoscimento facciale, presentati come la migliore tecnologia per aumentare la sicurezza urbana, soprattutto nelle aree pubbliche maggiormente sensibili, quali stazioni, ospedali e aree commerciali[463].

Nello specifico, il Ministro, in un'intervista al quotidiano *"Il Resto del Carlino"*, ha affermato che «[l]a videosorveglianza è uno strumento ormai unanimemente riconosciuto come fondamentale» nella misura in cui «dà ulteriori e significative possibilità di prevenzione e indagine». Mostrandosi, peraltro, consapevole degli elevati rischi per i diritti e le libertà fondamentali dell'uomo che tale tecnologia presenta, ha aggiunto che «[è] chiaro che il diritto alla sicurezza va bilanciato con il diritto alla *privacy*. C'è un punto di equilibrio che si può e si deve trovare». Poi, facendo riferimento alla moratoria prevista nel c.d. Decreto Capienze e alle relative eccezioni di cui all'art. 1, c. 12, ha aggiunto: «Proprio in questi giorni abbiamo avviato specifiche interlocuzioni con il Garante per trovare una soluzione condivisa»[464].

Invero, già nel gennaio 2023, il Ministro dell'Interno ha rafforzato il piano sulla sicurezza urbana, predisponendo operazioni militari e di polizia, soprattutto nelle stazioni ferroviarie di Roma, Milano e Napoli, a scopo di contrasto e repressione dei reati, mentre nel marzo 2023, lo stesso ha affidato ad una circolare la richiesta, rivolta ai Prefetti delle tre città metropolitane, di indicare altri luoghi da sottoporre a controllo[465]. L'impressione è che il Ministro Piantedosi stia guardando oltre il 31 dicembre 2023 e stia raccogliendo

[463] L. CARRER, *Riconoscimento facciale: come funziona e perché i piani del governo per introdurlo sono problematici,* in *ValigiaBlu,* 16 maggio 2023, consultabile su https://www.valigiablu.it/piantedosi-riconoscimento-facciale-luoghi-pubblici/#:~:text=A%20fine%20aprile%20Piantedosi%20ha,in%20un'intervista%20al%20quotidiano; K. CARBONI, *Il ministero dell'Interno vuole introdurre il riconoscimento facciale nei luoghi pubblici,* in *Wired,* 2 maggio 2023, consultabile su https://www.google.com/amp/s/www.wired.it/article/piantedosi-riconoscimento-facciale-stazioni-luoghi-pubblici/amp/.

[464] A. CARRUGGIA, *Il ministro Piantedosi: «Più polizia nelle stazioni»* in *Governo Italiano, Ministero dell'Interno,* consultabile su https://www.interno.gov.it/it/stampa-e-comunicazione/interventi-e-interviste/ministro-piantedosi-piu-polizia-nelle-stazioni.

[465] L. CARRER, *Riconoscimento facciale: come funziona e perché i piani del governo per introdurlo sono problematici,* in *ValigiaBlu,* 16 maggio 2023.

informazioni sui luoghi sensibili, in cui è maggiormente avvertita l'esigenza di prevenzione e repressione dei reati, in modo da disporre l'installazione dei sistemi di riconoscimento facciale incorporati nelle videocamere di sorveglianza.

Ad ogni modo, resta fermo che, qualora il Ministro Piantedosi intenda introdurre i sistemi *de quo* prima del 31 dicembre 2023, sia necessario il parere favorevole da parte del Garante per la protezione dei dati personale. Tuttavia, le speranze che il Garante *privacy* esprima il suo beneplacito sembrano poche: l'Autorità si è sempre mostrata molto attenta a tutelare i diritti e delle libertà fondamentali e particolarmente cauta nel consentire il trattamento dei dati biometrici dei cittadini italiani. Il Garante *privacy,* difatti, ha sempre espresso parere contrario a iniziative simili e ogni iniziativa in tal senso, volta ad introdurre il riconoscimento facciale, è sempre naufragata[466]: proprio nel 2021, il Ministero dell'Interno ha provato ad installare S.A.R.I. *Real Time,* al cui utilizzo il Garante ha espresso il proprio diniego[467]; nello stesso anno, il Garante ha bloccato il progetto *"ARGO per la sicurezza integrata"* presentato dal Comune di Torino, che prevedeva l'installazione di un sistema di videosorveglianza intelligente; parimenti, nel 2022, l'Autorità ha aperto un'istruttoria nei confronti dei Comuni di Lecce e Arezzo sui sistemi di sorveglianza intelligente[468]. Non sembra, dunque, che – rimasta invariata la disciplina legislativa – si possano scorgere spiragli perché il Garante esprima questa volta parere favorevole[469].

Resta, tuttavia, la circostanza che il 31 dicembre – termine ultimo per la moratoria sulla diffusione dei sistemi di riconoscimento facciale – è vicino, per cui il Governo Meloni potrebbe introdurre, per evitare il vuoto normativo, una legge di segno contrario, eliminando la necessità del parare favorevole da parte del Garante *privacy*[470]. In tale scenario, al Garante *privacy,* ultimo baluardo in materia di protezione dei dati personali, sarebbe affidato il difficilissimo compito di bilanciare, mediante il sindacato sul rispetto dei principi generali enucleati nel GDPR, le due opposte esigenze di sicurezza e di tutela dei diritti fondamentali.

---

[466] Si veda, *amplius,* il Capitolo Terzo, ove si tratteggia l'orientamento nel tempo espresso dal Garante per la protezione dei dati personali sulle tecniche di riconoscimento facciale.
[467] Si veda, *amplius,* il Capitolo Terzo, paragrafo §3.2.2.
[468] Si veda, *amplius,* il Capitolo Terzo, paragrafo §3.2.6.
[469] Cfr. M CASTIGLI, A. LONGO, *Riconoscimento facciale "anti-stupro", in Italia,* in *Network Digital 360, Cybersecurity 360,* 2 maggio 2023, consultabile su https://www.cybersecurity360.it/legal/ministro-dellinterno-vuole-il-riconoscimento-facciale-in-pubblico-ecco-i-rischi-principali/-.
[470] *Ibidem.*

Al quadro nazionale si aggiunga che, a livello sovranazionale, l'emanazione del Regolamento (UE) sull'Intelligenza Artificiale – recentemente emendato – potrebbe di nuovo cambiare le carte in tavola: *rebus sic stantibus*, cioè per come è stata presentata l'ultima bozza dell'*AI Act*[471], i sistemi di identificazione biometrica *in tempo reale* (quelli a cui sembra alludere il Ministro Piantedosi) in spazi aperti al pubblico per finalità di *law enforcement* sono del tutto vietati (art. 5, par. 1, lett. d)[472].

Tali considerazioni ci restituiscono l'immagine sfuocata di un mosaico i cui tasselli sono in continuo movimento. Non resta, dunque, che attendere gli sviluppi futuri.

## 2.3. Attuali utilizzi delle TRF da parte dei sistemi informatici dell'UE

La creazione di uno spazio di libertà, sicurezza e giustizia rappresenta uno dei principali obiettivi dell'Unione europea. In tale spazio, le autorità dei diversi Stati membri sono chiamate ad attuare misure di cooperazione e di condivisione di informazioni, utilizzando sistemi informativi su larga scala, allo scopo di tutelare i cittadini, contrastare la criminalità e garantire la sicurezza delle frontiere esterne. Affinché l'utilizzo dei sistemi informativi assurga a strumento utile per la protezione delle frontiere, per il controllo della migrazione e, in generale, per la sicurezza interna, è necessario che la gestione di tali informazioni sia efficace ed efficiente e, quindi, che le informazioni fornite dai sistemi informativi siano il più possibile complete, precise ed attendibili. In ragione di ciò, e in sostanziale risposta a particolari eventi terroristici o emergenziali verificatisi, le tecnologie utilizzate sono state rese sempre più accurate e basate sul trattamento dei dati biometrici[473].

I sistemi informativi dell'Unione europea utilizzano, infatti, le tecnologie di riconoscimento facciale e, in tal senso, forniscono indirettamente – per il tramite della

[471] Si badi: ci si riferisce agli emendamenti approvati dalla Commissione IMCO e dalla Commissione LIBE l'11 maggio 2023.
[472] Nella precedente bozza di Regolamento, quella presentata nell'Aprile 2021, invece, i sistemi *de quibus* erano ammessi solamente in presenza di una serie di stringenti condizioni.
[473] Per un'efficace ricostruzione, si veda N. VAVOULA, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement*?, in F. BIGNAMI (a cura di), *EU Law in Populist Times*, Cambridge University Press, Cambridge, 2020, 227 ss.; E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection, in European public law*, 26, 1, 2020, 71 ss. Per una panoramica si veda anche V. FERRARIS, *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere*?, in S. GOZZO, C. PENNISI, V. ASERO, R. SAMPUGNARO (a cura di), *Big Data e processi decisionali. Strumenti per l'analisi delle decisioni giuridiche, politiche economiche e sociali*, Egea, Milano, 2020, 136 ss.

disciplina che li regola – numerosi contributi e riferimenti normativi alle TRF. La caratteristica comune a tali sistemi, invero, oltre ad essere l'utilizzo del trattamento di tale particolare tipo di dato biometrico, è anche l'espressione di una particolare tecnologia – definita "*function creep*" – caratterizzata dalla possibilità di incrementarne le funzionalità in base alle esigenze[474].

Concepiti inizialmente per scopi diversi, tali strumenti convergono oggi verso obiettivi comuni e – seppur nell'architettura originaria apparivano poco organici, in quanto le informazioni venivano archiviate in sistemi non interconnessi, ossia, non in grado di scambiare i dati e condividere le informazioni – gli sviluppi e la gestione prossima di tali sistemi si muove verso una progressiva interoperabilità che, una volta implementata, consentirebbe un confronto dei dati acquisisti con quelli presenti nei diversi *database* in uso.

Venendo ad una disamina analitica dei principali sistemi dell'Unione che utilizzano le TRF, occorre, anzitutto, soffermare l'attenzione sul *"Sistema d'informazione Schengen"* (SIS), il quale è stato in origine previsto dalla Convenzione di applicazione dell'Accordo di Schengen[475] allo scopo di tutelare la sicurezza pubblica e facilitare la circolazione delle persone all'interno dello spazio Schengen, utilizzando le informazioni comunicate attraverso il sistema stesso[476]. In una fase successiva, ne è stata ampliata la portata di utilizzo, attraverso l'istituzione di un sistema di seconda generazione, il "*Sistema d'informazione Schengen di seconda generazione"* (SIS II), entrato in funzione il 9 aprile 2013[477], evolvendosi tale sistema da strumento di controllo a strumento investigativo[478]. Se in prima istanza le informazioni si basavano su dati di tipo

[474] G. MOBILIO, op. cit., 249.
[475] Si vedano, in particolare, gli artt. 92-119 della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, del 19 giugno 1990.
[476] Il Titolo IV della Convenzione di Schengen del 19 giugno 1990 è dedicato al "Sistema d'informazione Schengen". Ai sensi dell'art. 93, il suo scopo è quello «di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza dello Stato e di assicurare l'applicazione, nel territorio delle Parti contraenti delle disposizioni sulla circolazione delle persone stabilite nella presente Convenzione».
[477] Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II). A seguito del regolamento (UE) n. 2016/399, inoltre, il SIS II ha subito ulteriori modifiche nel 2018.
[478] M. TZANOU*, The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, in *Vienna Journal on International Constitutional Law,* 4, 3, 2010, 411 ss. Cruciale è stata l'esplicitazione del "principio di disponibilità" operata dal Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'unione europea (2005/C53/01), nell'ambito dell'obiettivo del "rafforzamento della sicurezza", secondo cui «in tutta l'Unione, un ufficiale

alfanumerico, successivamente sono state introdotte nuove funzionalità basate sulle tecnologie dell'utilizzo dei dati biometrici. I dati biometrici che possono essere conservati nel SIS consistono in fotografie, immagini del volto, impronte digitali, impronte palmari e profili del DNA. I dati raccolti devono essere trattati nel rispetto del principio di proporzionalità e le attività di trattamento dei dati personali sono sottoposte al controllo del Garante europeo della protezione dei dati[479].

Il sistema "*European dactylographic*" (EURODAC) – istituito con il Regolamento 2725/2000/CE – rappresenta un sistema centralizzato e informatizzato[480], costituito da un *database* in cui sono raccolte le impronte digitali di determinati cittadini di Paesi terzi[481]. In origine, il sistema veniva utilizzato con esclusivo riferimento alla comparazione delle impronte digitali dei richiedenti asilo o degli immigrati clandestini. Nel tempo, tuttavia, ne è stato ampliato l'utilizzo anche a scopi di sicurezza, per la gestione delle crisi migratorie e la protezione dei confini.

Il *"Sistema di informazione visti"* (VIS), disciplinato dal Regolamento (CE) 767/2008 e dalla decisione 2008/633/GAI, è una banca dati che semplifica la procedura per il rilascio dei visti per soggiorni di breve durata nei confronti dei cittadini di Stati terzi. In particolare, le autorità preposte possono accedere al VIS al fine di effettuare dei confronti biometrici e accertare l'identità delle persone, attraverso lo scambio di dati e informazioni tra gli Stati membri[482]. Il sistema consente l'accesso ad una serie di dati, sia alfanumerici, sia fotografie e impronte digitali[483]: il regolamento, a tal proposito, sancisce delle

---

di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e [...] il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliele per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato» (p. 2.1).

[479] Si veda, in particolare, l'art. 45 del regolamento (CE) n. 1987/2006.

[480] Cfr. E.R. BROUWER, *Eurodac: Its Limitations and Temptations, in European Journal of Migration and Law*, 4, 2, 2002, 231 ss.; F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Berlin-Heidelberg, 2012.

[481] Il riferimento, in particolare, è ai richiedenti asilo e ai cittadini di paesi extra-UE non appartenenti allo Spazio economico europeo.

[482] Il citato regolamento definisce la finalità "generica" del VIS nel «migliorare l'attuazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra le autorità centrali competenti per i visti, agevolando lo scambio di dati tra Stati membri in ordine alle domande di visto e alle relative decisioni».

[483] Art. 5, par. 1, lett. b, c, regolamento (CE) 767/2008. L'uso di dati biometrici è stato segnalato dal Garante europeo, anche qui, come un aspetto molto delicato, sottolineando la necessità di «porre in atto importanti garanzie», specie in termini di rispetto del principio della limitazione dello scopo, di restrizione dell'accesso e di misure di sicurezza; Cfr. GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata*, in *Gazzetta Ufficiale dell'Unione europea*, C 181/24, 22 giugno 2011.

differenze nell'utilizzabilità dei dati, in base agli scopi connessi all'utilizzo[484]. In particolare, le fotografie possono essere utilizzate solo nel caso in cui gli altri dati non fossero sufficienti all'identificazione, e limitatamente alla materia di immigrazione e asilo.

Il *"Sistema di ingressi/uscite"* (EES), disciplinato dal Regolamento (UE) 2017/2226, è uno strumento che prevede la rilevazione elettronica dell'ingresso e dell'uscita dei cittadini di Stati terzi, all'interno dello spazio Schengen[485]. Utilizzando le tecnologie di identificazione biometrica, nel dettaglio, il sistema crea per ciascun viaggiatore un fascicolo contenente i dati relativi all'identità, ai documenti di viaggio e ai dati biometrici, tra cui le immagini facciali[486]. L'utilizzo può essere ricondotto esclusivamente a scopi di identificazione o per attività istituzionali[487].

Da ultimo, il *"Sistema europeo di informazione sui casellari giudiziari"* (ECRIS), disciplinato dal Regolamento 2019/816, costituisce uno strumento che consente uno scambio di informazioni tra gli uffici dei casellari giudiziali dei Paesi membri, attraverso la creazione di un fascicolo contenente dati alfanumerici, impronte digitali e immagini del volto; queste ultime, tuttavia, non possono essere utilizzate a scopi identificativi[488].

## 2.4. Considerazioni finali

Alla luce dell'analisi svolta, emerge con chiarezza che le tecniche di riconoscimento facciale costituiscono mezzi di riconoscimento innovativi e sofisticati, epperò ancora privi, nel panorama europeo e nazionale, di una regolamentazione *ad hoc* che ne disciplini l'utilizzo, nonché le implicazioni e le conseguenze giuridiche.

---

[484] A fini di verifica ai valichi di frontiera esterni (art. 18); di verifica all'interno del territorio degli Stati membri dell'identità del titolare del visto, dell'autenticità del visto o della sussistenza delle condizioni d'ingresso, di soggiorno o di residenza (art. 19); di identificazione delle persone che non soddisfano le condizioni per l'ingresso, il soggiorno o la residenza nel territorio degli Stati (art. 20); per la determinazione della competenza per le domande di asilo (art. 21); per l'esame della domanda di asilo da parte delle autorità competenti (art. 22).

[485] Più in particolare, il sistema consente di registrare il momento e il luogo d'ingresso e di uscita dei soggetti sopra richiamati, di calcolare automaticamente la durata del soggiorno autorizzato, generare segnalazioni allo scadere del soggiorno e registrare il momento e il luogo di coloro che sono stati respinti per diniego del visto (art. 1, par. 1 regolamento (UE) 2017/2226).

[486] Artt. 16-17 regolamento (UE) 2017/2226. I dati dei viaggiatori che rispettano le norme di durata del soggiorno breve autorizzato vengono conservati per un periodo di tre anni, mentre quelli dei viaggiatori che hanno superato lo scadere del periodo di soggiorno autorizzato vengono conservati per cinque anni (art. 34, salvo le regole di modifica e cancellazione anticipata all'art. 35).

[487] Art. 27 regolamento (UE) 2017/2226.

[488] Artt. 5-6 Regolamento (UE) 2019/816.

È evidente che la disciplina applicabile ai dati biometrici estratti dalle TRF è costruita come una normativa basata sul rischio, il cui fine ultimo è la minimizzazione del rischio: infatti, per i dati biometrici è sempre richiesta la valutazione d'impatto da parte del titolare del trattamento.

In definitiva, la normativa applicabile alle TRF si risolve in pochissime norme, se non in grandi statuizioni di principio. In particolare, nel trattamento dei dati biometrici, i principi che devono essere osservati sono quelli di liceità, correttezza e trasparenza, di limitazione delle finalità, di minimizzazione dei dati, di esattezza, di limitazione della conservazione, nonché quelli di proporzionalità e di necessità.

In tale quadro normativo, il regolatore è chiamato ad applicare tali principi al caso concreto, godendo di amplissima discrezionalità. Alla luce di tali considerazioni, nel prossimo capitolo, studieremo l'orientamento del Garante per la protezione dei dati personali e del Comitato europeo per la protezione dei dati in merito alle tecniche di riconoscimento facciale.

# CAPITOLO TERZO

# *LAW IN ACTION*: LE TRF AL VAGLIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

## 3.1. L'orientamento del Garante per la protezione dei dati personali sulle TRF

Per apprezzare come i principi fin qui analizzati operino in concreto nel nostro ordinamento giuridico, occorre anzitutto ricostruire l'orientamento nel tempo espresso dal Garante per la protezione dei dati personali sulle tecniche di riconoscimento facciale.

Sin dalle prime applicazioni dei sistemi biometrici, il Garante della *privacy* ha assunto un atteggiamento di particolare cautela: già nel 2004 – in un convegno organizzato dal CNIPA sul tema "La biometria entra nell'*e-government*" – Gaetano Rasi, allora componente dell'Autorità Garante per la protezione dei dati personali, suggeriva di mantenere alto il livello di attenzione sui dati biometrici, affermando che «le legittime finalità per le quali vengono utilizzate le tecniche biometriche devono essere bilanciate da adeguate garanzie per i diritti e le libertà delle persone», pur rilevando che i dati biometrici, quali le impronte digitali, l'iride e il riconoscimento facciale, «per i loro stessi caratteri di universalità, permanenza e unicità, possono rivelarsi utili soprattutto a fini investigativi»[489].

Neppure lo scorrere del tempo è riuscito a scalfire tale atteggiamento di prudenza dell'Autorità: circa diciassette anni dopo, nell'aprile 2021, Ginevra Cerrina Feroni, attuale vicepresidente del Garante per la protezione dei dati personali, in un intervento al giornale "Il Messaggero"[490], ha affermato che «lo sviluppo tecnologico non deve essere frenato ma neppure si può ad esso aderire acriticamente senza porsi la visione del suo impatto sui fondamenti condivisi dell'etica e del diritto». Ciononostante, ha aggiunto che potrebbe essere consentito l'impiego delle TRF in luoghi pubblici, qualora sia necessario

[489] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Rasi: sui dati biometrici mantenere alto il livello di attenzione,* 23 novembre 2004.
[490] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il primato dell'uomo sulle macchine intelligenti – Intervento di Ginevra Cerrina Feroni – Il Messaggero,* 22 aprile 2021.

tutelare interessi fondamentali dello Stato – primo fra tutti la sicurezza nazionale – ma solamente a condizione che tale utilizzo sia limitato nel tempo e nello spazio.

Tale atteggiamento di prudenza ha sempre informato l'orientamento del Garante, che è rimasto uniforme e costante nel tempo.

Sin dalle prime pronunce, il Garante per la protezione dei dati personali è stato particolarmente restrittivo nel valutare la sussistenza dei presupposti che integrano il principio di proporzionalità e di necessità, soprattutto nei casi in cui i sistemi di rilevazione automatica mediante la raccolta dei dati biometrici fossero impiegati per il controllo degli accessi sul luogo di lavoro.

In un provvedimento, il Garante ha ritenuto che il ricorso alle tecnologie biometriche – si trattava in quel caso della racconta di impronte digitali dei dipendenti (c.d. *enrollement*), ma tali considerazioni possono estendersi anche alle TRF – fosse contrario al principio di necessità qualora potessero rivelarsi egualmente efficaci, in relazione alle finalità perseguite – in quel caso, la finalità consisteva nel prevenire condotte abusive nel rapporto di lavoro – strumenti alternativi di verifica dell'identità personale, egualmente rigorosi, che fossero «meno invasivi della sfera personale, della libertà individuale e che non coinvolgono il corpo […]»[491]. Allo stesso modo, come avremo occasione di approfondire, non ha superato il vaglio di proporzionalità l'utilizzo congiunto e sistematico di sistemi di rilevamento biometrico e di videosorveglianza per verificare la presenza in servizio dei dipendenti, con la conseguente finalità di contrastare il fenomeno dell'assenteismo sul posto di lavoro nelle pubbliche amministrazioni[492].

Viceversa, altrove, il ricorso ai sistemi biometrici di identificazione è stato considerato strettamente necessario e proporzionato rispetto alle finalità perseguite: è questo il caso che ha visto coinvolta l'azienda ospedaliera civile di Maria Paternò Arezzo di Ragusa, con riferimento al quale il Garante italiano ha ritenuto che i sistemi di autenticazione basati su tecniche biometriche – che rispondevano allo scopo di identificare con certezza i dati dei sanitari, dei pazienti e i prodotti ematici relativi alle operazioni di trasfusione – costituissero una modalità proporzionata in ragione dell'alto

[491] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante – Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro,* 21 luglio 2005

[492] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo",* 19 settembre 2019. Si veda, *amplius,* il paragrafo §3.2.1., reso a commento dell'intera vicenda.

valore della finalità perseguita e dei gravissimi rischi connessi[493]. Parimenti, il Garante ha ritenuto conforme ai canoni di proporzionalità e di necessità la richiesta di verifica preliminare – avanzata dall'Azione Policlinico Umberto I – di installazione di lettori biometrici rispondenti alla finalità di permettere l'accesso a locali ed aree a rischio, non ritenendo invece proporzionato l'uso delle tecniche biometriche per il perseguimento della diversa finalità di rilevazione della presenza in servizio del personale, in quanto tale modalità è particolarmente invasiva «in rapporto alle finalità perseguite», potendo essere sostituita con misure più tradizionali non lesive dei diritti della persona (quali apposizioni di firme, fogli di presenza o sistemi di timbratura mediante *badge* magnetico)[494].

Or dunque, tracciata la linea prospettica che informa l'orientamento del Garante, si può osservare che un conto è professare la necessaria osservanza del principio di proporzionalità, tutt'altra questione dover valutare che siano state effettivamente rispettate, nello specifico caso concreto, le condizioni di proporzionalità. Invero, pare che il regolatore sia chiamato – nell'estrema duttilità delle disposizioni regolamentari che disegnano contorni piuttosto sfumati e indefiniti – a specificare, o quasi creare, la norma da applicarsi nel caso concreto.

Ebbene, da un lato, la flessibilità e la snellezza della norma consentono un agevole adattamento ai cambiamenti sociali imposti da innovazione tecnologica e globalizzazione, oltre a perseguire gli obiettivi di contenere l'iperregolazione ed evitare che un'eccessiva quantità di regole pregiudichi la competitività del nostro sistema economico; tale elasticità, d'altro canto, non può tradursi in un potenziale arbitrio: ciò che va evitato è che la decisione del Garante della *privacy* giunga, per tale via, a trasmutarsi da giudizio di proporzionalità a "giudizio sul bene e sul male". In altri termini, il Garante si trova ad essere, in assenza di limiti ben delineati dal legislatore, arbitro di cosa è giusto e cosa è sbagliato nel nostro ordinamento giuridico: è giusto sorvegliare tramite l'impiego congiunto di sistemi biometrici e videosorveglianza i dipendenti della Pubblica Amministrazione, laddove la finalità consiste nel prevenire il fenomeno dell'assenteismo? È, invece, giustificato, raccogliere dati biometrici del personale sanitario e dei pazienti, laddove la finalità perseguita sia quella di prevenire errori di identificazione delle unità di sangue in caso di trasfusione?

[493] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Uso di dati biometrici nelle operazioni di trasfusione,* 19 giugno 2008 (doc. web n. 1532480).
[494] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Più sicurezza in ospedale con le impronte digitali,* 15 aprile 2008 (doc. web n. 1523435).

Il nodo cruciale, in buona sostanza, risiede nell'esigenza di stabilire quali siano i limiti entro i quali il Garante possa intervenire: il rischio paventato è che il Garante si spinga al di là di quanto consentito dalla norma, assumendo anche decisioni politiche idonee ad interferire con le prerogative del potere legislativo.

Appare, invece, evidente che si tratta di questioni che – prima di approdare dinanzi ad un'autorità amministrativa – necessitano di una più attenta e approfondita riflessione in sede parlamentare e, prima ancora, di un lungo dibattito di carattere culturale.

Riprendendo la nostra analisi giuridica, egualmente rigoroso è il Garante nel valutare il modo in cui gli operatori economici (e non economici) concretizzano la trasparenza dell'informativa sul trattamento dei dati personali di cui all'art. 13 del Regolamento, quale presupposto imprescindibile del diritto all'*autodeterminazione informativa*[495].

A titolo esemplificativo, come avremo modo di approfondire nel proseguo della presente trattazione, con il provvedimento che ha riguardato l'Università Commerciale "Luigi Bocconi" di Milano (16 settembre 2021), il Garante della *privacy* ha ingiunto all'Ateneo di pagare una somma pari a duecentomila euro, vietandogli altresì di porre in essere ogni ulteriore trattamento avente ad oggetto i dati biometrici degli studenti mediante il sistema "*Respondus"*, perché – tra gli altri motivi – l'informativa fornita agli interessati, oltre ad essere frammentaria e disorganica, non conteneva tutte le informazioni richieste dal Regolamento europeo ai fini di un trattamento corretto e trasparente[496].

In particolare, mostrando di guardare alla sostanza delle cose, il Garante ha sottolineato – avallando l'orientamento espresso dal Gruppo di lavoro "Articolo 29", poi fatto proprio dal Comitato europeo per la protezione dei dati[497] – che un'informativa

[495] Il diritto all'*autodeterminazione informativa* rappresenta uno degli ultimi approdi della tutela dei dati personali, in quanto per tale via viene tutelata anche l'identità digitale. Per un maggiore approfondimento sul diritto all'identità digitale, si veda G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 61 ss.

[496] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988). Si veda, *amplius,* il paragrafo §3.2.3., reso a commento del provvedimento *de quo.*

[497] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del Regolamento 216/679,* WP260, 11 aprile 2018, rev.01, 18 e 19, ove si specifica che certamente per evitare un «subissamento informativo» sono consentite, e anzi incoraggiate, informative stratificate, dovendo pur tuttavia guardarsi da creare confusione e smarrimento in chi legge: «le dichiarazioni/informative sulla *privacy* non sono mere pagine annidiate in altre che richiedono diversi clic per arrivare all'informazione voluta: il *design* e il *layout* del primo strato della dichiarazione/informativa sulla *privacy* dovrebbe essere tale da offrire all'interessato una panoramica chiara delle informazioni a sua disposizione sul trattamento dei dati personali e del luogo e del modo in cui può trovarle fra i diversi strati». Tali considerazioni sono

stratificata è in grado di integrare il principio di trasparenza e correttezza solamente «se le informazioni di primo e secondo livello sono presentate tra loro in maniera coerente e strutturata», in modo tale che gli interessati abbiano la possibilità «di conoscere gli elementi essenziali del trattamento nella prima informativa di primo livello, potendo poi scegliere di approfondire determinati aspetti nelle informative di dettaglio»[498]. Al contrario, nel caso di specie, le informazioni fornite agli studenti dall'Ateneo erano confusionarie e frammentarie, tanto che il trattamento posto in essere dall'Università non può ritenersi conforme al principio di liceità, trasparenza e correttezza.[499]

Ancor più recentemente, il 10 novembre 2022, il Garante della *privacy* ha irrogato una sanzione amministrativa pecuniaria pari a venti mila euro nei confronti di Sportitalia, una società sportiva dilettantistica che aveva introdotto un sistema di rilevamento delle impronte digitali allo scopo di verificare la presenza in servizio dei propri dipendenti, nonostante l'organizzazione sindacale segnalante – la CGIL – avesse chiesto di adottare mezzi di attestazione della presenza meno invasivi (*id est* non biometrici)[500]. In particolare, il Garante ha rilevato che l'introduzione del sistema di rilevazione biometrica violasse i principi di liceità, correttezza e trasparenza[501], in quanto l'informativa fornita ai dipendenti risultava eccessivamente stringata e laconica. Si legge nel provvedimento che «le uniche informazioni fornite ai dipendenti […] sono contenute in un breve capoverso presente all'interno dell'informativa relativa alla generalità del trattamenti effettuati nel contesto del rapporto di lavoro», risultando l'informativa del tutto inidonea a descrivere le caratteristiche del trattamento da effettuare. In aggiunta, il documento predisposto dalla società non contemplava la possibilità per il dipendente di utilizzare, in alternativa al sistema di cui trattasi, il tradizionale *badge*[502].

state fatte proprie dall'EDPB mediante COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Endorsement* 1/2018, 25 maggio 2018.

[498] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).

[499] *Ibidem.*

[500] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022.

[501] Art. 5, par. 1 del GDPR – Principi applicabili al trattamento di dati personali.

[502] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022.

## 3.2.Le principali decisioni del Garante per la protezione dei dati personali

Val la pena ora analizzare le principali decisioni assunte dal Garante aventi ad oggetto i sistemi biometrici, con la precisazione che sono state tutte pronunciate dopo l'entrata in vigore del Regolamento europeo in materia di protezione dei dati personali.

### 3.2.1. Il parere del Garante sulla Legge n. 56/2019 recante "*Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*": l'introduzione sistematica e generalizzata di sistemi di rilevazione delle presenze tramite l'identificazione biometrica viola i principi di proporzionalità e di necessità (19 settembre 2019)

Le tecnologie basate sui dati biometrici hanno visto applicazioni e sviluppi sempre più ampi e nei campi più variegati. Anche nel settore pubblico tali tecnologie giocano un ruolo sempre più importante.

In tal senso, è stato ipotizzato l'impiego della biometria anche per il contrasto a fenomeni come l'assenteismo e per il controllo dell'accesso dei dipendenti sul posto di lavoro: nella Legge n. 56/2019, la c.d. legge «concretezza»[503], l'art. 2, comma 1 – poi abrogato dall'art. 1, comma 958 della legge n. 178/2020 – disponeva, come misura di contrasto all'assenteismo che «[a]i fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche […] introducono sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso»[504]. Tale norma prevedeva, quindi, l'introduzione di sistemi di rilevazione dei dati biometrici e di videosorveglianza degli accessi per la verifica del rispetto degli orari di lavoro, al fine di combattere il fenomeno della falsa attestazione della presenza in servizio nelle pubbliche amministrazioni. I "sistemi di verifica biometrica dell'identità", in sostanza, si sarebbero concretizzati nel controllo delle impronte digitali e dell'iride, in sostituzione del "vecchio" cartellino; nel novero dei soggetti destinatari di tali misure, sarebbero state escluse soltanto alcune categorie di dipendenti pubblici, tra cui le forze dell'ordine, la magistratura, i prefetti ed il personale

[503] Legge 19 giugno 2019, n. 56 – Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo, G.U. Serie Generale n. 145 del 22 giugno 2019.
[504] Art. 2, legge n. 56 del 2019 (*abrogato*).

scolastico (ad eccezione dei presidi), individuando quali destinatari, invece, il resto del personale dipendente della pubblica amministrazione[505].

Il Garante per la protezione dei dati personali, con riferimento all'utilizzo dei dati biometrici in ambito lavorativo, nel tempo, ha manifestato posizioni diverse e, se in alcuni casi ha autorizzato l'utilizzo di tali dati[506], recentemente ha adottato provvedimenti più restrittivi sull'utilizzo dei sistemi di riconoscimento nei luoghi di lavoro, in ragione della delicatezza dei dati in questione, i quali – in quanto consentono o confermano «l'identificazione univoca»[507] – sono soggetti ad una tutela rafforzata.

In merito alle misure ipotizzate per contrastare i fenomeni di assenteismo e false timbrature nella pubblica amministrazione, l'Autorità si è espressa più volte[508], sia con riferimento al disegno di legge 920 del 2018[509], sia con riferimento alla successiva legge 56 del 2019[510], rappresentando le proprie considerazioni circa l'utilizzo dei sistemi di rilevazione biometrica, così come prospettati dai diversi testi normativi.

Più nel dettaglio, nel primo parere reso sulla questione[511] – risalente al 11 ottobre 2018 – su richiesta della Presidenza del Consiglio dei Ministri, il Garante della *privacy* aveva espresso parere parzialmente favorevole allo schema di disegno di legge recante *"interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*"[512]. In tale circostanza, infatti, l'Autorità aveva rilevato la

[505] Art. 2, legge n. 56 del 2019 (*abrogato*).
[506] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamenti di dati biometrici dei dipendenti. Verifica Preliminare*, 18 giugno 2015 (doc. web n. 4173465).
[507] Art. 4, par. 1, n. 14, GDPR.
[508] Diverse sono state le pronunce del Garante con riferimento alle misure ipotizzate dal Governo per la prevenzione dell'assenteismo, sia avendo riguardo al disegno di legge 920/2018, sia, da ultimo, avendo riguardo alla legge n. 56/2019: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 11 ottobre 2018 (doc. web. 9051774); ID., *Audizione informale di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sul disegno di legge n. 920, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 27 novembre 2018 (doc. web. 9064421); ID., *Audizione del Presidente dell'Autorità Garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 6 febbraio 2019 (doc. web. 9080870); ID., *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56 recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 19 Settembre 2019 (doc. web.9147290).
[509] Disegno di legge 920 del 2018, presentato in data 6 novembre 2018, su iniziativa governativa del Ministro senza portafoglio per la pubblica amministrazione Giulia Bongiorno (Governo Conte-I).
[510] Legge n. 56/19 del 19 giugno 2019, GU n. 145 del 22 giugno 2019.
[511] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 11 ottobre 2018 (doc. web. 9051774).
[512] Disegno di legge 920 del 2018.

liceità delle basi giuridiche prospettate dal disegno di legge 920 del 2018, considerandole idonee a legittimare il trattamento dei dati biometrici; al contempo, tuttavia, aveva sollevato dubbi in merito all'utilizzo simultaneo dei sistemi di videosorveglianza e di raccolta di dati biometrici, in ragione della mancata compatibilità con il principio di proporzionalità, suggerendo, quindi, una modifica al disegno di legge al fine di utilizzare uno solo dei due sistemi previsti dalla norma. Da ultimo, con riguardo al principio di "minimizzazione dei dati", rilevava sproporzionata e non necessaria l'introduzione non graduale e generalizzata di tali sistemi, ove questi non apparivano necessari rispetto agli scopi perseguiti o alla presenza di particolari presupposti, quali, ad esempio «le dimensioni dell'ente, il numero dei dipendenti coinvolti, la ricorrenza di situazioni di criticità che potrebbero essere anche influenzate dal contesto ambientale»[513].

Successivamente – anche in ragione della mancata attuazione delle modifiche suggerite sul disegno di legge dall'Autorità – il Garante è tornato sulla questione attraverso l'intervento del Presidente Antonello Soro[514], in data 6 febbraio 2019, confermando i dubbi già espressi nel precedente parere[515], con particolare riferimento al rispetto del principio di proporzionalità da parte dell'art. 2 del disegno di legge summenzionato. In altre parole, come già in precedenza rappresentato, per il Garante «l'introduzione sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni di sistemi di rilevazione biometrica delle presenze non può ritenersi in alcun modo conforme al canone di proporzionalità a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato»[516], suggerendo, quindi – ancora una volta – di apportare le modifiche alla norma, prima della trasposizione nel testo definitivo di legge. Infatti, secondo il parere dell'Autorità, in assenza di fattori di rischio specifici, tali misure di controllo biometrico – pur essendo l'assenteismo un fenomeno il cui contrasto è sicuramente condivisibile – non sarebbero supportate da

[513] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 11 ottobre 2018 (doc. web. 9051774).
[514] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Audizione informale di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sul disegno di legge n. 920, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 27 novembre 2018 (doc. web. 9064421).
[515] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 11 ottobre 2018 (doc. web. 9051774).
[516] *Ibidem.*

situazioni di necessità tali da giustificare l'utilizzo indiscriminato, a qualsiasi contesto lavorativo della pubblica amministrazione, di tali strumenti.

Nonostante le considerazioni espresse dal Garante, il 19 giugno 2019 la c.d. legge «concretezza»[517] è entrata in vigore, senza aver integrato o modificato quanto suggerito più volte dall'Autorità, con particolare riferimento all'art. 2.

*Rebus sic stantibus*, il 19 settembre 2019, il Garante si è pronunciato sulla Legge 56 del 2019, rilevando tutti i profili di dubbia compatibilità con la disciplina europea e nazionale in materia di protezione dei dati personali. La posizione dell'Autorità, anche in tale provvedimento, è stata coerente con i precedenti pareri e con le precedenti audizioni sulla questione: è stata ribadita sia la non necessarietà dell'utilizzo contestuale degli strumenti di videosorveglianza e rilevazione biometrica sia che l'utilizzo di tali strumenti in misura generalizzata e sistematica per ogni pubblica amministrazione si pongono in contrasto con il principio di proporzionalità[518].

Il Garante, inoltre, nella Relazione annuale del 2019, ha inteso chiarire la propria posizione in merito all'utilizzo dei dati biometrici dei dipendenti pubblici e privati per finalità di rilevazione delle presenze, anche in relazione ai quesiti posti con riferimento alla legge n. 56 del 19 giugno 2019. *In primis*, l'Autorità ha rappresentato il particolare rilievo che il Regolamento europeo riserva ai dati biometrici, in quanto rientranti nel novero delle «categorie particolari di dati personali»[519], e la necessaria conseguenza che il loro trattamento sia consentito solo qualora «necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro [...], 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»[520]. L'Autorità, sulla scorta di tali considerazioni, ha ribadito la propria posizione, già espressa nei pareri resi con riguardo alla summenzionata legge, rintracciando le principali criticità nel mancato rispetto del principio di proporzionalità della norma. Secondo quanto affermato dal Garante, tali disposizioni normative, incompatibili con i canoni di

[517] Legge 19 giugno 2019, n. 56 – Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo, G.U. Serie Generale n. 145 del 22 giugno 2019.
[518] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56 recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 19 Settembre 2019 (doc. web.9147290).
[519] Art. 9, par. 1, del GDPR.
[520] Art. 9, par. 2, lett. b), del GDPR; si vedano pure art. 88, par. 1 e Cons. 51-53 del GDPR.

proporzionalità e di necessità, non sarebbero superabili nemmeno con il consenso dei dipendenti, non costituendo quest'ultimo una base giuridica idonea al trattamento dei dati biometrici in ambito lavorativo, al fine della rilevazione delle presenze[521].

### 3.2.2. Il parere del Garante sull'utilizzo del sistema S.A.R.I. *Real Time* non è favorevole: il *software* realizzerebbe un controllo su "larga scala" senza la necessaria base giuridica adeguata (16 aprile 2021)

Il S.A.R.I. (Sistema Automatico Riconoscimento Immagini) è un sofisticato sistema elettronico impiegato per l'elaborazione delle immagini, adottato a partire dal 2017 dal Ministero dell'Interno e offerto in dotazione alla Polizia di Stato quale strumento investigativo. Il *software* utilizza una tecnologia molto simile, nel funzionamento, a quella in uso alla *South Wales Police*, forza di polizia del Regno Unito, la quale, dal 2017 ha iniziato a sperimentare, con il progetto pilota "*Automated Facial Recognition (AFR) Locate*" l'utilizzo delle TFR per le attività di prevenzione, indagine e repressione dei reati attraverso la processazione e la comparazione di immagini[522].

Più precisamente, il sistema S.A.R.I. si basa sull'utilizzo, contestuale o separato, di due diversi algoritmi per l'elaborazione delle immagini (il *Parsec*, sviluppato da una società italiana, e il *Neurotechnology*, sviluppato in USA), in grado di analizzare l'immagine di un volto posto frontalmente e di estrapolarne fino ad 850 tratti caratteristici, i cc.dd. "punti fiduciari"[523], al fine di confrontarli con le foto raccolte nel database AFIS[524]. Il sistema S.A.R.I., invero, confronta una qualsiasi fotografia del soggetto ricercato – anche estrapolata da canali esterni – con le foto segnaletiche presenti nelle banche dati. L'analisi viene effettuata, innanzitutto, secondo un modello di comparazione uno-a-molti (1-n), nel senso che la foto dell'individuo ricercato viene confrontata con

[521] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *13.12 il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze*, Relazione 2019.
[522] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 240.
[523] R. V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, il Penalista, 16 gennaio 2019, consultabile su https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti.
[524] Acronimo di "*Automated Fingerprint Identification System*", o "*Sistema Automatizzato di Identificazione delle Impronte*".

quella dei profili compatibili; in secondo luogo, attraverso un *matching* di ricerca uno-a-uno (1-1), che si conclude con un riscontro positivo o negativo[525].

Il S.A.R.I. presenta due diverse versioni: da un lato, si colloca il S.A.R.I. *Real Time*, non attivo, che secondo l'idea originaria dovrebbe assurgere a strumento di controllo, da utilizzare in occasione di eventi e manifestazioni[526]. In particolare, il *software*, mediante riprese in tempo reale in un'area territorialmente delimitata, confronta le immagini dei volti dei presenti con quelle inserite in una *watchlist*[527] – una banca dati predefinita e creata *ad hoc* per l'evento – e in caso di *match* positivo allerta gli operatori. La *watchlist*, inoltre, può comprendere al suo interno non solo le immagini foto segnaletiche ma qualsiasi foto, seppur in posizione frontale, acquisita, anche, per esempio, dai *social network*[528].

Dall'altro lato, il S.A.R.I. *Enterprise*, in uso dal 2018, nasce in un'ottica investigativa e permette la ricerca, in maniera automatica, di un volto all'interno di un'immagine, attraverso il confronto tra le immagini acquisite e quelle presenti nella banca dati AFIS[529]. Il *software*, quindi, riesce a individuare da un'immagine il volto di un soggetto e a generare, attraverso la ricerca nel *database*, le immagini di circa 50 volti simili, sottoponendo le corrispondenze alla valutazione dell'operatore affinché quest'ultimo valuti il candidato corrispondente all'immagine. Per ogni immagine rintracciata, inoltre, il sistema è in grado di stabilire la percentuale di somiglianza. In via ulteriore, tale tecnologia permette all'operatore di adattare la ricerca alle esigenze di specie, scegliendo, se del caso, di interrogare una specifica banca dati o una sezione di essa, integrando la ricerca anche con informazioni descrittive o anagrafiche associate alle immagini[530].

---

[525] S. MARASCIO, *Intelligenza Artificiale, biometria e indagini di Polizia*, Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022), 44 e ss. Sulla distinzione tra comparazione uno-a-molti (1-n) e comparazione uno-a-uno (1-1), si rinvia, *infra,* Capitolo Primo, paragrafo §1.2.

[526] MINISTERO DELL'INTERNO DIPARTIMENTO DELLA PUBBLICA SICUREZZA, *Capitolato tecnico - procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. lotto n° 1*.

[527] *"Banca dati di soggetti attenzionati, dell'ordine di centinaia di migliaia di immagini, impiegata dal sistema di riconoscimento in* real-time *per la generazione di alert",* in MINISTERO DELL'INTERNO DIPARTIMENTO DELLA PUBBLICA SICUREZZA, *Capitolato tecnico - procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. lotto n° 1*.

[528] R. V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, il Penalista, 16 gennaio 2019, consultabile su https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti.

[529] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 240.

[530] R. V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, il Penalista, 16 gennaio 2019, consultabile su https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti.

È di recentissima la notizia di stampa[531] l'arresto dell'uomo accusato di aver accoltellato, il 31 dicembre 2022, una turista israeliana alla stazione Termini di Roma. L'uomo, in particolare, sarebbe stato identificato dalle forze dell'ordine proprio attraverso il *software* S.A.R.I. *Enterprise:* dal filmato registrato presso la stazione Termini, il sistema di riconoscimento facciale ha estrapolato la foto segnaletica del sospettato confrontandolo con oltre 10 milioni di identità presenti nel *database* AFIS. Data l'impossibilità di utilizzare anche la versione *Real Time* del *software,* per i motivi qui di seguito riportati, la ricerca dell'uomo è proseguita attraverso l'attività investigativa delle forze di polizia.

Nonostante l'entusiasmo per la portata tecnologica e innovativa di tali strumenti, il sistema di riconoscimento facciale S.A.R.I. ha suscitato sin dagli albori numerosi dubbi in merito alla presenza di una valida base giuridica nell'ordinamento in grado di consentire l'utilizzo di tale tecnologia.

Per tale ragione, in data 27 luglio 2018, il Garante della *privacy* è intervenuto a sciogliere ogni dubbio, pronunciandosi favorevolmente sulla legittimità dell'utilizzo del S.A.R.I, nella versione *Enterprise*, in quanto di fatto lo strumento *de quo* non costituisce un diverso trattamento dei dati, ma semplicemente «una diversa modalità di trattamento di dati biometrici»[532], già disciplinato dal d. m. del 24 maggio 2017. Difatti, il sistema ivi richiamato non effettua nuove o diverse elaborazioni delle immagini, ma va ad automatizzare, attraverso l'algoritmo, alcune operazioni che altrimenti avrebbero richiesto l'intervento manuale dell'operatore. Da qui, il beneplacito del Garante all'utilizzo del S.A.R.I. *Enterprise*[533].

Quanto alla versione *Real Time*, l'istruttoria del Garante della *privacy* era stata avviata nel 2017 e poi interrotta nel 2018, a seguito della richiesta, trasmessa al Viminale dal Garante*,* di fornire la valutazione di impatto relativa al sistema di riconoscimento facciale

---

[531] F. TONACCI, *Roma, il "cervellone" che ha scovato l'aggressore di Termini: meno di un minuto per cercare tra 10 milioni di volti,* 5 gennaio 2023, La Repubblica, consultabile su https://www.repubblica.it/cronaca/2023/01/05/news/polacco_roma_termini_riconoscimentofacciale-382147119/.

[532] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto,* 26 luglio 2018, (doc. web. 9040256).

[533] *Ibidem.*

(c.d. DPIA)[534], a cui tuttavia, il Viminale non aveva dato immediatamente seguito[535]. Successivamente, assolto il titolare del trattamento l'adempimento richiesto, il Garante, nel parere del 25 marzo 2021, ha espresso il proprio diniego all'utilizzo del *software* nella versione *Real Time* per le seguenti ragioni[536].

Nel provvedimento in esame il Garante afferma – in linea con quanto statuito dal Consiglio d'Europa – che tale strumento, nella modalità *Real Time*, «oltre ad essere privo di fondamento legislativo che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, realizzerebbe per come è progettato una forma di sorveglianza indiscriminata di massa»[537].

In particolare, dal momento che il sistema di riconoscimento facciale è in grado di analizzare in tempo reale i volti di tutte le persone presenti, confrontandoli con quelli inseriti nella *whatch-list,* un simile trattamento delle immagini, in quanto volte all'identificazione delle persone in contesti pubblici, realizzerebbe un controllo "su larga scala". Ancorché nella valutazione d'impatto presentata dal Ministero dell'Interno si sottolinei che le immagino sono immediatamente cancellate dal *database,* tale sistema, attraverso sistemi di videosorveglianza in tempo reale, permetterebbe l'analisi dei volti di tutti i partecipanti alla manifestazione o all'evento, e quindi anche di coloro non oggetto di indagini da parte delle forze di Polizia[538]: si assisterebbe, dunque, al «passaggio da una sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale»[539].

Proprio in ragione della forte pervasività nella vita privata delle persone di tali strumenti, la normativa in materia di trattamento dei dati personali appresta rigorose cautele per il trattamento di dati biometrici. Invero, non v'è dubbio che i dati trattati costituiscono «dati biometrici intesi a identificare in modo univoco una persona fisica»,

---

[534] Ricompresa tra gli strumenti che garantiscono l'*accountability* del titolare del trattamento, abbiamo già analizzato nel presente elaborato la disciplina sulla valutazione d'impatto per la protezione dei dati (c.d. *Data Protection Impact Assessment* o DPIA), con riferimento alla quale si rinvia, *infra,* Capitolo Secondo, paragrafo §2.3.6.

[535] R. COLUCCINI, *Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale*, IRPIMEDIA, 13 gennaio 2021, consultabile su https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/.

[536] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 [9575877], Registro dei provvedimenti n. 127 del 25 marzo 2021.

[537] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy,* 16 aprile 2021, consultabile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842.

[538] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 [9575877], Registro dei provvedimenti n. 127 del 25 marzo 2021.

[539] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy,* 16 aprile 2021.

rientranti nel novero delle «categorie particolari di dati» di cui all'art. 9 del GDPR, ma non si può escludere *ex ante* che siano coinvolti altri dati personali (come, ad esempio, quelli idonei a rivelare opinioni politiche, sindacali, religiose, orientamenti sessuali del soggetto) [540].

In ossequio alla disciplina introdotta dal Regolamento europeo sulla protezione dei dati personali, è necessaria la presenza di una valida base giuridica volta a disciplinare tale sistema di riconoscimento facciale, in grado di soddisfare i requisiti previsti dall'art. 8 della CEDU e dall'art. 52 CDFUE, nonché dall'art. 10 della LED, dall'art. 9 del GDPR e dall'art. 7 del d.lgs. n. 51/2018, il quale prevede che il trattamento sia «specificatamente previsto» dal diritto dell'UE o da legge[541].

Secondo quanto ritenuto dal Garante, nella documentazione fornita dal Ministero dell'Interno, non è menzionata alcuna disposizione specifica idonea a soddisfare i requisiti richiesti dalla normativa summenzionata: il complesso delle norme richiamate dal Ministero[542] – non operando alcuna ponderazione dei diritti delle libertà in gioco – non rende «adeguatamente prevedibile» l'uso del sistema di riconoscimento facciale, in quanto conferisce una discrezionalità talmente ampia che il suo utilizzo dipende, in buona sostanza, «da coloro che saranno chiamati a disporlo, anziché dalla emananda previsione normativa[543]».

Più nel dettaglio, il Garante suggerisce in via esemplificativa gli elementi che dovrebbero essere individuati *de iure condendo*: oltre ad individuare i criteri di selezione

---

[540] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 [9575877], Registro dei provvedimenti n. 127 del 25 marzo 2021.

[541] *Ibidem;* cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 242.

[542] Il Garante opera un'attenta disamina delle norme richiamate dal Ministero dell'Interno nella valutazione d'impatto, scardinando uno ad uno la loro pretesa idoneità a soddisfare i requisiti richiesti: il d.lgs. n. 51 del 2018, nonostante preveda in astratto tali trattamenti, non costituisce fonte normativa idonea a legittimarli, perché volto a specificare le condizioni che ne giustificherebbero l'utilizzo (tra cui, appunto, la sussistenza di una norma di legge che lo autorizzi in modo specifico); l'art. 1 del T.U.L.P.S. non contiene riferimenti al trattamento di cui si discorre; il d.P.R. 15 gennaio 2018, n. 15, adottato in attuazione dell'art. 57 del previgente Codice *privacy*, disciplina al Capo V il trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video – sistemi ontologicamente diversi da quelli che sfruttano i dati biometrici; similmente, gli articoli 134 co. 4, 234, 266 e 431 co. 1, lett. b, del codice di procedura penale, citati nella valutazione di impatto, riguardano, trattamenti diversi da quelli implicanti dati biometrici diretti all'identificazione personale; parimenti, gli articoli 55, 348, 354 e 370 del codice di procedura penale non prevedono il trattamento dei dati biometrici, con la conseguenza che non sono tali da integrare quella fonte normativa specifica richiesta dall'art. 7 del Decreto.

[543] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 [9575877], Registro dei provvedimenti n. 127 del 25 marzo 2021; la medesima considerazione è ripresa anche in GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*.

dei soggetti che possono essere inseriti nella *watch-list* e i criteri di individuazione dei casi che giustificano l'utilizzo del sistema, il legislatore, tenendo in debito conto i limiti di tale innovativa tecnologia – notoriamente fondata su schemi e correlazioni su base statistica – dovrebbe disciplinare le eventuali conseguenze per gli interessati nel caso in cui il sistema abbia ingenerato falsi positivi[544].

Sulla scorta di tali considerazioni, in definitiva, il Garante ha espresso parere non favorevole all'utilizzo del sistema S.A.R.I. *Real Time* nei termini di cui in motivazione, ritenendo il sistema non conforme alla disciplina dettata in materia di protezione dei dati personali[545].

### 3.2.3. Il caso dell'Università "Luigi Bocconi" di Milano: illecito il trattamento dei dati biometrici in sede di svolgimento delle prove scritte d'esame sostenute *online* dagli studenti (16 settembre 2021)

Il caso dell'Università "Luigi Bocconi" (di seguito, anche "Università" o "Ateneo") riguarda un'ordinanza di ingiunzione del 16 settembre 2021 disposta dal Garante, in relazione all'illecito trattamento dei dati biometrici da parte dell'Ateneo[546]. In particolare, ad essere contestato è stato l'utilizzo, da parte dell'Università, di due *software*, di proprietà della società americana *Respondus Inc,* per la supervisione degli studenti nel corso dello svolgimento degli esami *online*. L'istruttoria ad opera del Garante ha avuto avvio a seguito di una segnalazione da parte di uno studente dell'Ateneo, il quale aveva sollevato dubbi in merito alla liceità dei sistemi di controllo utilizzati per le sessioni d'esame, durante le restrizioni dovute alla diffusione della pandemia da Covid-19, in quanto foriere di possibili violazioni della disciplina sulla protezione dei dati personali[547].

Nel dettaglio, l'Università si sarebbe avvalsa di un sistema di supervisione a distanza, di c.d. "*proctoring*", strutturato nelle due diverse componenti *"Respondus Monitor"* e *"LockDown Browser"*: il primo, in particolare, attraverso la *webcam,* acquisisce e tratta dati biometrici attraverso registrazioni video e scatti di istantanee sia dello schermo che dello studente stesso, generando al termine dell'esame un video in

[544] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 [9575877], Registro dei provvedimenti n. 127 del 25 marzo 2021.
[545] *Ibidem*.
[546] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).
[547] *Ibidem.*

grado di segnalare all'operatore (il docente esaminatore), mediante un *alert,* specifiche anomalie nel comportamento (come, ad esempio, «sguardo non rivolto verso il monitor, volto parzialmente assente dalla foto, volto mancante»[548]) al fine di convalidare o invalidare l'esame. Il secondo, invece, è in grado di bloccare lo schermo del *computer*, impedendo allo studente di uscire dalla pagina d'esame o visualizzare altre pagine nel *web* o in locale[549].

In risposta alla richiesta di informazioni del Garante, l'Ateneo ha inteso fornire le proprie argomentazioni con una nota di riscontro all'Autorità, dichiarando che «l'impossibilità di svolgere le sessioni d'esame secondo la consueta procedura, ha portato l'Università […] a strutturare un processo che, nel rispetto del [Regolamento] e del Codice Privacy, unicamente per le prove d'esame scritte, fosse in grado di identificare gli Studenti attraverso l'utilizzo temporaneo del loro dato biometrico e, dunque, elaborando automaticamente le immagini digitali che raffigurano il volto degli stessi a fini di identificazione, autenticazione e verifica " in particolare la "fotografia del tesserino" e "l'immagine fotografica scattata da *Respondus*»[550], rappresentando, inoltre, le motivazioni e le basi giuridiche relative al trattamento dei dati, nonché il funzionamento dei *software* in questione.

L'attività del Garante per la protezione dei dati personali, tuttavia, ha evidenziato diverse violazioni nell'attività posta in essere dall'Ateneo, concludendo l'istruttoria con una sanzione pecuniaria nei confronti dell'Università "Luigi Bocconi" per trattamento illegittimo dei dati personali degli studenti nel corso delle prove d'esame sostenute *online*[551].

Sinteticamente, le eccezioni sollevate dal Garante fanno riferimento ad una base giuridica errata, ad un'informativa non corretta e trasparente e all'invio di dati all'estero[552].

Nello specifico, con riferimento al primo aspetto, il Garante della *privacy* ha contestato all'Ateneo l'assenza di una base giuridica idonea al trattamento dei dati

[548] *Ibidem.*
[549] *Ibidem.*
[550] *Ibidem.*
[551] *Ibidem*.
[552] Agendadigitale.eu [2021], *Controllo remoto degli studenti, vizio di tanti: il Garante non sanzioni solo Bocconi*, 30 settembre 2021, consultabile su https://www.agendadigitale.eu/sicurezza/privacy/controllo-remoto-degli-studenti-tanti-peccano-il-garante-non-sanzioni-solo-bocconi.

biometrici degli studenti[553]. Infatti, pur avendo l'Università dichiarato in seconda istanza – in rettifica a quanto precedentemente dalla stessa sostenuto – che il sistema "Respondus" non comporta il trattamento dei dati biometrici, il Garante ha rilevato come, invero, il *software* effettui un trattamento dei dati biometrici consistente nella verifica dell'identità e, più nello specifico, «nella raccolta, elaborazione e analisi del video prodotto dal software tramite un algoritmo di intelligenza artificiale al fine di produrre i *"flag*"»[554]. Appurato quindi il trattamento dei dati biometrici da parte dell'Università, l'Ateneo ha individuato nel consenso dello studente la base giuridica per il trattamento dei dati raccolti mediante il sistema "*Respondus*". Tuttavia, il Garante ha rappresentato come il consenso degli studenti non può ritenersi idoneo ad assurgere quale base giuridica valida, vista l'impossibilità di considerarsi come «manifestazione di volontà libera»[555] da parte degli studenti in ragione della posizione di squilibrio tra il titolare del trattamento e quest'ultimi. Inoltre, escluso il consenso quale base giuridica, il trattamento dei dati biometrici sarebbe consentito solo qualora risulti «necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[556].

Quanto al secondo aspetto, è noto l'obbligo del titolare del trattamento di fornire all'interessato l'informativa «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato»[557]. A seguito dell'istruttoria svolta dal Garante, è stata rilevata la mancata correttezza e trasparenza dell'informativa resa dall'Università agli studenti, in quanto questa, a parere dell'Autorità, non rappresentava tutte le informazioni richieste

[553] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).
[554] *Ibidem.*
[555] Art. 4, n. 11 del Regolamento UE 2016/679 – Definizioni.
[556] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).
[557] Art. 12, par. 1 del GDPR - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato.

dal Regolamento[558]. In particolare, il Garante ha contestato all'Ateneo che l'informativa in questione non indicava espressamente il trattamento posto in essere dal *software*, con particolare riferimento alla profilazione e al monitoraggio del comportamento dello studente durante l'esame, alle informazioni relative alla fotografia scattata all'inizio della prova e a quelle relative ai temi di conservazione dei dati. Sotto tale ultimo aspetto, infatti, l'informativa, si limitava a prevedere «un tempo strettamente necessario al perseguimento delle finalità indicate»[559].

Da ultimo, il Garante ha contestato all'Università la violazione degli artt. 44 e 46 del Regolamento europeo, relativi al trasferimento internazionale dei dati personali[560]. Anche in questo caso, infatti, l'informativa era priva dell'indicazione della circostanza che i dati sarebbero stati oggetto di trasferimento al responsabile del trattamento – individuato nella società *Respondus, Inc.* – sito al di fuori del territorio europeo e stabilito negli Stati Uniti d'America. Tale questione, relativa al trasferimento dei dati in paesi non appartenenti allo Spazio Economico Europeo, era già stata affrontata dalla Corte di Giustizia dell'Unione europea nella sentenza Schrems II[561], in cui si era stabilita la non conformità dei trattamenti svolti negli Stati Uniti, salvo il caso in cui questi avessero previsto le garanzie ulteriori previste nel GDPR. A seguito dell'istruttoria svolta dal Garante in merito all'accordo tra l'Università e Respondus Inc., le garanzie e le tutele previste non sono state ritenute idonee a garantire la sicurezza dei trasferimenti dei dati[562].

### 3.2.4. Il caso *Clearview AI Inc.*: vietati l'uso dei dati biometrici e il monitoraggio degli italiani (10 febbraio 2022)

Il 10 febbraio 2022 il Garante per la protezione dei dati personali ha emesso nei confronti della *startup* americana *Clearview AI Inc.* (di seguito anche la "Società") un'ordinanza di ingiunzione al pagamento di una somma di venti milioni di euro a titolo

[558] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).
[559] *Ibidem.*
[560] *Ibidem*
[561] Sentenza della Corte di Giustizia dell'Unione europea (Grande Sezione) del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, adottata il 23 luglio 2020, Causa C-311/18;
[562] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).

di sanzione amministrativa[563], in quanto la Società ha posto in essere un monitoraggio biometrico nei confronti di persone collocate nel territorio italiano[564], senza l'adeguata base giuridica necessaria, nonché per la violazione del principio di liceità, correttezza e trasparenza[565], del principio di limitazione della finalità[566] e del principio di conservazione[567].

In particolare, il caso ruota attorno alla società *Clearview AI* e all'omonimo *software* di intelligenza artificiale dalla stessa sviluppato. L'azienda tecnologica statunitense – fondata nel 2017 da Hoan Ton-That e Richard Schwartz a New York – a partire dal 2020 si è fatta conoscere al grande pubblico a seguito di un'inchiesta del New York Times[568] in merito al funzionamento del *software* ed al suo utilizzo dei dati biometrici per il riconoscimento facciale (*facial recognition search engine*)[569]. Il *software* – come si legge dal sito *internet* della Società[570]– non sarebbe accessibile al pubblico, ma rivolto esclusivamente a particolari categorie di destinatari, quali le forze dell'ordine o le Agenzie governative statali. Come già accennato, dall'inchiesta condotta dal New York Times[571] emerge che *Clearview* avrebbe distribuito il *software* a numerosi dipartimenti di polizia, FBI, CBP, Interpool, per un utilizzo in più di 27 Stati dell'America[572]. In realtà, tuttavia, sulla base dell'ulteriore inchiesta svolta da BuzzFeed – sito *web* di informazione – *Clearview* avrebbe venduto la propria tecnologia, e quindi l'accesso al proprio *database,* anche ad organizzazioni di tutto il mondo, comprese aziende private[573].

---

[563] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[564] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022 (doc. web. 9751323).
[565] Art. 5, par. 1, lett. a), del Regolamento.
[566] Art. 5, par. 1, lett. b), del Regolamento.
[567] Art. 5, par. 1, lett. e), del Regolamento.
[568] C. DEL KASHMIR, *The Secretive Company That Might End Privacy as We Know It*, 18 gennaio 2020, New York Times, consultabile su https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[569] J. CONDEMI, *Clearview AI: cos'è e come funziona il riconoscimento facciale*, 2 maggio 2022, Ai4business, consultabile su https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/.
[570] https://www.clearview.ai/.
[571] C. DEL KASHMIR, *The Secretive Company That Might End Privacy as We Know It*, 18 gennaio 2020, New York Times, consultabile su https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[572] *Ibidem*.
[573] R. MAC, C. HASKINS, L. MCDONALD, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, 27 febbraio 2020, consultabile su https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

La tecnologia di *machine learning* su cui si basa la piattaforma *Clearview* – denominata "*Metodo per fornire informazioni su una persona sulla base di riconoscimento facciale*" – è stata depositata per una richiesta di brevetto[574], approvata nel 2021 dal US Patent & Trademark Office e dal World Intellectual Property Organization, e proprio per ottenere tale brevetto la Società ha offerto dati tecnici precisi sul funzionamento del suo *software*[575].

In sostanza, si tratta di una piattaforma in grado di confrontare le immagini inserite oggetto della ricerca con quelle presenti nel *database*: il *software*, infatti, si avvarrebbe di un vastissimo *database* proprietario, popolato, ad oggi, da più di 10 miliardi di immagini di volti, raccolte negli anni attraverso la c.d. tecnica di *web scraping*[576]. Tale tecnica, in particolare, permette di raccogliere le immagini o i video pubblicati e presenti nel *web*, compresi quelle dei *social network* (Facebook, YouTube, Twitter etc.[577]), quelle dei *blog* o di una qualsiasi pagina *web* accessibile. Tale pratica – che in precedenza non era stata oggetto di valutazione in termini di legalità o meno – è stata giudicata, proprio in occasione della decisione del Garante su *Clearview*, come illegittima[578]. Lo *scraping*, infatti, sarebbe privo di una base giuridica che legittimi il trattamento dei dati raccolti[579]: il fatto che l'immagine o il dato siano pubblici – e, quindi, potenzialmente accessibili a tutti – non ne autorizzerebbe automaticamente la raccolta e il successivo utilizzo per scopi diversi rispetto a quelli individuati dall'interessato[580].

---

[574] J. CONDEMI, *Clearview AI: cos'è e come funziona il riconoscimento facciale*, 2 maggio 2022, Ai4business, consultabile su https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/.
[574] https://www.clearview.ai/.
[575] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[576] *Ibidem.*
[577] I gestori dei *social network* in questione, inoltre, hanno ingiunto a *Clearview* di porre fine a tale pratica di *web scraping* sulle loro piattaforme e, in riscontro a tale ingiunzione, la Società «ha replicato come la sua attività di raccolta dati sia coperta dal Primo Emendamento della Costituzione degli USA», come sottolineato in G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 178.
[578] D. DI MALTA, *Clearview AI, sanzione privacy importante ma danni irreversibili*, 10 marzo 2022, Agendadigitale.eu, consultabile su https://www.agendadigitale.eu/sicurezza/privacy/clearview-ai-sanzione-privacy-importante-ma-danni-irreversibili/.
[579] Sul punto, l'Autorità di controllo Irlandese ha sanzionato Meta per 265 milioni di euro, a seguito dell'indagine "Data Screping", per violazione del GDPR, in quanto la Società non avrebbe protetto adeguatamente i dati degli utenti di Facebook, oggetto di attacchi *hacker* mediante la tecnica di *scraping*, v. Decisione LSA del 25 novembre 2022, consultabile su https://edpb.europa.eu/news/national-news/2022/irish-supervisory-authority-announces-decision-facebook-data-scraping_en.
[580] D. DI MALTA, *Clearview AI, sanzione privacy importante ma danni irreversibili*, 10 marzo 2022, Agendadigitale.eu, consultabile su https://www.agendadigitale.eu/sicurezza/privacy/clearview-ai-sanzione-privacy-importante-ma-danni-irreversibili/.

Successivamente, le immagini raccolte mediante *web scraping* vengono elaborate dal *software* – attraverso strumenti biometrici in grado di estrarne le caratteristiche identificative – e trasformate in "rappresentazioni vettoriali" sottoposte ad *hashing* (ossia «una sorta di impronta digitale facciale»[581]) per l'indicizzazione e per la successiva ricerca[582]. *Clearview*, inoltre, permette di arricchire le immagini presenti nel *database* con le informazioni e i metadati alle stesse correlate (ad esempio, «il titolo dell'immagine o della pagina web, il link della fonte, la geolocalizzazione, il genere, la data di nascita, la nazionalità, la lingua»[583]) permettendo, una volta trovata la corrispondenza, di risalire alla pagina sorgente da cui l'immagine è stata estrapolata[584]. In definitiva, dunque, il *software* sarebbe in grado di comparare l'immagine ricercata con i modelli biometrici inseriti nel *database* e generare un processo di verifica *da uno a molti* (1-n)[585].

L'istruttoria del Garante è stata avviata su iniziativa dell'Autorità a seguito della diffusione di alcune notizie di stampa che sollevavano dubbi circa il rispetto dei dati personali degli utenti, nonché sulla base dei reclami ricevuti da alcuni cittadini italiani nel corso del 2021 nei confronti di *Clearview*[586]. Inoltre, sempre nel 2021, il Garante è stato destinatario anche di alcune segnalazioni da parte di organizzazioni a difesa della *privacy* e dei diritti fondamentali delle persone, in merito alla base giuridica del trattamento posto in essere dal *software* e alle procedure predisposte dalla Società per l'accesso agli atti[587]. Ebbene, il 9 marzo 2022, il Garante ha dato avvio alla propria attività istruttoria (prot. del Garante n. 16155/2021), con la richiesta informazioni trasmessa alla Società e la successiva notifica del provvedimento, a cui *Clearview* ha risposto presentando le proprie memorie difensive[588].

Innanzitutto, la Società ha contestato le violazioni addotte dall'Autorità adducendo la non applicabilità del Regolamento e la conseguente mancanza di giurisdizione del Garante italiano. Secondo quanto rappresentato dalla *Clearview*, infatti, l'omonimo *software,* a inizio 2019, sarebbe stato promosso dalle forze dell'ordine statunitensi,

---

[581] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[582] *Ibidem.*
[583] *Ibidem.*
[584] A. PRATOLINI, *Il Garante Privacy su Clearview AI: capire la sanzione per l'uso dei dati biometrici,* 16 marzo 2022, Industry News, consultabile su https://blog.didomi.io/it/il-garante-privacy-su-clearview-ai-capire-la-sanzione-per-luso-dei-dati-biometrici.
[585] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[586] *Ibidem.*
[587] *Ibidem*.
[588] *Ibidem*.

generando l'interesse da parte delle agenzie governative nel panorama internazionale, motivo per cui gli erano stati offerti in dotazione alcuni *account* di prova[589]. Tuttavia, la Società, a seguito dei reclami ricevuti dalle autorità di controllo europee[590], aveva provveduto alla chiusura dei suddetti *account* nonché all'implementazione di uno strumento capace di impedire al *software* l'accesso agli indirizzi IP europei[591]. In sostanza, quindi, *Clearview* ha rivendicato l'inapplicabilità del Regolamento, dal momento che non ha sedi o filiali all'interno del territorio dell'Unione europea, nè è in possesso, allo stato attuale, di elenchi di clienti italiani[592].

Da ultimo, la Società ha contestato l'assimilazione, fatta dal Garante, della propria attività a quella di "monitoraggio", così come intesa dal Regolamento[593]. Infatti, secondo quanto asserito da *Clearview*, il *software* non effettuerebbe un trattamento finalizzato all'analisi del comportamento degli utenti, né alla creazione di profili a loro riconducibili, dando luogo solamente a «un'istantanea dei risultati della ricerca al momento del compimento della stessa»[594] – non sostanziandosi la sua attività né in attività di monitoraggio né in attività di profilazione –. In particolare, con riferimento a quest'ultimo profilo, la Società ha rappresentato come «la profilazione implichi una qualche forma di valutazione o giudizio in merito a una persona. La semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza non determina necessariamente una profilazione. Quest'ultima dipende infatti dalla finalità della classificazione»*[595]* e la finalità di *Clearview* non sarebbe quella di classificare, in quanto il servizio offerto dal *software* consisterebbe esclusivamente nell'offrire una corrispondenza tra le immagini ricercate e quelle presenti nel *database* del *software*[596]. Le successive attività, una volta trovata la corrispondenza – a parere della Società – non rientrerebbero tra le attività di *Clearview*, ma in quella del cliente, con la conseguenza che gli usi che poi di tale strumento ne venissero fatti e l'eventuale rispetto della cornice normativa rimarrebbero a

[589] *Ibidem*.
[590] Anche altre Autorità europee hanno adottato provvedimenti nei confronti della Società: l'Autorità di controllo svedese (DI-2020-2719: A126.614/2020 del 10 febbraio 2021); l'Autorità di controllo ellenica, il 13 luglio 2022, con la decisione 35/2022, l'Autorità di controllo francese, il 19 ottobre 2022, con la decisione SAN-2022-019 du 17 octobre 2022.
[591] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[592] *Ibidem*.
[593] Art. 3, par. 2, lett. b) del Regolamento UE 2016/679.
[594] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[595] *Ibidem.*
[596] *Ibidem.*

carico del cliente-utilizzatore e non della Società, la quale si limita a vendere il servizio, il cui successivo uso non rientrerebbe nel proprio ambito di competenza[597].

Ciononostante, non accogliendo le difese presentate da *Clearview*, il Garante, il 10 febbraio 2022, ha provveduto ad irrogare una sanzione amministrativa pecuniaria pari a venti milioni euro nei confronti della Società[598].

Innanzitutto, il Garante ha riconosciuto la sussistenza della propria giurisdizione: infatti, pur non essendo la Società stabilita all'interno del territorio dell'Unione Europea, ricorrono – a parere dell'Autorità[599] – i criteri di cui all'art. 3, par. 2 del GDPR (c.d. criterio di *targeting*), i quali definiscono l'ambito di applicazione del Regolamento[600].

In particolare, con riferimento al primo dei criteri previsti dalla norma *de qua*, vale a dire «l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione»[601] – secondo quanto si legge nel provvedimento – *Clearview* effettuerebbe un trattamento dei dati personali di interessati italiani: ciò si evincerebbe sia dalla presenza nei *database* del *software* di immagini di italiani, elaborate biometricamente e associate ai rispettivi metadati[602], sia dalla circostanza che la Società ha in passato fornito *account* anche a clienti europei (come da essa stessa ammesso). Ad ulteriore riprova della volontà di *Clearview* di offrire i propri servizi anche a clienti europei, l'Autorità ha rilevato che la stessa *privacy policy* predisposta dalla Società, prima del 20 marzo 2021 – ossia, prima della richiesta avanzata dal Garante – menzionava una serie di indicatori espressione della volontà della Società di offrire i propri servizi anche al mercato europeo[603].

Quanto al secondo dei criteri previsti dall'art. 3, par. 2, del Regolamento, vale a dire il «monitoraggio» del comportamento degli interessati «nella misura in cui tale comportamento ha luogo all'interno dell'Unione»[604], il Garante ha ritenuto che l'attività svolta dalla piattaforma possa essere ricondotta in quella di "monitoraggio": secondo

[597] *Ibidem.*
[598] *Ibidem.*
[599] *Ibidem.*
[600] A norma dell'art. 3, par. 2 del Regolamento, «Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione , indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nell'Unione».
[601] Art. 3, par. 2, lett. a), Regolamento.
[602] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[603] *Ibidem*.
[604] Art. 3, par. 2, lett. b) del Regolamento.

quanto si legge nel provvedimento dell'Autorità, «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su *Internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali»[605]. Or dunque, sulla base dell'analisi condotta dal Garante in merito al funzionamento di *Clearview*, l'attività posta in essere dal *software* sarebbe assimilabile a quella di monitoraggio e anche di profilazione[606], proprio in considerazione della rielaborazione tecnica delle immagini per la trasformazione in dati biometrici e della conseguente estrazione dei profili corrispondenti a quelli dell'immagine caricata dall'utente[607].

Da ultimo, con riferimento alla sussistenza di un trattamento di dati biometrici, secondo il Garante, l'immagine fotografica può assurgere a "dato personale"[608] nella misura in cui permette l'identificazione della persona[609], mentre, invero, assurge a "dato biometrico" nella misura in cui, attraverso un trattamento tecnico, permette l'individuazione delle caratteristiche fisiche, fisiologiche o comportamentali che ne consentono l'identificazione univoca[610]. Come ampiamente illustrato nel Secondo Capitolo[611], dunque, i due tipi di dati si differenziano – secondo quanto sottolineato dal Considerando n. 51 del Regolamento – in quanto «il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica»[612]. A parere del Garante, tuttavia,

---

[605] Considerando n. 24 del Regolamento.
[606] Sulla base delle Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione, adottate dal Comitato per la protezione dei dati personali il 3 ottobre 2017 ed emendato il 6 febbraio 2018, «la diffusa disponibilità di dati personali su Internet e di quelli ricavabili dai dispositivi di Internet delle cose, associata alla capacità di trovare correlazioni e creare collegamenti, può consentire la determinazione, l'analisi e la previsione di aspetti della personalità, del comportamento, degli interessi e delle abitudini di una persona. Le Linee guida citate individuano tre fasi specifiche che caratterizzano l'attività di profilazione stabilendo che debba a) riguardare dati personali, b) essere una forma di trattamento automatizzato e c) essere finalizzata a valutare aspetti personali relativi a una persona fisica».
[607] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[608] Art. 4, par. 1, n. 1), del Regolamento UE 2016/679.
[609] Sul punto è intervenuta anche la Corte di Giustizia dell'Unione Europea: «l'immagine di una persona registrata da una telecamera costituisce un dato personale […] se e in quanto essa consente di identificare la persona interessata» (*cfr*. sentenza 11 dicembre 2014, causa C-212/13, par. 22).
[610] Art. 4, par. 1, n. 14), del Regolamento.
[611] Si veda, *amplius,* il paragrafo §2.1.1 riportato nel Secondo Capitolo.
[612] Considerando n. 51 del Regolamento.

l'attività di *web scraping* effettuata dal *software* – oltre ad essere per la maggior parte dei casi vietata ai gestori delle piattaforme *social* mediante clausole espresse nei termini di servizio – sarebbe a tutti gli effetti un trattamento dei dati biometrici e, in quanto tale, necessiterebbe della legittimazione in una delle basi giuridiche previste dall'art. 6 del Regolamento, carente nel caso di specie.

Occorre, inoltre, segnalare che, sulla base della legge 205/2021 (c.d. "decreto capienze"), è previsto il divieto di utilizzo dei sistemi biometrici di riconoscimento facciale in luoghi pubblici o aperti al pubblico fino al 31 dicembre 2023.

Infine, il Garante ha contestato alla Società la violazione dei principi di liceità, correttezza e trasparenza nel trattamento dei dati nei confronti dell'interessato[613]: gli interessati, infatti, non sarebbero in alcun modo informati dell'attività posta in essere dalla *Clearview*, né direttamente né indirettamente mediante consultazione del sito *web*[614]. Inoltre, è stata contestata alla Società la violazione del principio di limitazione della finalità[615]: la natura pubblica delle immagini, infatti, non sarebbe sufficiente a far sì che gli interessati possano ragionevolmente attendersi che le stesse vengano utilizzate da una piattaforma privata per finalità di riconoscimento facciale[616]; nonché la violazione del principio di conservazione[617]: la Società non avrebbe stabilito alcun periodo di conservazione dei dati biometrici, e tale circostanza – a parere del Garante – lascerebbe presupporre un trattamento a tempo indeterminato dei dati raccolti[618].

In conclusione, per i motivi illustrati, il trattamento dei dati biometrici posto in essere da *Clearview* non sarebbe in alcun modo legittimo.

Il Garante, infine, ha imposto alla società, quali misure correttive addizionali, «un divieto del trattamento, consistente nel i) divieto di ulteriore raccolta, mediante tecniche di *web scraping*, di immagini e relativi metadati concernenti persone che si trovano nel territorio italiano; ii) divieto di ogni ulteriore operazione di trattamento dei dati, comuni e biometrici, elaborati dalla Società attraverso il suo sistema di riconoscimento facciale

[613] Art. 5, par. 1, lett. a), del Regolamento.
[614] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[615] Art. 5, par. 1, lett. b), del Regolamento UE 2016/679.
[616] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).
[617] Art. 5, par. 1, lett. e), del Regolamento UE 2016/679.
[618] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).

relativi a persone che si trovano nel territorio italiano»[619], nonché l'ordine di cancellazione di tutti i dati raccolti in violazione del Regolamento e il divieto di raccolta e trattamento ulteriori[620].

Parallelamente all'istruttoria avviata dall'Autorità italiana, a partire da maggio 202, la CNIL – l'Autorità francese per la protezione dei dati – ha avviato una propria indagine nei confronti di *Clearview,* invitando il 26 novembre 202 la Società a cessare la raccolta e l'utilizzo dei dati delle persone sul territorio francese in assenza di una base giuridica. Inoltre, alla Società è stato intimato di facilitare l'esercizio dei diritti delle persone con riferimento alle richieste di cancellazione. In ragione del mancato riscontro da parte di *Clearview* all'intimazione *de quo,* il 17 ottobre 2022 il Comitato ristretto dell'Autorità francese ha aggiunto una sanzione di 100.000 euro per ogni giorno di ritardo nell'adempimento. Le violazioni addebitate dall'Autorità a *Clearview* si sostanziano nel trattamento illecito dei dati personali (art. 6 GDPR), nel mancato rispetto dei diritti delle persone fisiche (artt. 12, 15 e 17 GDPR) e nella mancata cooperazione con la CNIL (art. 31 GDPR)[621].

### 3.2.5. Ordinanza ingiunzione nei confronti di Sportitalia: è illecito il trattamento dei dati biometrici effettuato sul personale dipendente (10 novembre 2022)

Come già accennato, in data 10 novembre 2022, l'Autorità Garante per la protezione dei dati personali ha emesso nei confronti della società sportiva dilettantistica a responsabilità limitata Sportitalia (di seguito anche, la "Società") un'ordinanza di ingiunzione al pagamento di una sanzione amministrativa pecuniaria di euro ventimila[622], in quanto la Società, in qualità di titolare, ha effettuato un trattamento dei dati biometrici dei propri dipendenti in assenza di una base giuridica legittima e in violazione del principio di proporzionalità e di minimizzazione dei dati personali[623]; inoltre, la Società ha ommesso di dare riscontro alla richiesta di informazioni notificata dal Garante

[619] *Ibidem.*
[620] *Ibidem.*
[621] CNIL, *Riconoscimento facciale: sanzione di 20 milioni di euro contro CLEARVIEW AI*, 20 ottobre 2022, consultabile in https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai.
[622] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022 (doc. web. 9832838).
[623] C. FIORE [2023], *Garante privacy: sanzionata una società per il trattamento dei dati biometrici dei propri lavoratori,* Diritto al Digitale, 13 aprile 2023, consultabile su https://dirittoaldigitale.com/2023/04/13/trattamento-dati-biometrici/.

dapprima in data 5 settembre 2019 e, non essendo pervenuta alcuna risposta, successivamente in data 10 gennaio 2020[624].

Più nello specifico, l'istruttoria dell'Autorità è stata avviata a seguito di una segnalazione pervenuta in data 15 maggio 2019 dalla SLC CGIL (Sindacato Lavoratori della Comunicazione) a seguito dell'introduzione da parte di Sportitalia di un sistema per la rilevazione delle presenze, attraverso un terminale biometrico in grado di rilevare le impronte digitali, utilizzato per la registrazione degli accessi e delle uscite dall'azienda da parte del personale dipendente[625]. In particolare, l'organizzazione sindacale, nella segnalazione, ha rappresentato che, a partire da ottobre 2018, presso le palestre milenesi – Club Get Fit – gestite della Società, erano stati introdotti sistemi di «timbratura per rilevazione delle presenze, con terminale biometrico (rilevamento delle impronte digitali)»[626], nonostante la richiesta dello stesso sindacato di utilizzare degli strumenti di rilevazione delle presenze «meno invasivi – scegliendo procedimenti non biometrici»[627] nei confronti degli oltre 130 dipendenti e collaboratori in essere alla Società[628].

Nell'attività svolta dal Garante, effettuata anche mediante accessi ispettivi svoltisi nei giorni 28, 29 e 30 settembre 2021, è stato dichiarato dai referenti della Società che il requisito di liceità dei trattamenti «si fonda sul consenso specifico e libero espresso da parte di ogni singolo dipendente»[629]; tale consenso, a parere della Sportitalia, sarebbe stato acquisito nel documento "Informativa sulla privacy per i dipendenti"[630], mediante la sottoscrizione per presa visione e consenso al trattamento dei dati biometrici, ad opera del personale dipendente sottoposto al trattamento. Nondimeno, dopo l'avvio dell'istruttoria da parte del Garante, la Società ha dichiarato la volontà di interrompere, a

---

[624] PORTALE CONSULENTI [2023], *Impronte digitali senza specifici requisiti*, 9 gennaio 2023, consultabile su https://www.portaleconsulenti.it/impronte-digitali-senza-specifici-requisiti/.
[625] WIKILABOUR [2022], *Garante per la protezione dei dati personali, ordinanza ingiunzione contro Sportitalia ssd,* 10 novembre 2022, consultabile su https://www.wikilabour.it/segnalazioni/privacy/garante-per-la-protezione-dei-dati-personali-ordinanza-ingiunzione-contro-sportitalia-ssd/.
[626] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy*, consultabile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842.
[627] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022 (doc. web. 9832838).
[628] PORTALE CONSULENTI [2023], *Impronte digitali senza specifici requisiti*, 9 gennaio 2023, consultabile su https://www.portaleconsulenti.it/impronte-digitali-senza-specifici-requisiti/.
[629] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022 (doc. web. 9832838).
[630] *Ibidem*.

partire dal 2 maggio 2022, il sistema di rilevazione delle impronte e provvedere contestualmente alla cancellazione dei dati raccolti[631].

A livello tecnico, la tecnologia di rilevazione dei dati biometrici prodotta dalla Kronotech s.r.l. e fornita da Cronos s.r.l. alla Sportitalia, tratterebbe «unicamente il modello biometrico (*template*) che viene creato a seguito di elaborazione all'atto della registrazione dell'account identificativo biometrico di ogni utente»[632] attraverso una modalità di confronto, al momento dell'autenticazione, di tipo "uno a molti" (1-n).

L'istruttoria del Garante, analizzata la documentazione acquisita e le dichiarazioni rese da Sportitalia, si è conclusa con l'addebito in capo alla Società di diverse violazioni del Regolamento europeo sulla protezione dei dati personali.

In particolare, l'Autorità ha contestato alla Sportitalia la non conformità del trattamento dei dati biometrici effettuato sui propri dipendenti: per la violazione degli artt. 5, par. 1, lett. a) e 9 del Regolamento, in ragione della mancanza di una base giuridica idonea ad autorizzare l'utilizzo dei dati biometrici da parte della Società[633], nonché per la non conformità rispetto ai principi di proporzionalità e minimizzazione del trattamento nell'utilizzo del dato biometrico nel contesto dell'ordinaria gestione del rapporto di lavoro[634].

In secondo luogo, il Garante ha contestato alla Società la violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento, ritenendo che la Società abbia fornito ai dipendenti esclusivamente il documento "Informativa sulla privacy per i dipendenti" il quale, a parere dell'Autorità, appare del tutto inidoneo a rappresentare in maniera lecita, corretta e trasparente le caratteristiche del trattamento effettuato attraverso gli strumenti biometrici, anche per l'assenza nel documento *de quo* di qualsiasi riferimento alla

---

631 *Ibidem.*

632 *Ibidem.*

633 Il Garante, infatti, già in altri provvedimenti aveva stabilito che «il consenso del lavoratore non costituisce, di regola, un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro, ciò alla luce della asimmetria tra le rispettive parti del rapporto di lavoro e la conseguente, eventuale, necessità di accertare di volta in volta e in concreto l'effettiva libertà della manifestazione di volontà del dipendente» (si vedano, tra gli altri, i provv.ti n. 16 del 14 gennaio 2021, doc. web n. 9542071; n. 35 del 13 febbraio 2020, doc. web n. 9285411; n. 500 del 13 dicembre 2018, doc. web n. 9068983; v. altresì artt. 6-7 e considerando 42-43, Regolamento (UE) 2016/679; vedi, altresì, in senso conforme, GRUPPO DI LAVORO ARTICOLO 29, *Linee Guida sul consenso ai sensi del Regolamento UE 2016/679,* WP 259, 4 maggio 2020, spec. par. 3.1.1.; GRUPPO DI LAVORO ARTICOLO 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro,* WP 249, 8 giugno 2017, spec. par. 3.1.1 e 6.2).

634 GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022 (doc. web. 9832838).

possibilità da parte del dipendente di avvalersi di strumenti alternativi di rilevazione della presenza (*badge*) o di poter revocare il consenso prestato[635].

Inoltre, il Garante ha contestato alla Società la violazione dell'art. 30, par. 1, lett. c) del Regolamento, ritenendo che Sportitalia abbia omesso di indicare i dati biometrici all'interno del registro delle operazioni di trattamento[636].

Da ultimo, l'Autorità ha contestato a Sportitalia la violazione dell'art. 157 in relazione a quanto previsto dall'art. 166, comma 2, del Codice, in quanto la Società non fornito al Garante il riscontro alle richieste di informazioni trasmesse da quest'ultima, nonostante la regolare notifica[637].

### 3.2.6. L'autorità Garante apre un'istruttoria nei confronti dei Comuni di Lecce e Arezzo sui sistemi di sorveglianza intelligente (14 novembre 2022)

Ancora con riferimento agli usi sempre più frequenti da parte delle amministrazioni pubbliche delle TRF, il Garante della *privacy*, con il comunicato stampa del 14 novembre 2022[638], informava dell'apertura di due istruttorie, rispettivamente nei confronti dei Comuni di Lecce e di Arezzo, in merito ai progetti avviati da questi ultimi per l'utilizzo di videosorveglianze intelligenti in spazi pubblici.

Quanto al Comune di Lecce, l'amministrazione comunale aveva annunciato l'avvio di un sistema di riconoscimento facciale, mediante l'installazione di "18 telecamere con riconoscimento facciale in punti strategici della città"[639]. A seguito della diffusione della notizia, il Garante per la protezione dei dati personali richiedeva al Comune in questione di fornire i dettagli relativi alle tecnologie utilizzate, alle finalità e alle basi giuridiche del trattamento e alle banche dati consultate dal sistema, nonché il documento sulla valutazione d'impatto sulla protezione dei dati (c.d. DPIA) [640], prevista come obbligatoria

---

[635] *Ibidem.*
[636] *Ibidem.*
[637] *Ibidem.*
[638] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282),
[639] S. DE CESAREbocco [2022], *In arrivo 18 telecamere con riconoscimento facciale: posizionate in punti strategici della città*, Quotidiano di Puglia, Giovedì 10 novembre 2022, https://www.quotidianodipuglia.it/lecce/lecce_telecamere_riconoscimento_facciale_dove_a_cosa_servono_cosa_cambia-7043768.html?refresh_ce.
[640] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282).

in tutti i casi di «sorveglianza sistematica su larga scala di una zona accessibile al pubblico»[641]. Il Garante, nel comunicare l'avvio dell'istruttoria, precisava, inoltre, che «in base alla normativa europea e nazionale il trattamento di dati personali realizzato da soggetti pubblici, mediante dispositivi video, è generalmente ammesso se necessario per l'esecuzione di un compito di interesse pubblico o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri» o «a condizione che venga stipulato il cosiddetto patto per la sicurezza urbana tra Sindaco e Prefettura»[642].

L'Autorità, nondimeno, dopo aver analizzato i documenti e le controdeduzioni trasmesse dall'Ente, ha espresso parere favorevole nei confronti dei sistemi di videosorveglianza installati dal Comune di Lecce, chiudendo l'istruttoria preliminare senza assumere provvedimenti, in ragione della circostanza che le telecamere installate sul territorio comunale non si baserebbero su tecnologie di riconoscimento facciale: pur trattandosi di sistemi "avanzati", tali dispositivi," non sarebbero predisposti per l'analisi dei dati biometrici[643].

Parallelamente, il Garante ha avviato un'istruttoria nei confronti del Comune di Arezzo che, a far data dal 1° dicembre 2022, si preparava alla sperimentazione del progetto pilota per l'utilizzo di occhiali a infrarossi, offerti in dotazione agli agenti di Polizia Municipale a garanzia della sicurezza delle strade e per il controllo del territorio. Infatti, con il comunicato stampa del 10 novembre 2022[644], il Comune di Arezzo presentava il dispositivo *"laBglasses"* come un sistema integrato di visore e telecamere, ideato per rilevare le targhe dei veicoli e al contempo verificare la validità dei documenti degli utenti: «Sono occhiali "speciali" che grazie al software URBANO 2.0, integrato nel device abbinato al sistema, consentono l'accesso alle principali banche dati e l'acquisizione in tempo reale delle informazioni richieste che saranno impresse direttamente sul visore oculare. Grazie ai *laBGlasses* sarà inoltre possibile effettuare foto

[641] Art. 35, par. 3, lett. b) del GDPR – Valutazione d'impatto sulla protezione dei dati.
[642] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282).
[643] Città di Lecce, *Telecamere di videosorveglianza: il Garante chiude l'istruttoria preliminare*, 1 dicembre 2022, https://www.comune.lecce.it/news/dettaglio/2022/12/01/telecamere-di-videosorveglianza-il-garante-chiude-l-istruttoria-preliminare.
[644] Comune di Arezzo, *La Polizia Municipale di Arezzo protagonista del progetto pilota di sperimentazione Sicurezza sulla strada: occhiali "speciali" in dotazione agli agenti*, Comunicato stampa del 10 Novembre 2022, https://www.comune.arezzo.it/notizie/polizia-municipale-arezzo-protagonista-del-progetto-pilota-sperimentazione-sicurezza-sulla.

e/o segnalazioni georeferenziate, per immortalare, ad esempio, immagini di sinistri stradali»[645].

Anche in questo caso, il Garante richiedeva all'amministrazione di fornire la valutazione d'impatto sul trattamento dei dati[646], nonché i dettagli dell'informativa resa agli interessati, sia con riferimento ai cittadini che al personale di Polizia a cui sarebbero stati destinati gli occhiali ad infrarossi per il controllo delle strade[647].

In Italia, infatti, fino all'entrata in vigore di una legge *ad hoc* e, in ogni caso, fino al 31 dicembre 2023 non è consentito l'utilizzo di sistemi di riconoscimento facciale che si basano sul trattamento di dati biometrici, salvo che tale trattamento «non sia effettuato per indagini della magistratura o prevenzione e repressione dei reati»[648]. Inoltre, la moratoria non riguarda neppure i trattamenti di dati biometrici «effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione delle sanzioni penali» previste al d.lgs. n. 51/2018, a condizione che sia espresso parere favorevole da parte del Garante per la protezione dei dati personali[649].

### 3.3. L'orientamento del Comitato europeo per la protezione dei dati personali sulle TRF

Il Gruppo di lavoro "Articolo 29" – ora Comitato europeo per la protezione dei dati – è storicamente piuttosto scettico sulle funzionalità offerte dai sistemi biometrici: già nel *Documento di lavoro sulla biometria* (1° agosto 2003), il Gruppo di lavoro aveva affermato che fosse necessario individuare con precisione le finalità del ricorso ai sistemi biometrici e valutare se il medesimo scopo potesse essere conseguito mediante «modalità

[645] Comune di Arezzo, *La Polizia Municipale di Arezzo protagonista del progetto pilota di sperimentazione Sicurezza sulla strada: occhiali "speciali" in dotazione agli agenti*, Comunicato stampa del 10 Novembre 2022, https://www.comune.arezzo.it/notizie/polizia-municipale-arezzo-protagonista-del-progetto-pilota-sperimentazione-sicurezza-sulla.
[646] Art. 35, par. 3, lett. b) del GDPR – Valutazione d'impatto sulla protezione dei dati.
[647] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282).
[648] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282).
[649] Art. 1, c. 12 del Decreto Capienze. Del Decreto Capienze abbiamo parlato nel Secondo Capitolo, al paragrafo §2.2.4.

meno invasive»[650], suggerendo altrove[651] i vari passaggi da attuare per verificare l'adeguatezza di un sistema biometrico: innanzitutto, occorre valutare se tale sistema sia «inevitabile» per il soddisfacimento dello scopo prefissato, nella duplice accezione di essenziale e conveniente dal punto di vista economico; in secondo luogo, bisogna valutare la «potenziale efficacia» del sistema rispetto al raggiungimento di tale finalità, considerate le sue peculiarità e le sue caratteristiche intrinseche; il terzo fattore da considerare è se la perdita di riservatezza conseguente all'uso del sistema biometrico sia «proporzionata» rispetto al vantaggio atteso; infine, occorre accertare se un altro «mezzo meno invasivo» della riservatezza potrebbe raggiungere il medesimo scopo[652].

Ancora una volta, materia elettiva di riflessione del Gruppo di Lavoro "Articolo 29" è costituita dal monitoraggio video e videosorveglianza dei lavoratori: attraverso i sistemi di riconoscimento facciale, il datore di lavoro può controllare, avvalendosi di mezzi automatizzati, le espressioni facciali del lavoratore e «acquisire informazioni sul comportamento del lavoratore», «al fine di individuare deviazione da modelli di movimento predefiniti»[653]. In definitiva, l'uso delle TRF sarebbe sproporzionato «nei confronti dei diritti e delle libertà dei dipendenti», motivo il per quale esse non possono trasformarsi nella modalità normale di controllo[654]. Nonostante dichiari tendenzialmente illecito ricorrere a tali tecnologie, il Gruppo di lavoro "Articolo 29" pare aperto a riconoscere l'esistenza di alcune eccezioni a questa regola generale, le quali tuttavia non possono essere utilizzate per fondare una legittimazione generale di tali sistemi biometrici[655].

In linea di continuità con i precedenti orientamenti, più recentemente il Comitato europeo per la protezione de dati ha osservato che l'uso dei dati biometrici volti ad identificare in modo univoco una persona fisica – tra cui spicca il riconoscimento facciale – comporta notevoli rischi per i diritti e le libertà degli interessati, per cui il titolare del

[650] GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* WP 80, 1° agosto 2003.
[651] GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche,* WP193, 27 aprile 2012.
[652] *Ibidem.* Vedi anche G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021, 165.
[653] GRUPPO DI LAVORO ARTICOLO 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro,* WP249, 8 giugno 2017, 22.
[654] *Ibidem.*
[655] *Ibidem.*

trattamento deve sempre valutare l'impatto su tali diritti e considerare di utilizzare «mezzi meno intrusivi per raggiungere il legittimo scopo del rispettivo trattamento»[656].

Da ultimo, il 12 maggio 2022, il Comitato europeo ha emanato le Linee Guida n. 5/2002, con le quali ha affrontato la delicata questione relativa all'uso del riconoscimento facciale nell'ambito delle autorità competenti in materia di prevenzione, indagine, accertamento e perseguimento dei reati[657], ove sono confermati e ampliati orientamenti e preoccupazioni già emersi in seno all'Autorità *de qua*.

Dopo aver tratteggiato le caratteristiche e gli usi principali delle TRF[658] – questioni su cui ci siamo intrattenuti ripetutamente nei Capitoli precedenti – l'EDPB osserva che le TRF costituiscono importanti strumenti per le autorità competenti (*law enforcement authorities*, c.d. LEAs), definite come autorità esecutive dotate di poteri che dipendono dagli Stati sovrani[659]. Ciononostante, anche quando impiegate dalle forze dell'ordine, esse «sono in grado di incidere sulla nostra stabilità politica, sociale e democratica», dal momento che rischiano di pregiudicare diritti fondamentali dell'uomo[660].

Di conseguenza, affinché l'uso del riconoscimento facciale sia lecito, è necessario rispettare i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della propria vita privata e familiare di cui all'art. 7 della Carta, il diritto alla protezione dei dati di carattere personale che lo

---

[656] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020.
[657] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nell'ambito delle forze dell'ordine,* 12 maggio 2022.
[658] In particolare, in COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida* cit., 7 ss, l'EDPB definisce espressamente le TRF come una «tecnologia probabilistica in grado di riconoscere automaticamente gli individui in base al volto con scopi di autenticazione o di identificazione»; ribadisce, inoltre, che tale tecnologia – la quale sfrutta componenti di Intelligenza Artificiale o di machine learning – rientra nel novero delle tecniche biometriche, le quali comprendono tutti i processi automatizzati per riconoscere un individuo sulla base delle caratteristiche fisiche, fisiologiche o comportamentali, quali impronte digitali, struttura dell'iride, voce, pattern dei vasi sanguigni; inoltre, dopo aver operato una ricognizione delle diverse fasi in cui si articola il procedimento biometrico, il Comitato europeo ricorda che la tecnologia in discorso presenta – attualmente o in fase di sperimentazione – notevoli varietà di applicazioni, tanto di natura commerciale quanto di natura pubblicistica, sia per accesso ad un luogo specifico (c.d. filtraggio specifico o *phisical filtering*) sia senza alcuna limitazione nello spazio pubblico (c.d. riconoscimento facciale in tempo reale o *live facial recognition*): a titolo meramente esemplificativo, il Comitato europeo menziona l'accesso a servizi o applicazioni nell'ambito di un ambiente domestico; ricerca, in un database di fotografie, dell'identità di una persona fisica non identificata (vittima, indagato, persona scomparsa); monitoraggio dei movimenti della persona in caso di accesso ad un servizio pubblico o privato o ad un luogo specifico; ricostruzione del percorso intrapreso da una persona e le sue successive interazioni con altre persone; tracciamento del viaggio di un passeggero. Si veda anche G. BORGHI, *Riconoscimento facciale e Polizia: le linee guida n. 5/2022 dell'EDPB,* in *Il Quotidiano Giuridico,* 23 giugno 2022, 2.
[659] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nell'ambito delle forze dell'ordine,* 12 maggio 2022, 3.
[660] *Ibidem.*

riguardano di cui all'art. 8 della Carta, nonché il rispetto della dignità, della libertà di pensiero, di coscienza, di religione e di associazione sanciti agli artt. 1, 10, 11 e 12 della Carta[661].

In secondo luogo, il Comitato europeo enuclea principi volti a salvaguardare i cittadini da eventuali abusi delle autorità competenti in materia di prevenzione, indagine, accertamento e perseguimento dei reati: costituendo il trattamento dei dati biometrici una grave interferenza *in re ipsa*, non connessa soltanto all'esito di un *matching* positivo, l'art. 52 della CDFUE – da leggersi congiuntamente all'art. 8 della CEDU – impone che, in ossequio al principio di legalità, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali riconosciute dalla Carta debbano essere previste dalla legge e rispettare l'essenza di tali diritti e libertà[662].

Il principio di legalità sarebbe rispettato nella forma, ma eluso nella sostanza qualora la legge che individui tali limitazioni le configurasse in termini così generici che il cittadino non sia in grado di individuare con sufficiente precisione il comportamento consentito alle autorità competenti. È immanente al principio di legalità il principio di sufficiente determinatezza della base giuridica: la base giuridica individuata dal legislatore deve essere sufficientemente precisa e chiara nei suoi termini, in modo tale da costituire un'indicazione specifica delle condizioni e delle circostanze in cui le autorità sono autorizzate a ricorrere alla raccolta di dati per motivi di sorveglianza[663]. Una mera trasposizione nel diritto interno della clausola generale prevista all'art. 10 LED non sarebbe in grado di integrare tali principi, mancando di precisione e prevedibilità[664].

Quanto all'essenza di tali diritti e libertà, il Comitato europeo sottolinea la necessità di rispettare il nucleo essenziale del diritto, rifuggendo da interpretazioni eccessivamente formali[665].

---

[661] *Ivi,* 12 ss.
[662] *Ivi,* 13.
[663] *Ibidem*.
[664] *Ivi*, 3.
[665] In COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida* cit., 14, sono indicati anche gli indizi di una potenziale violazione dell'essenza del diritto: i) una disposizione che impone limitazioni indipendentemente dalla condotta individuale di una persona o di circostanze eccezionali; ii) il diritto non può essere azionato davanti ad un giudice; iii) prima di una rigida limitazione ai diritti sanciti dalla Carta, non sono prese in considerazione le specifiche condizioni in cui si trova l'interessato; iv) è prevista una raccolta ampia e indiscriminata, con successiva conservazione, dei dati personali e dei metadati riferibili ad una persona che usufruisce di un servizio.

Inoltre, è necessario che le limitazioni ai diritti fondamentali – sempreché siano proporzionate, appropriate e strettamente necessarie[666] – siano finalizzate al perseguimento di obiettivi di interesse generale riconosciuti dall'Unione europea ovvero alla protezione dei diritti fondamentali e delle libertà altrui. Detto in diversi termini, i reati da perseguire devono essere gravi al punto tale da giustificare le limitazioni dei diritti fondamentali riconosciuti dalla Carta, in modo da evitare un sistematico e generalizzato trattamento di dati personali[667].

Quanto al quadro giuridico specifico da applicare, a fini di protezione dei dati biometrici nell'ambito delle forze dell'ordine, devono essere anzitutto soddisfatti i requisiti sanciti dalla LED, in particolare l'art. 3, par. 13 LED (che contiene la definizione di «dato biometrico»); l'art. 4 LED (che enuclea i principi relativi al trattamento dei dati personali); l'art. 8 LED (che si occupa della liceità del trattamento); l'art. 10 LED (dedicato al trattamento di categorie particolari di dati); l'art. 11 LED (che si riferisce al processo decisionale automatizzato)[668].

Più precisamente, l'art. 8 della LED vuole che il trattamento di dati personali è lecito solamente nella misura in cui è necessario per il perseguimento delle finalità indicate nell'art. 1, par. 1 (vale a dire prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica), purchè sia disciplinato da una legge nazionale, che specifichi quantomeno gli obiettivi del trattamento, i dati personali da trattare e le specifiche finalità del trattamento. Strettamente connesso a tale norma è l'art. 10 della LED – dedicato ad una *species* del *genus* dati personali – il quale stabilisce che il trattamento delle «categorie particolari di dati personali», nell'ambito delle quali rientrano i dati biometrici estratti dalle TRF, è autorizzato solamente se i) strettamente necessario; ii) presidiato da adeguate garanzie per i diritti e le libertà dell'interessato; iii) previsto dal diritto dell'Unione o dello Stato membro; iv) necessario per salvaguardare un interesse vitale dell'interessato o di altra persona fisica; v) riguardante dati resi manifestamente pubblici dall'interessato.

Quanto al requisito della stretta necessità *sub* i), il Comitato europeo sottolinea che il trattamento dei dati biometrici deve avvenire in condizioni ancora più rigorose rispetto a quelle cui è consentito il trattamento dei dati personali comuni. Inoltre, leggendo tale

[666] Riecheggia il principio di proporzionalità, più volte esaminato nel corso della presente trattazione.
[667] *Ivi*, 13 ss.
[668] *Ivi*, 3.

norma in combinato disposto con il Considerando n. 33 della LED, la riserva di legge *sub* iii) non esclude necessariamente che fonti normative secondarie concorrano a configurare le condizioni in cui è consentito il trattamento di dati biometrici. Da ultimo, quanto al punto *sub* v), si osserva che la circostanza che una fotografia sia stata manifestamente resa pubblica dall'interessato, ad esempio sui *social network,* non implica di per sé che i relativi dati biometrici siano stati resi pubblici, motivo per cui anche in questo caso deve essere raccolto il consenso dell'interessato[669].

Peraltro, considerati i rischi intrinseci che disvelano le TRF, prima che il legislatore nazionale emani una base giuridica idonea al trattamento dei dati biometrici mediante riconoscimento facciale, è obbligatorio esperire una valutazione d'impatto sulla protezione dei dati personali (c.d. DPIA) – che il Comitato europeo raccomanda di rendere pubblica quale misura di rafforzamento del clima di fiducia e di trasparenza da parte dei cittadini – mentre costituisce una mera facoltà dello Stato membro la consultazione preventiva dell'autorità di controllo competente in materia di protezione dei dati personali, pur essendo anche tale adempimento fortemente consigliato[670].

In aggiunta, considerato che spesso il riconoscimento facciale estrae dati biometrici senza alcuna interazione con l'interessato, il procedimento di riconoscimento facciale è subordinato al previo adempimento degli obblighi informativi che gravano in capo al titolare del trattamento di cui all'art. 13 della LED[671].

Oltre a quanto detto, il Comitato europeo si occupa anche del processo decisionale automatizzato: qualora una decisione sia adottata esclusivamente sulla base del responso della tecnologia di riconoscimento facciale – circostanza ammessa solamente nei casi in cui siano previste adeguate garanzie a tutela dei diritti e delle libertà degli interessati – quest'ultimi devono essere informati sulle caratteristiche del processo decisionale *de quo*[672].

Da ultimo, ai fini del rispetto del principio di *privacy by design* e *privacy by default*[673], costituisce un importante strumento a presidio della liceità del trattamento la

[669] *Ivi,* 19.
[670] *Ivi,* 24.
[671] *Ivi*, 19 e 20.
[672] *Ivi,* 20. Si osserva come, *in apicibus,* l'art. 11 della LED contenga un generale divieto a che una decisione sia fondata esclusivamente su un trattamento automatizzato, salvi i casi espressamente previsti e disciplinati dal diritto dell'Unione o da una legge nazionale.
[673] Art. 25 del GDPR – Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita.

registrazione: è opportuno che nei sistemi automatizzati di riconoscimento facciale siano registrate le varie operazioni di trattamento dei dati personali, quali raccolta, modifica, consultazione, divulgazione, trasferimento, combinazione, cancellazione, tentativi di identificazione o verifica e i relativi esiti e punteggi di affidabilità[674].

In sede conclusiva, l'EDPB mette in luce, ancora una volta, le ambivalenze delle TRF: per un verso, non si possono disconoscere i pregi delle nuove tecnologie, che certamente costituiscono uno strumento importante nelle mani delle forze dell'ordine per identificare in maniera rapida gli autori di atti terroristici e di altri gravi reati; per altro verso, il Comitato europeo mette in guardia gli operatori del settore, sottolineando che le moderne tecnologie non sono affatto un «proiettile d'argento»: dal momento che il riconoscimento biometrico può generare falsi positivi e, di conseguenza, comportare discriminazioni, alcune tipologie di riconoscimento facciale presentano «rischi inaccettabilmente elevati per gli individui e per la società (le c.d. linee rosse)», che non trovano spazio in una società democratica[675].

Non a caso, il Comitato europeo ribadisce il suo orientamento di granitica chiusura verso determinati tipi di trattamento di dati biometrici, che – in una richiesta congiunta con quella del GEPD – aveva già chiesto di vietare[676]: i) identificazione biometrica remota delle persone in spazi aperti al pubblico; ii) sistemi di riconoscimento facciale supportati dall'Intelligenza artificiale che operano una categorizzazione delle persone sulla base della loro etnia, genere, orientamento politico o sessuale; iii) uso del riconoscimento facciale *et similia* per dedurre le emozioni di una persona fisica; iv) trattamento di dati personali in occasione dell'applicazione della legge che si basa su una banca dati costruita con dati personali raccolti su larga scala e in modo indiscriminato, come ad esempio il *web scraping* di fotografie e immagini del volto disponibili sui *social network*[677].

---

[674] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida* cit., 25.
[675] *Ivi*, 26.
[676] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI E GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento e del Consiglio che stabilisce regole di armonizzazione sull'Intelligenza Artificiale,* 18 giugno 2021. Si veda, *amplius,* nel Primo Capitolo, il paragrafo §1.2.2. reso a commento del parere congiunto *de quo.*
[677] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nell'ambito delle forze dell'ordine,* 12 maggio 2022, 26.

# CAPITOLO QUARTO

# DAL *PANOPTICON* BENTHAMIANO AL PANOTTICO DIGITALE: LA SOCIETA' DELLA SORVEGLIANZA

## 4.1.La biopolitica: la sorveglianza sul corpo

### 4.1.1. *(Segue):* Dal supplizio alla punizione: il corpo è da sempre bersaglio del potere

Nel suo saggio *"Sorvegliare e punire: nascita della prigione"*, il filosofo e storico francese Michel Foucault mette a fuoco il passaggio storico dal vecchio codice della sovranità, in cui il potere regio esercita sui sudditi il diritto di vita o di morte, ad un nuovo codice biopolitico, che origina dalla società disciplinare, in cui al potere è attribuito il diritto di individuare, incasellare, classificare e organizzare il corpo. Nel tracciare tale passaggio, Foucault opera una disamina dei meccanismi sociali e teorici che hanno condotto agli ingenti cambiamenti verificatisi nei sistemi punitivi dei Paesi europei a cavallo dei secoli XVII e XVIII[678].

In Francia, fino alla Rivoluzione francese, l'Ordinanza del 1670 enucleava le pene che potevano essere irrogate dal giudice in conseguenza del compimento di un delitto: la morte[679], la *quaestio*[680] (*i.e.* la tortura) «con riserva di prova», la galera, la frusta, la confessione pubblica e il bando. Com'è evidente, si trattava in gran parte di pene fisiche – ogni delitto grave comportava una parte di supplizio – la cui crudeltà era graduata in base alle consuetudini, alla gravità dei delitti e allo *status* dei condannati. Oltre a queste,

[678] Bisogna tenere presente che il filosofo MICHEL FOUCAULT ripercorre, attraverso la descrizione della società disciplinare e del sistema biopolitico, la nascita della prigione nel solo sistema penale francese, muovendo però considerazioni che si estendono alla maggior parte dei Paesi europei. Foucault presenta uno stile complesso e si lascia spesso ad un'argomentazione prolissa, soprattutto quando descrive le tecniche storicamente determinate con cui si manifesta il potere disciplinare, ma al contempo – e anzi forse proprio per questo – è un Autore facilmente comprensibile. Siamo dinanzi ad un filosofo e storico magistrale, un vero pensatore, che al di là della singola tesi che vuole sostenere ci porta a riflettere sulla società che abbiamo ereditato e che ancora oggi contribuiamo a creare: una società che non si accontenta di fenomeni episodici, ma che tende a categorizzare e incasellare ogni cosa, forse per la smania atavica di tenere tutto sotto controllo.

[679] La pena di morte poteva assumere diverse forme: vi era chi era condannato all'impiccagione, chi alla mano o alla lingua tagliata; si poteva essere condannati a morire sulla ruota dopo che tutte le membra erano state spappolate; si poteva morire sul rogo, arsi vivi; vi era anche chi era condannato a morire bruciato dopo essere stato strangolato ovvero tirato da quattro cavalli in direzioni opposte.

[680] Con tale termine si intende la *veritatis indagatio per tormentum,* vale a dire la tortura.

le consuetudini prevedevano pene più leggere: soddisfazione alla persona offesa, biasimo, ammonizione, interdizione di un luogo, ammenda o confisca quali pene pecuniarie[681].

Invero, la pratica penale era molto distante dalle rigide previsioni dell'Ordinanza: i supplizi non costituivano la pena più frequente, dal momento che, da un lato, i giudici si rifiutavano di perseguire con rigore violazioni per le quali era prevista una pena eccessivamente severa, dall'altro lato, i tribunali tendevano a modificare la qualificazione giuridica del reato in modo tale da poter applicare la pena che ritenevano più confacente al crimine. Ciononostante, nella prassi, molte condanne costituite dal bando o dall'ammenda erano spesso accompagnate, a titolo accessorio, da una dimensione di supplizio[682].

Eppure, il supplizio – definito da Jaucourt[683] come «pena corporale, dolorosa, più o meno atroce» – sebbene crudele, non era certamente selvaggio: al pari di qualsiasi pena, anche il supplizio seguiva regole ben precise e predeterminate. In particolare, per essere tale, un supplizio doveva rispondere ad un «codice del dolore». Innanzitutto, era necessario che esso comportasse nel condannato una certa quantità di dolore fisico; la morte, infatti, assurgeva a supplizio solamente qualora non privasse semplicemente l'individuo del diritto di vivere, ma era necessario che la vita venisse sbriciolata in "mille morti", ognuna delle quali doveva costituire momento di acuta sofferenza. In secondo luogo, il supplizio era «l'arte di trattenere la vita nella sofferenza»: il condannato doveva vivere e soffrire; la sofferenza non era casuale, ma il tipo di dolore, la lunghezza e l'intensità dell'afflizione erano accuratamente calcolati in base allo *status* sociale della persona, alla gravità del delitto e al tipo di delinquenza. Infine, il supplizio si inseriva in una cerimonia punitiva con la precisa e duplice funzione di marchiare il corpo della persona che ne era vittima (sul corpo del suppliziato erano spesso lasciati segni di cui si doveva mantenere traccia nella memoria dei presenti) e di rendere gloriosa e trionfale la giustizia che, tramite di esso, si svelava in tutta la sua magnificenza e la sua forza (il supplizio doveva essere clamoroso perché esercitasse una funzione deterrente). In altri termini, il supplizio doveva essere eccesso, potere, doveva sottomettere gli uomini[684].

La procedura penale, volta ad accertare la verità storica e che si concludeva spesso con la comminatoria del supplizio, doveva rimanere segreta non solo per la collettività,

[681] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione,* Einaudi, Torino, 2014, 35-36.
[682] *Ibidem.*
[683] *Encyclopédie,* voce *Supplice.*
[684] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione,* Einaudi, Torino, 2014, 37-38.

ma per lo stesso accusato. Il magistrato – per delega ed estensione del sovrano – era l'unico detentore della verità e della giustizia. Tuttavia, questo non impediva che, per stabilire la verità, egli dovesse attenersi ad una rigida casistica di prove e dovesse seguire un multiforme calcolo combinatorio degli indizi[685]. Dunque, in campo penale, la verità era «il risultato di un'arte complessa», in quanto conseguiva a regole ben precise, conosciute solo agli specialisti[686].

Allo scopo di aggirare l'incerto e intricato calcolo combinatorio delle prove, la procedura penale tendeva naturalmente alla confessione (attuata mediante giuramento o tortura), la quale assurgeva a due funzioni fondamentali, ambigue ma strettamente correlate: per un verso, essa costituiva un elemento di prova nell'ambito dell'istruttoria, liberando peraltro l'accusatore dal difficile compito di fornire ulteriori prove; per altro verso, essa costituiva la massima aspirazione del sistema penale, in quanto, per mezzo della confessione, il condannato si inseriva nel meccanismo di produzione della verità penale, giudicandosi e condannandosi da sé[687].

La confessione era spesso strappata mediante *quaestio* (*i.e.* tortura)*,* pratica crudele ma anch'essa non esente da rigide regole giudiziarie: si teneva una sorta di scontro cavalleresco tra il magistrato che poneva le domande e il suppliziato (definito "paziente"), il quale era sottoposto ad una serie di prove, progressivamente più dure, all'esito delle quali poteva vincere – qualora non confessasse – o perdere – qualora confessasse. Tuttavia, la posta in gioco era piuttosto alta, in quanto – disponendo la *quaestio* – il giudice poteva perdere il diritto di pronunciare la condanna se l'accusato, sottoposto a tortura, non confessasse. Da qui era emersa la prassi di disporre la *quaestio* «con riserva di prova»: se il condannato non confessava, il magistrato conserva comunque il diritto di

[685] *Ivi*, 38-41, ove si sottolinea che le prove erano classificate in prove vere, dirette o legittime e prove indirette o congetturali; poi vi erano prove manifeste, prove considerevoli, prove imperfette o leggere; prove urgenti e necessarie (cioè prove piene del fatto, che non ammettevano prove contrarie); indizi prossimi o prove semipiene (cioè elementi che costituivano prova fino a quando non fosse fornita una prova contraria da parte del condannato); gli indizi lontani o «ammenicoli», vale a dire le opinioni dei testimoni. Tali prove si combinavano tra loro restituendo regole di calcolo piuttosto precise: ad esempio, le prove piene giustificavano qualsiasi tipo di condanna, mentre le prove piene potevano giustificare l'applicazione di pene afflittive, ma non potevano condurre alla morte; gli indizi imperfetti potevano convincere il giudice ad adottare un "decreto" o un'ammenda contro il sospettato; due prove semipiene costituivano una prova completa, laddove indizi lontani potevano fondare soltanto una pena afflittiva, purché numerosi e concordanti tra di loro.
[686] *Ivi*, 41.
[687] *Ivi*, 43.

far valere le prove già raccolte, ma il paziente guadagnava perlomeno il diritto di non essere messo a morte[688].

Fino al XVIII secolo, nella tortura si mescolavano elementi istruttori ed elementi di punizione: essa era innanzitutto una pena (ed era annoverata tra le pene più gravi), ma contemporaneamente era una prova. In un sistema giudiziario che non conosceva la presunzione di innocenza, la pena non conseguiva alla condanna al di là di ogni ragionevole dubbio: il solo fatto di essere accusato legittimava il magistrato ad irrogare una pena che da lieve diveniva crudele fino a quando non si fosse raggiunta la piena prova. In definitiva, a differenza di quanto avviene oggi, la giustizia penale non rispondeva ad uno schema dualista vero o falso, ma ad un principio di graduazione in base al quale un sospettato non era semplicemente in attesa di essere condannato o scagionato, ma parzialmente punito. Una volta raggiunto un certo grado di colpevolezza, il magistrato era legittimato a sottoporre a tortura l'accusato, in modo tale da iniziare la punizione e, contemporaneamente, estorcere mediante la pena il resto di verità mancante: il corpo del suppliziato era sia luogo di applicazione del castigo sia momento di estorsione della verità[689].

Questo intreccio di rituali continuava una volta pronunciata la sentenza di condanna, ove ancora una volta il corpo del condannato era elemento essenziale della cerimonia penale: il corpo era mostrato, esposto, suppliziato, spettacolarizzato, quasi a voler pubblicizzare quella giustizia che era rimasta per troppo tempo nell'ombra. In qualche modo, si incaricava il condannato di essere «pubblico ufficiale della sua propria condanna»: passeggiava per le vie con la folla attorno, a piedi nudi, leggeva la sentenza di condanna, confessava pubblicamente, talvolta con un cartello appeso al petto o alla schiena. Se ognuno dei personaggi incarnava bene il proprio ruolo, l'esecuzione si traduceva in una lunga confessione pubblica[690].

Allo stesso tempo, la pena manteva «losche parentele» con il delitto che si voleva estirpare dalla società[691]. Il supplizio era corredato di una serie di gesti ed elementi simbolici, senza soluzione di continuità con il crimine per cui si era condannati: la morte era data nello stesso luogo in cui il delitto si era consumato, si ripercorrevano le stesse vie e gli stessi gesti compiuti dall'assassino, era utilizzati gli stessi strumenti. Boia e

[688] *Ivi*, 45-46.
[689] *Ibidem.*
[690] *Ivi*, 47-48.
[691] *Ivi*, 11.

condannato erano avviluppati in un torbido spettacolo di violenza che continuava lo scontro fisico avvenuto tra condannato e persona offesa[692]. Il castigo sembrava eguagliare, se non superare, il delitto compiuto nella sua essenza selvaggia; alle volte, sembrava quasi che i ruoli si invertano: il giudice finiva per assomigliare ad un carnefice che non aveva timore di sporcarsi di sangue le mani, mentre il suppliziato era supportato dalla folla con pietà o ammirazione[693].

L'esecuzione non era priva di elementi spirituali: il supplizio era avvertito come punto di congiunzione tra il giudizio degli uomini e il giudizio di Dio. Gli spettatori erano intenti a decifrare ogni momento e ogni segno: così, una morte veloce era sintomo del divino che non aveva abbandonato il condannato nella disperazione, mentre urla e sofferenze inimmaginabili divenivano chiaro segno di una dannazione imminente[694].

Il cerchio si chiude: dalla *quaestio* alla condanna, fino al XVII secolo, il corpo era il vero protagonista della cerimonia penale e della liturgia punitiva[695].

Si capisce, allora, come l'*Ancien Régime* il supplizio giudiziario costituisce uno dei modi in cui il potere politico si manifesta: il delitto, oltre alla vittima immediata, arreca un'offesa al sovrano, detentore assoluto del potere legislativo e giudiziario. La legge è l'esternalizzazione della volontà del sovrano: chi la viola, attacca personalmente il potere regio[696]. Ogni infrazione costituisce un *crimen majestatis* e in ogni criminale vi è un potenziale attentatore all'unità del regno e alla grandezza del sovrano[697]. Mediante il castigo, il sovrano esercita una vendetta sia privata che pubblica; mediante lo spettacolo di violenza insito nell'esecuzione pubblica, il sovrano ostenta la sua forza indomabile, ristabilendo l'equilibrio violato, il potere eclissato, ricostruendo la naturale asimmetria «tra il suddito che ha osato violare la legge e l'onnipotente sovrano che fa valere la legge».[698] La pena è manifestazione plastica della superiorità intrinseca del sovrano: una superiorità non solo giuridica, ma anche fisica. Commettendo il delitto, il trasgressore ha osato sfidare il sovrano non meno di quanto faccia colui che viola i confini della nazione, motivo per il quale nei casi più gravi l'esecuzione della pena esibisce il medesimo fasto di una vittoria militare contro l'invasore straniero, tutta contornata da un apparato bellico

[692] *Ivi*, 49.
[693] *Ivi*, 11.
[694] *Ivi*, 49-50.
[695] *Ivi*, 51.
[696] *Ibidem.*
[697] *Ivi*, 58.
[698] *Ivi*, 52-53.

presente in tutta la sua sontuosità: sono presenti cavalieri, ufficiali di polizia, soldati; sono esibite sfilate, vi sono soste ai crocevia, inginocchiamento, pentimento davanti a Dio e al re. Il corpo non solo è marchiato, ma è anche spezzettato, maciullato, polverizzato e gettato al vento. Nulla deve restare di chi ha osato sfidare il sovrano. Nella liturgia del supplizio, il boia e il condannato sono avversari in un duello impari, il cui esito è certo: il carnefice domina il corpo del suppliziato, adopera la stessa forza e la stessa violenza del crimine commesso[699].

Fino al XVII secolo, la cerimonia del supplizio è strettamente connessa ad una cerca dinamica del potere: un potere regio che «non nasconde di esercitarsi direttamente sul corpo, ma si esala e si rinforza nelle sue manifestazioni fisiche»; un potere regio che tratta i rapporti politici non diversamente dai legami familiari, riproponendone le stesse regole e le stesse obbligazioni; un potere che considera l'infrazione un momento di rivolta nei confronti dell'ordine costituito, al pari di una guerra; un potere che non ammette disobbedienza delle sue leggi; un potere che «in mancanza di una sorveglianza ininterrotta, cerca il rinnovamento del proprio effetto nello splendore delle manifestazioni eccezionali»[700].

Meno di un secolo dopo, a partire dalla seconda metà del secolo XVIII, in molti Stati europei si assiste ad una rivoluzione della giustizia penale[701]: a seguito di profondi mutamenti sociali e istituzionali, sono presentati numerosi progetti di riforma in materia penale, prende vita una nuova teoria della legge e del crimine, viene portata alla luce una nuova giustificazione etica e politica del diritto di punire. Tali elementi si intrecciano con la redazione dei codici penali moderni, i quali contengono regole di procedura unificate e definiscono il carattere essenzialmente correttivo della pena[702]. Tra i tanti mutamenti in materia di amministrazione della giustizia – elemento spesso trascurato nella storia del

[699] *Ivi*, 56. Volendo ricercare le ragioni di un simile accanimento e disprezzo del corpo, Foucault osserva che da un lato, il corpo umano non ha ancora quel «valore commerciale» legato al suo sfruttamento economico, che acquisterà soltanto con la Rivoluzione industriale; dall'altro lato, fattori quali la fame, le malattie, la mortalità infantile rendevano la morte più accettabile e gli uomini meno attaccati alla vita.
[700] *Ivi*, 62-64, ove si sottolinea che proprio per tale motivo, in queste esecuzioni che toccano il corpo, il popolo è invitato non solo a guardare, ma addirittura ad inserirsi nella vendetta del re: la popolazione deve difendersi dai turbamenti dell'ordine costituito, appoggiando senza riserve il proprio sovrano quando è minacciato dai nemici della patria.
[701] Russia, 1769; Prussia, 1780; Toscana, 1786; Austria, 1788; Francia, 1791, anno IV, 1808 e 1810, come sottolineato in M. FOUCAULT, op. cit., 9.
[702] *Ibidem.*

diritto – si staglia la sparizione dei supplizi, a testimonianza di una nuova morale dell'atto di punire[703].

L'epoca dei Lumi porta con sé la protesta contro il supplizio quale metodo punitivo: i filosofi e i teorici del diritto, i riformatori, i giuristi, i parlamentari mettono in luce che la giustizia criminale debba punire senza vendicarsi. Il supplizio diviene inaccettabile e indecoroso per chi lo subisce, ridotto alla disperazione e polverizzato; diviene rivoltante per il potere sovrano, in quanto tradisce l'eccesso e chiama alla rivolta. Diviene evidente che il supplizio sia pericoloso per la sopravvivenza stessa della Nazione: abituato al sangue e alla violenza, il popolo impara che per ribellarsi ai soprusi non vi sia altro modo che vendicarsi con il sangue[704].

Quale giustificazione morale di tale movimento di riforma, gli Illuministi del XVIII secolo pongono la regola fondamentale che l'uomo debba essere misura e frontiera legittima del potere di punire: è necessario rispettare l'essenza dell'uomo, la sua umanità, per correggere le sue azioni senza far scorrere altro sangue[705].

Prima ancora di porre i pilastri di una nuova giustizia criminale, i riformatori illuministi, oltre ad attaccare la barbarie dei castighi e il «dispotismo del patibolo», condannano la discontinuità e l'irregolarità dell'organizzazione giudiziaria, elementi che paradossalmente rendono lacunosa la giustizia penale: vi sono tribunali, procedure, strati sociali della popolazione e addirittura delitti che cadono fuori dal diritto comune; esistono vari circuiti incaricati di reprimere i reati (giustizie signorili, giustizie reali, numerosi tribunali amministrativi mal coordinati tra di loro, istanze di polizia come le provosture o le luogotenenze di polizia); è ancora presente il potere personale del re di punire; si condanna l'eccessivo potere delle giurisdizioni inferiori nel determinare la pene; sono emesse sentenze arbitrarie noncuranti dei principi giuridici[706].

[703] *Ivi*, 10. Si parla poco del pregevole ruolo che hanno assunto le agitazioni popolari nel mutamento delle pratiche punitive: l'insofferenza nei confronti della spettacolarizzazione della pena è partita dal basso, attirando solo successivamente l'attenzione di persone abbienti e illuminate che ne hanno dato un fondamento filosofico-giuridico. A partire dalla fine del XVIII secolo, difatti, uno strato della popolazione comincia a sovvertire questa manifestazione del potere regio. In particolare, durante i giorni delle esecuzioni, la tensione è crescente, la popolazione mostra maggiore simpatia e solidarietà più per coloro che dovevano essere condannati (soprattutto i piccoli delinquenti) che non per coloro che avrebbero dovuto attuare la punizione voluta dal re, come sottolineato in M. FOUCAULT, op. cit., 67-69.
[704] *Ivi*, 79-80.
[705] *Ivi*, 81.
[706] *Ivi*, 85.

La nuova teoria giuridica della scienza penale si inserisce in una riforma di più ampio respiro volta alla razionalizzazione della distribuzione del potere di punire e della ripartizione degli effetti della politica criminale: non tanto punire meno, quanto punire meglio; dolcezza della pena, ma soprattutto uniformità degli effetti[707]; rendere accettabile e controllabile in tutti gli strati della popolazione il potere di castigare[708]; diminuire il costo economico e politico della punizione[709].

Dalla fine del secolo XVIII, a poco a poco, il meccanismo della punizione muta i suoi connotati[710], conducendo, all'inizio del secolo XIX, all'epoca della «sobrietà punitiva»[711]. Progressivamente scompare la «lugubre festa punitiva» e il corpo non costituisce più il luogo principale della repressione penale[712]. Tale mutamente avviene mediante due processi che però non condividono né genesi né ordine temporale: da un lato, scompare lo spettacolo della punizione, dall'altro lato, l'azione punitiva non mira più a infliggere dolore al corpo del condannato[713].

Il giudice vuole discolparsi dall'essere puramente e semplicemente colui che pronuncia la pena: l'esecuzione della pena inizia a divenire un settore autonomo, a testimonianza del fatto che la giustizia tende a prendere le distanze da quella parte di violenza che aveva caratterizzato sino al allora i supplizi, e che pure resta legata al suo esercizio[714]; per altro verso, parte del giudizio è trasferito a istanze diverse dal giudice: sorveglianti, medici, cappellani, psichiatri, psicologi, educatori[715].

Ebbene, la sofferenza fisica e il dolore non sono più elementi costitutivi della pena; la giustizia priva il condannato di diritti senza imporre la sofferenza sul corpo e comanda «pene libere dal dolore»[716]; non vi è più un accanimento sul corpo che perdura

---

[707] *Ivi*, 95 fa riferimento all'«infrapotere degl'illegalismi conquistati e tollerati» per indicare che in ogni strato della popolazione si annidavano privilegi e lacune giuridiche, tanto odiosi quanto coerenti con la loro storia e necessari per la tenuta della nazione, che talvolta assumevano le forme di una massiccia inosservanza generale delle leggi.
[708] *Ivi*, 88-89, ove viene sottolineato che tale riforma fu preparata non dall'esterno contro l'apparato giudiziario, ma le istanze di rinnovamento pervennero dall'interno, soprattutto da magistrati e uomini di legge, che misero in luce non solo l'esigenza di pervenire ad un «castigo senza supplizio», ma anche la necessità di esercitare un potere di punire scevro dalla pretesa di legiferare e affrancato dalle interferenze del sovrano. Sono ricordati filosofi del calibro di Voltaire e Brissot o Marati; magistrati come Le Trosne, Lacretelle, Dupaty e Servant.
[709] *Ivi*, 97.
[710] *Ivi*, 11.
[711] *Ivi*, 17.
[712] *Ivi*, 10.
[713] *Ibidem.*
[714] *Ivi*, 11.
[715] *Ivi*, 13.
[716] *Ivi*, 14.

oltre la morte del condannato; inizia a serpeggiare l'idea che ciò che deve tenere lontani dal delitto non è la sua triste e ripugnante rappresentazione, quanto la certezza di essere puniti[717]. Resta tuttavia l'esigenza di punire: la giustizia penale e coloro che la distribuiscono lo faranno da lontano, con discrezione, secondo regole rigide e prestabilite, rinunciando a supplizi lunghi e crudeli e mirando ad un obiettivo di gran lunga più pregevole, vale a dire la rieducazione del condannato[718].

Mentre nei supplizi medievali il corpo costituiva il bersaglio principale della pena, le pene di inizio Ottocento, che pure incidono sul corpo (basti pensare alla prigione, alla reclusione, ai lavori forzati, alla deportazione), fanno del corpo uno strumento per privare il colpevole di una libertà, considerata insieme diritto e bene. Secondo la nuova teoria della penalità, l'espiazione della pena si trasforma in «un sistema di costrizioni e di privazioni, di obblighi e di divieti»[719]: «il castigo passa da un'arte di sensazioni insopportabili a una economia di diritti sospesi»[720].

La pena aspira a colpire non tanto il corpo nella sua materialità quanto l'anima nella sua immaterialità[721]: filo conduttore della «pena incorporea» diviene il tormento del cuore, lo strazio della volontà, la conversione del pensiero, con lo scopo ultimo di modificare il comportamento del condannato[722]. Ciononostante, la pena fatica a dissociarsi dal dolore fisico: anche pene che non colpiscono direttamente il corpo comportano, in una certa misura, la sofferenza fisica (nelle prigioni, i condannati patiscono il freddo, la fame, il sovraffollamento, subiscono percosse, sono ristretti in celle di isolamento) [723].

Ebbene, anche se non secondo un processo univoco, in Europa scompare progressivamente lo spettacolo del supplizio[724].

---

[717] *Ivi*, 11.
[718] *Ivi*, 13.
[719] *Ibidem.*
[720] *Ibidem.*
[721] G. DE MABLY, *De la législation,* in Œuvres complètes, 1789, tomo IX, 326.
[722] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione*, Einaudi, Torino, 2014, 19, ove si sottolinea che nel medesimo secolo si inizia a giudicare, oltre all'elemento oggettivo del reato, anche la volontà del soggetto, prestando contemporaneamente attenzione a pulsioni, passioni, infermità mentali e disadattamenti: non a caso, alla pena si accompagnano le misure di sicurezza (quali interdizione di soggiorno, libertà sorvegliata, trattamento medico obbligatorio), destinate a risocializzare il condannato e a modificarne la tendenza criminale.
[723] *Ivi*, 18-19.
[724] *Ivi*, 17.

Il filosofo francese Foucault si interroga se gli elementi summenzionati – l'accresciuta dolcezza della pena, l'innesto del sapere scientifico nei meccanismi della giustizia penale, la metamorfosi dei metodi punitivi, lo spostamento del loro campo di applicazione – presentino la stessa matrice epistemologica-giuridica, vale a dire «la trasformazione del modo in cui il corpo è investito dai rapporti di potere»[725]. Secondo la teoria sostenuta da Foucault, le tecniche punitive discendono, secondo relazioni complesse, dalla "tecnologia politica del corpo", vale a dire dai rapporti di dominio politico, ovvero, in altri termini, dall'utilizzazione economica del corpo: il corpo diviene (utile) forza produttiva solo quando è assoggettato al potere[726]. Coloro che vengono sorvegliati, addestrati, puniti, i bambini, i colonizzati, i lavoratori che fanno dipendere la loro esistenza da un apparato di produzione sono ridotti a schiavi di tale potere[727]. La signoria sulle forze dell'uomo deve essere ben maggiore della capacità umana di vincerle. Siffatto assoggettamento può derivare dalla violenza (come avveniva nell'*Ancien Régime*) ovvero, in alternativa, dall'ideologia (come avviene dopo la Rivoluzione francese)[728]. Ciò vuol dire che il gioco del potere non risparmia neppure l'anima: «l'anima, prigione del corpo», scrive Foucault[729] rovesciando il tradizionale impianto filosofico secondo il quale il corpo è prigione dell'anima e la vita corporea l'espiazione di una colpa atavica. Secondo l'assunto di Foucault, castigata l'anima, il corpo è libero.

Nondimeno, bisognerà attendere a lungo perché questa strada sia compiutamente percorsa. Difatti, i tempi per un simile mutamento delle relazioni di potere non sono ancora maturi nell'epoca dei Lumi. Nel secolo XVIII, la formulazione della «nuova economia del potere»[730] viene ancorata alla teoria generale del contratto: i governati stipulano un patto sociale con i governanti, accettando spontaneamente, per la propria stessa sopravvivenza, che gli siano imposte leggi dal sovrano in cambio di una maggiore tranquillità e sicurezza. Colui che viola le leggi diviene nemico della comunità, un traditore della patria, ben presto un anormale, che mette a repentaglio la conservazione dello Stato, attivando di conseguenza il potere di punire di chi ha sottoscritto il patto[731].

---

[725] *Ivi*, 27.
[726] *Ivi*, 29.
[727] *Ivi*, 33.
[728] *Ivi*, 29.
[729] *Ivi*, 33.
[730] *Ivi*, 88.
[731] Come accennato, secondo gli Illuministi, le pene devono essere umane. Inoltre, perché sia utile, la pena deve essere proporzionata non tanto alla gravità del delitto quanto alla sua possibile ripetizione futura: inizia a farsi strada l'idea che la punizione riguardi non tanto il passato quanto il futuro e che la pena debba servire sia a punire l'infrazione sia a dissuadere altri soggetti e il soggetto medesimo a ripetere lo stesso crimine

Secondo i riformatori illuministi, il castigo deve servire da monito per tutti gli altri potenziali colpevoli: il condannato è solo uno dei bersagli della pena e i suoi segni devono essere da esempio per l'intera collettività. Si insinua l'idea per la quale il corpo del condannato – anziché divenire proprietà del re come nell'*Ancien Régime* – si deve elevare a bene sociale di cui si appropria la collettività[732].

Non a caso, secondo i riformatori illuministi, i lavori pubblici costituiscono la migliore pena possibile, in quanto conseguono il duplice scopo di riabilitare il condannato e di conseguire un profitto sociale tramite la riparazione del danno cagionato alla società[733].

Viceversa, tanto nell'*Ancien Régime* quanto nei vari progetti di riforma presentati durante l'epoca dei Lumi, la prigione non assume che un ruolo marginale nel sistema delle pene. Invero, essa costituiva una delle numerose pene che potevano essere previste nel Codice e irrogate dal giudice; in particolare, la prigione è prevista quale pena specifica di determinati delitti (specialmente delitti contro la libertà dell'individuo o quelli che derivano dall'abuso della libertà, come la violenza o il disordine) ovvero, alternativamente, costituisce una pena sostitutiva di quella principale per coloro – donne, bambini, invalidi – che non possono svolgere lavori di utilità sociale. Anzi, l'idea della detenzione penale quale forma generale di pena è aspramente e apertamente criticata dai filosofi e teorici del diritto, in quanto nell'insieme risulta incompatibile con tutti i principi ispiratori della riforma della giustizia criminale del secolo XVIII: innanzitutto, la prigione non costituisce una pena in grado di far fronte alla specificità dei delitti e all'esigenza che vi sia una correlazione tra l'idea del crimine e l'idea della pena; in secondo luogo, è inutile

(quelle che oggi sono definite come funzione punitiva della pena e funzione specialpreventiva e generalpreventiva della pena). Per un maggiore approfondimento si rinvia a M. FOUCAULT, op. cit., 99-112. Inoltre, come sottolineato in M. FOUCAULT, op. cit., 113-124, l'arte di punire dovrebbe far leva su tutta una tecnica della rappresentazione che obbedisce a principi rigorosi. Innanzitutto, la punizione non deve essere arbitraria; anzi, all'opposto, devono essere istituite pene che abbiano una certa analogia con il delitto commesso. Vi deve essere una correlazione tra l'idea del crimine e l'idea della pena. Tuttavia, a differenza dell'*Ancien Régime*, in cui si poteva ravvisare una sorta di continuità tra delitto e supplizio, le pene devono essere prevedibili: così, chi aveva abusato della libertà pubblica, potrà prevedere con notevole grado di certezza che sarebbe stato privato della propria libertà; chi aveva beneficiato illegittimamente dei privilegi delle funzioni pubbliche, potrà prevedere che sarebbe stato privato dei propri diritti civili, e così via. In altre parole, ogni cittadino deve prefigurarsi la pena che potrebbe conseguire alla commissione dell'illecito. In secondo luogo, tale prefigurazione deve essere presagio di uno svantaggio: lo svantaggio conseguente alla violazione deve superare il piacere dell'illecito. Ancora, la pena deve essere a termine. Una pena perpetua sarebbe inutile, in quanto in sé contraddittoria: *in primis,* bisogna dotare il condannato di un motivo per correggere il proprio comportamento; inoltre, dopo aver sostenuto costi e sforzi, la società deve poter beneficiare del comportamento nuovamente virtuoso del condannato.

[732] *Ivi*, 113-124.

[733] *Ibidem.*

per la società, in quanto questa non trae beneficio dal lavoro impiegato dai criminali, anzi è costosa per lo Stato; essa è nociva per gli stessi detenuti, in quanto non favorisce la rieducazione del condannato e, all'opposto, mantiene nell'ozio i criminali; soprattutto, per gli Illuministi, la sua particolare struttura fa della prigione un luogo di tirannia, che facilmente si espone all'arbitrio e ai soprusi dei guardiani; è un «luogo di tenebre», che si erge lontano dagli occhi dei cittadini, che non possono controllare né il numero né il trattamento dei reclusi. Addirittura, la reclusione o era caduta in desuetudine durante l'*Ancien Régime,* al pari di altri supplizi, o era annoverata tra le "pene leggere"[734].

Può stupire, allora, che in pochissimo tempo la detenzione sia divenuta la forma generale di pena, sostituendo nel Codice penale francese del 1810 tutte le pene intermedie tra la pena di morte e le pene pecuniarie. In altre parole, tutti i delitti che non erano tanto gravi da meritare la pena di morte né troppo blandi da essere perseguiti con una pena pecuniaria erano puniti con la carcerazione, presentata con forme diverse ma di identica sostanza: i lavori forzati, il bagno, la detenzione, la reclusione, l'incarceramento correzionale sono solo denominazioni diverse che indicano lo stesso castigo[735].

Ecco, dunque, che viene previsto un grande sistema carcerario in grado di accogliere la maggior parte dei condannati, che si presenta come un'architettura chiusa e complessa incorporata nel potere statale, con alti muri invalicabili: «una tutt'altra materialità, una tutt'altra fisica del potere, una tutt'altra maniera di investite il corpo umano». Non più il patibolo, non più il teatro punitivo e lo sfarzo del supplizio dove il sovrano poteva manifestare plasticamente tutto il suo potere di vita e di morte, ma una struttura chiusa, al riparo dagli occhi dei cittadini, che cela i modi in cui viene amministrata la punizione diviene il simbolo del potere di punire[736].

La promessa varietà delle pene, la promessa di una pena utile per il benessere collettivo furono rase al suolo da una «penalità uniforme e grigia»[737].

Tale mutamento di prospettiva fu favorito, in buona sostanza, dall'importazione di alcuni grandi e prestigiosi modelli di carcerazione punitiva, che rispondono ad una

[734] *Ivi*, 124-129.
[735] *Ivi*, 125.
[736] *Ivi*, 126.
[737] *Ivi*, 127. Questa è la situazione che si verifica non soltanto nella Francia del XVIII secolo, ma anche in altri Paesi, fra cui spicca il Granducato di Toscana all'indomani del Trattato *Dei delitti e delle pene* di Cesare Beccaria.

funzione essenzialmente pedagogica[738]: il modello carcerario olandese[739], l'archetipo inglese[740] e il modello di Filadelfia[741].

In definitiva, verso la fine del secolo XVIII, coesistevano tre diversi modelli di organizzazione del potere punitivo: il modello monarchico, l'archetipo disegnato dai giuristi riformatori, il modello carcerario[742]. Vediamo perché, alla fine, prevalse il modello carcerario.

[738] *Ivi*, 131.

[739] Il più antico modello, che ispirò tutti gli altri, è quello olandese (il Rasphius di Amsterdam), che iniziò a funzionare nel 1596: sul solco dell'idea che l'ozio costituisce la causa principale di tutti i delitti, il tempo dei condannati era rigidamente scandito non solo da obblighi e regole, ma soprattutto dal lavoro, che peraltro veniva retribuito, nella speranza che il salario potesse favorire il loro reinserimento morale e materiale nella società dopo la prigione. Per un approfondimento, si veda M. FOUCAULT, op. cit., 131-133.

[740] Anche l'archetipo inglese – ideato da Hanway nel 1775 – è volto alla ricostituzione dell'*homo oeconomicus,* a cui aggiunge l'aspirazione di innestare nel detenuto imperativi morali. A tale scopo, la detenzione inglese accompagna al lavoro l'isolamento, giustificato innanzitutto dallo scopo di evitare che la promiscuità nelle prigioni possa dar luogo ad evasioni e rivolte, ma anche dalla convinzione che il soggetto – sfuggito da cattive influenze – possa guardarsi dentro e fare un «ritorno in se stesso», ritrovando la coscienza perduta. La prigione diviene, dunque, un luogo di trasformazione individuale e di ritrovamento della propria dignità, nella prospettiva di restituire alla società un soggetto nuovo. Per un approfondimento, si veda M. FOUCAULT, op. cit., 134-135.

[741] Infine, si staglia il modello di Filadelfia: anche qui la giornata del detenuto è scandita da rigidi orari, ogni momento della giornata prescrive un certo tipo di lavoro (con cui la prigione si autofinanzia) e ha una sua destinazione precisa. A differenza degli altri modelli, tuttavia, la solitudine e il ritorno a se stessi non bastano, perché si insinua l'aspirazione di trasformare lo spirito del detenuto: durante tutto l'arco della detenzione, egli è sorvegliato e le sue attività e il suo comportamento sono costantemente annotati. Tramite la costante sorveglianza da parte dei guardiani, la prigione diviene «una sorta di osservatorio permanente che permette di distribuire la varietà del vizio o della debolezza», che spira a riformare l'anima del detenuto. Il castigo e la correzione attuano un processo di trasformazione di tutto l'individuo: non solo del suo corpo (mediante il lavoro quotidiano e le rigide regole impartite), ma anche della sua anima e della sua volontà (tramite gli esercizi spirituali a cui è costretto). Lo Stato esercita sul detenuto un potere totale. Per un approfondimento, si veda M. FOUCAULT, op. cit., 127 e 135-138.

[742] *Ivi*, 143, ove si ripercorrono e sintetizzano le differenze tra i modelli sia nel fondamento teorico sia nella «tecnologia della pena», cioè il dispositivo pratico cui dà luogo: nel diritto monarchico, la pena è una vendetta del re, che tramite il castigo vuole ricostruire la sovranità violata; si utilizzano marchi; la folla è chiamata a partecipare alla punizione non diversamente da quanto accadrebbe se si trattasse di una guerra contro invasori stranieri. Gli altri due modelli condividono il fondamento teorico della pena, cui è affidata una funzione preveniva e correttiva, ma sono molto distanti tra loro quanto al modo in cui la colpa è espiata: nel modello carcerario, l'apparato della penalità correttiva non si serve di rappresentazioni (rappresentazione degli interessi, rappresentazione dei vantaggi e degli svantaggi, rappresentazione del piacere e del castigo) come nel modello ideato dagli Illuministi, ma piuttosto la correzione avviene tramite l'assoggettamento del detenuto a certe regole, abitudini, ordini e la sorveglianza del suo tempo. In entrambi i casi, peraltro, si rinviene un unico scopo: quello di creare individui, anche quelli più refrattari alle regole, che siano sottomessi al potere costituito. In altri termini, si tratta di formare un soggetto obbediente.

### 4.1.2. *(Segue):* La società disciplinare

In tutte le società, si presta una grande attenzione per il corpo: al corpo che si allena, al corpo che si manipola, al corpo sottoposto a rigide costrizioni, al corpo che obbedisce, al corpo che si piega alla volontà del potere[743].

Sulle soglie del XVII secolo, tuttavia, il corpo è investito da una nuova tecnica del potere, da una nuova formula generale di dominazione e costrizione. Nella società, si insinua lentamente, ma inesorabilmente, un processo evolutivo che mira ad ottenere l'effetto di un assoggettamento continuo e penetrante del corpo, mediante un controllo minuzioso e ininterrotto delle sue forze, che lo rendano docile e sottomesso. Se è vero che i procedimenti disciplinari esistono da sempre, è pur vero che in questi secoli si affinano le tecniche di intervento sul corpo. Innanzitutto, si modifica la scala del controllo: non si interviene più all'ingrosso, come se il corpo fosse un'unica massa, ma si esercita su di esso un controllo infinitesimale, che agisce sui dettagli, cioè sui movimenti, sui gesti, sulle attitudini. In secondo luogo, muta l'oggetto del controllo: la sorveglianza verte non più sulla condotta o sul linguaggio del corpo, ma piuttosto sui movimenti, sull'esercizio, sull'organizzazione del corpo. Infine, le modalità del controllo si fanno sempre più penetranti e incisive: il tempo entro cui il corpo si esercita è sempre più segmentato, con lo scopo di ottenere effetti di utilità ed obbedienza sempre più grandi[744].

In definitiva, nel corso dei secoli XVII e XVIII, si afferma una «società disciplinare», cioè un nuovo metodo generale di investimento politico del corpo che tende a permeare l'intero corpo sociale: partendo dagli ordini religiosi e dai conventi, che da sempre sono maestri di disciplina, tale movimento politico e culturale permea dapprima i collegi e le scuole elementari, poi si insinua nelle case di educazione, negli istituti di assistenza, negli spazi ospedalieri e nelle grandi manifatture, fino a lambire e ristrutturare l'organizzazione militare[745].

Nel corso di quegli anni, va nascendo un meccanismo mediante il quale tanto più il corpo è obbediente al potere, quanto più è utile e viceversa: si va formando, cioè, una «anatomia politica» del corpo. La coercizione disciplinare ottiene, da un lato, l'effetto di aumentare le forze fisiche del corpo (e di conseguenza la sua utilità) e,

[743] *Ivi*, 149.
[744] *Ibidem.*
[745] *Ivi*, 150.

contemporaneamente, quello di sottometterne la volontà. Detto diversamente, si stabilisce una stretta correlazione tra «un'attitudine maggiorata ed una dominazione accresciuta»[746].

In una società simile, la disciplina è «l'arte è di ripartire i corpi, di estrarne e cumularne il tempo», ma al contempo costituisce la tecnica di composizione delle forze per estrarne una maggiorazione di utilità[747].

Il momento storico in cui le discipline si affermano è quello in cui il corpo entra in un meccanismo di dominazione e di coercizione costante, tramite un esercizio dettagliato e cellulare da parte del potere: si tratta di una «microfisica del potere» che si insinua nel corpo e lo manipola[748].

L'avvento delle discipline è evidente in tutta una serie di tecniche essenziali che si rinvengono in molte istituzioni dell'epoca: tecniche modeste, sottili, all'apparenza innocue e trascurabili, fenomeniche, che ben presto trascendono i campi in cui sono sorte per conquistare territori sempre più estesi[749]. Ogni dettaglio è importante, nulla può essere trascurato. Questo tipo di società mutua dall'eduzione cristiana l'arte del dettaglio e poi – passando per la pedagogia scolare, per la medicina e per l'opificio e attraversando la tattica miliare e tutte le forme di addestramento – acquista un contenuto laicizzato generale, generando un nuovo mondo fatto di minuzie tecniche e descrizioni, procedimenti e dati[750].

Non interessa qui mettere in luce le singole peculiarità delle diverse istituzioni disciplinari, ma piuttosto rinvenire il cammino comune da esse percorso.

Volendo sintetizzare, Foucault descrive la genesi della società disciplinare, sostenendo che essa fabbrica, nel secolo XVIII, quattro tipologie di individualità: l'individualità-cellulare, attraverso la tecnica della ripartizione nello spazio dell'individuo; l'individualità-organica, mediante la prescrizione delle attività e delle manovre; l'individualità-genetica, volta al cumulo e alla capitalizzazione del tempo; infine, l'individualità combinatoria, mediante la composizione delle forze.

[746] *Ivi*, 149-151.
[747] *Ivi*, 149.
[748] *Ivi*, 150-151.
[749] *Ibidem.*
[750] *Ivi*, 152-153.

***Il principio della suddivisione individualizzante: una microfisica del potere «cellulare»***

Tutti gli apparati disciplinari si ispirano, anzitutto, al principio della clausura, utilizzato per operare una ripartizione spaziale degli individui. Difatti, la prima operazione della disciplina consiste nel riportare ad organizzazione e categorizzazione la moltitudine confusa (e potenzialmente pericolosa) delle cose. La società disciplinare opera una divisione, sistemazione e organizzazione di tutte le cose esistenti.

A tal fine, occorre innanzitutto individuare uno spazio isolato, chiuso su se stesso: a cavallo dei secoli XVII e XVIII, i collegi si apprestano a divenire il regime di educazione ordinario; nascono diverse centinaia di caserme, ove riportare e mantenere l'esercito nell'ordine, lontano dalla popolazione civile che mal sopporta i saccheggi; iniziano a svilupparsi grandi spazi manifatturieri e poi le fabbriche, ove il lavoro degli operai è organizzato rigorosamente, con lo scopo di neutralizzare i contrattempi e ottimizzare i vantaggi[751].

Il principio della clausura non è, tuttavia, sufficiente: occorre che ogni individuo sia assegnato al proprio posto, secondo il principio della localizzazione elementare o *quadrillage.* Lo spazio di ogni istituzione disciplinare è suddiviso e distribuito con rigore analitico; la disciplina organizza gli spazi in modo rigoroso; le moltitudini confuse e sfuggenti non sono tollerate, perché non sono controllabili[752].

È necessario, inoltre, assicurare un controllo al contempo generale e individuale delle persone. Nelle officine, la forza lavoro è scomposta in unità individuali; ogni operaio ha i propri turni, ad ogni operaio è assegnato il proprio lavoro e lo svolge in solitudine; al contempo, la qualità del suo lavoro è sorvegliata, gli operai sono confrontati tra di loro e classificati secondo le proprie abilità; la produzione è articolata in stadi successivi. È la nascita delle grandi industrie. Parimenti, la scienza medica inizia a classificare le malattie, con lo scopo di arginare i contagi. Frattanto, inizia la sorveglianza militare sui disertori, il controllo fiscale sulle merci, i controlli amministrativi sul territorio[753].

Infine, ogni individuo deve occupare il proprio «rango», in modo tale che sia possibile un lavoro simultaneo e privo di intermezzi vuoti. Ognuno è definito dal posto che gli è stato assegnato e dallo spazio che lo divide dall'altro posto: il rango diviene

[751] *Ivi*, 154-155.
[752] *Ivi*, 155-156.
[753] *Ivi*, 156-158.

l'unità di misura della società disciplinare. I "posti", i "ranghi", le "celle" assicurano l'ubbidienza e la docilità degli individui. L'organizzazione dello spazio seriale si ispira al modello dell'esercito romano: ad esempio, nei collegi gesuiti, le classi erano composte da due o trecento allievi; ogni allievo, in base al suo valore, al suo carattere, alla ricchezza dei suoi genitori, è incasellato in un posto che corrisponde alla sua funzione; di mese in mese, di anno in anno, egli si sposta alle classi successive, alle materie successive, secondo un ordine di difficoltà crescente. In questo modo, è possibile controllare i tempi e le modalità di apprendimento di ciascuno: l'educazione scolare diviene una «macchina […] per sorvegliare, gerarchizzare, ricompensare»[754].

La razionalizzazione dello spazio e la sorveglianza degli individui divengono la condizione essenziale per una microfisica del potere che Foucault definisce «cellulare»[755].

### *Rigida scansione del tempo: il tempo si insinua nel corpo*

Sebbene sin dai tempi antichi le comunità monastiche avessero suggerito un impiego rigoroso del tempo, nella società disciplinare, il tempo assume un taglio sempre più stretto. Le discipline stabiliscono delle scansioni temporali sempre più brevi; tra il comando e il gesto, non vi deve essere dispendio di tempo. Siffatto procedimento di regolarizzazione temporale è evidente non solo nelle istituzioni religiose, ma soprattutto nelle grandi manifatture, in cui la valutazione salariale del tempo fa sì che il lavoratore venga sorvegliato ininterrottamente, in modo che sia assicurata la qualità della produzione e che sia proibito tutto ciò che può distrarre e che non è produttivo. Detto in altri termini, si cerca di costruire «un tempo integralmente utile»[756].

Inoltre, il tempo è scandito da fattori esterni, nella misura in cui il corpo è manipolato dall'autorità. In tutti gli apparati di addestramento del XVIII secolo, i movimenti delle truppe diventano un programma rigidamente imposto dall'esterno:

[754] *Ivi*, 158-161, ove si sottolinea che tutta la società del secolo XVIII è incentrata alla costituzione di «quadri» in ogni ambito (scientifico, politico ed economico): in questo periodo, si inizia a costruire un sistema economico più razionale e consapevole; iniziano i controlli sulla circolazione della moneta e delle merci, in modo da regolare le ricchezze; si costruiscono forze armate più moderne; negli ospedali, i malati sono separati gli uni dagli altri in base alla malattia; si sistemano gli orti botanici e i giardini zoologici. Si tratta di dividere lo spazio, organizzarlo in base alle diverse funzioni che vengono assegnate agli individui, di dare un ordine alla società, in vista di una sempre maggiore efficienza.
[755] *Ivi*, 162.
[756] *Ivi*, 164.

bisogna ripartire i soldati in file o battaglioni, abituarli alla marcia a ritmo di tamburo, iniziando con il piede destro e tenendo tutti lo stesso passo, a testa alta e schiena dritta. Il tempo si insinua nel corpo. Al contempo, la disciplina definisce pedissequamente i gesti e i movimenti che il corpo deve fare con l'oggetto che manipola: posizione del capo, flessione della gamba, movimento delle braccia. Il controllo disciplinare non consiste solo nell'insegnare e prescrivere una serie di manovre e di gesti ripetitivi, ma impone anche che vi sia la massima rapidità e la massima efficienza possibile: si pretende un addestramento utile del corpo[757].

Infine, si impone in tutta la società disciplinare un'utilizzazione esaustiva del tempo: la morale dominante richiede che il tempo non sia sprecato. Le discipline organizzano il tempo in modo tale che in ogni attività prescritta non vi siano imperfezioni o impurità di tempo; vi deve essere un *continuum* temporale tra un'operazione e l'altra: non tanto impiego, quanto esaustione del tempo. Utilizzando le parole di Foucault, si cerca di «estrarre dal tempo sempre più istanti disponibili e da ogni istante sempre più forze utili»[758].

La microfisica del potere fabbrica, partendo dal corpo che tenta di manipolare, oltre che un'individualità «cellulare», anche un'individualità «organica», mediante la codificazione delle attività e la prescrizione dei gesti[759].

### *L'organizzazione degli inizi: la capitalizzazione del tempo*

Nel XVIII secolo si assiste ad un importante fenomeno per il quale il potere si fa carico del tempo delle singole esistenze, per governarne le forze, i corpi, per trasformare in utilità sempre maggiori lo scorrere del tempo. Il tempo disciplinare si impone sin dall'età scolare, in modo da evitare dispersioni di tempo nella vita di un individuo, in un'ottica di addizionamento e di capitalizzazione del tempo di ciascuno[760].

La pratica pedagogica mutua dalle istituzioni militari l'organizzazione del tempo: ogni attività è suddivisa in segmenti successivi, ognuno dei quali è preordinato ad una specifica attività; queste trafile di attività si succedono tra di loro secondo uno schema di difficoltà crescente; ogni attività è sottoposta ad esame da parte degli ufficiali superiori

[757] *Ivi*, 164-167.
[758] *Ivi*, 169.
[759] *Ivi*, 162.
[760] *Ivi*, 172.

nel caso dell'organizzazione militare o da parte dei maestri nelle scuole, in modo da verificare l'apprendimento delle abilità e il raggiungimento del livello stabilito dallo statuto; si qualificano gli individui in virtù del modo in cui raggiungono queste serie. A tal fine, giocano un ruolo fondamentale gli esercizi: ad ogni allievo o soldato sono prescritti esercizi progressivi, in base al livello, all'anzianità, al grado, alle abilità di ognuno[761].

La genesi degli individui e l'evoluzione della società fanno da contraltare alla trasformazione delle tecniche del potere, e in particolare al nuovo modo di cumulare il tempo, di economizzarlo, ridurlo ad una forma di utilità[762]: il tempo organizzato diviene l'intermediario tramite il quale esercitare il potere sugli uomini. Detto diversamente, il cumulo del tempo e l'esercizio costituiscono una parte fondamentale del modo di funzionamento del potere: la messa in serie di attività e l'esercizio garantiscono un controllo dettagliato della vita degli individui e la possibilità di intervenire in caso di deviazioni rispetto al cammino tracciato. Il potere si esercita direttamente sul tempo: prescrive il modo di utilizzazione del tempo e ne garantisce una stretta sorveglianza[763].

In definitiva, l'individualità-genesi si accompagna all'individualità-cellula e all'individualità-organismo quale modo di essere della società disciplinare[764].

### *L'arte della combinazione delle forze: massimizzare l'efficacia*

La disciplina non è semplicemente la scienza che permette di ripartire i corpi, di prescriverne attività e manovre e di cumularne il tempo, ma è soprattutto l'arte di comporre le forze con lo scopo di ottenere la massima efficacia possibile. Si tratta, in altri termini, di pensare un metodo mediante il quale combinare tra di loro le forze, di modo che il risultato finale sia «superiore alla somma delle forze elementari che la compongono»[765].

Ciò è evidente anzitutto nell'organizzazione militare: il soldato è l'unità elementare dell'esercito, ma a sua volta deve formare l'ingranaggio di un meccanismo più elevato (reggimento, sezione, battaglione, divisione): ogni singola operazione di ogni

[761] *Ivi*, 172-175.
[762] *Ivi*, 175.
[763] *Ibidem.*
[764] *Ivi*, 176.
[765] *Ivi*, 179.

soldato deve essere combinata con quella di un altro, il tempo dell'uno deve raccordarsi al tempo dell'altro, in modo da raggiungere una configurazione specifica e un risultato ottimale. Senza dubbio, tuttavia, tale metodologia di ingranaggi e di frammenti diversi raggiunge la sua massima espressione nell'insegnamento primario: nella scuola mutuale, il tempo di ogni allievo deve combinarsi al massimo con quello di tutti gli altri di modo che il maestro possa sfruttare al massimo le ore di insegnamento per insegnare a tutti in egual misura[766].

Questo ingranaggio di forze esige un rigido sistema di controllo e di comando: più il comando è breve e conciso, maggiore è la sua efficacia. Così, nell'organizzazione militare, il soldato deve reagire senza indugio ai comandi degli ufficiali superiori – ogni tentennamento sarebbe un crimine – mentre nell'istituzione scolastica, semplici gesti o occhiate del maestro devo essere sufficienti per riportare gli scolari alla cieca obbedienza[767].

Ecco, dunque, che si delinea l'ultimo dei quattro caratteri di cui si compone l'individualità creata dalla società disciplinare: l'individualità combinatoria, che organizza la «tattica». Una volta ripartito l'individuo nello spazio, prescritte le attività e le manovre, imposti gli esercizi ripetitivi assegnati a ciascuno, si costruisce un apparato – composto da individui – che produca un risultato maggiorato dalla combinazione calcolata delle sue forze[768].

In effetti, il potere disciplinare si propone lo scopo di addestrare: non di togliere, di punire, di sottrarre forze, ma piuttosto di scomporre, analizzare, suddividere per addestrare le forze e utilizzarle nella maniera più efficiente possibile. Non è il potere fastoso e grandioso ostentato del sovrano che esercita una vendetta privata e pubblica, mediante lo spettacolo di violenza insito nel supplizio, ma piuttosto è un potere modesto, calcolato, quasi segreto, ma permanente[769].

---

[766] *Ivi*, 179-181, che riprende il pensiero di uno dei massimi sostenitori della scuola mutuale, Samuel Bernand, esemplificando il concetto appena espresso: «In una scuola di 360 bambini, il maestro che volesse istruire ogni allievo singolarmente, non potrebbe, in una seduta di tre ore, dare a ciascuno che mezzo minuto. Col nuovo metodo, tutti i 360 allievi scrivono, leggono o fanno di conto per due ore e mezzo ciascuno».
[767] *Ivi*, 181-182.
[768] *Ivi*, 183.
[769] *Ivi*, 186.

Lo sviluppo e il prestigio della società disciplinare sono stati favoriti senz'altro dall'uso sapiente di tre strumenti fondamentali: una sorveglianza gerarchizzata, continua e funzionale, la comminatoria di sanzioni "normalizzatrici" e l'esame[770].

### *La sorveglianza gerarchizzata, continua e funzionale*

È connaturata alla società disciplinare l'esigenza di un rigido e preciso controllo: nella società disciplinare, la sorveglianza è organizzata come una rete di relazioni che si sviluppano principalmente dall'alto verso il basso, ma anche dal basso verso l'alto e collateralmente, nella quale sorvegliati e sorveglianti sono ingranaggi dello stesso meccanismo e nella quale le maglie del potere si appoggiano e si incastrano le une alle altre[771].

Durante il secolo XVIII, si sviluppa così un apparato di sorveglianza nel quale i sorvegliati sono consapevoli di essere costantemente e ininterrottamente osservati, senza sapere bene da chi o da cosa. Non si tratta di sofisticate tecnologie, che pure in quel periodo sono comparse nella scienza e nella fisica, ma piuttosto di piccole tecniche di geometrie e di forme, ove il sorvegliato è stabilmente esaminato da «sguardi che devono vedere senza essere visti» e in cui «ogni sguardo sarà una tessera nel funzionamento globale del potere»[772].

Tale sorveglianza è realizzata innanzitutto mediante lo studio dell'architettura, che sarebbe divenuta un meccanismo di trasformazione degli individui che l'edificio ospita. Non a caso, tali "osservatori" hanno come modello ideale il campo militare: le forme e le geometrie militari, il posizionamento degli ingressi degli ufficiali e dei soldati, nonché la disposizione delle file e delle righe tipiche dell'organizzazione miliare ispirano ogni aspetto della vita, dall'urbanistica alla costruzione degli ospedali, degli ospizi, delle case di eduzione, delle prigioni[773].

La società disciplinare si dà, anzitutto, un'organizzazione circolare, al cui centro il sorvegliante è in grado di osservare tutto, in permanenza, senza essere a sua volta osservato. Le architetture circolari – manifestazione plastica di una certa ideologia politica – si rinvengono nell'ospedale-edificio, che non è più un tetto dove trovano riparo

[770] *Ivi*, 186-187.
[771] *Ivi*, 194.
[772] *Ivi*, 187.
[773] *Ivi*, 187-188.

miserabili e mendicanti, ma diviene il luogo in cui tutti gli ammalati devono essere osservati bene, per impedire che essi si contagino l'uno l'altro; nella scuola-edificio, in cui gli allievi sono addestrati, suddivisi in livelli, in base al principio di difficoltà crescente; ovviamente, nelle scuole militari, in cui da una pasta informe si ricavano ufficiali competenti, corpi vigorosi e forti, soldati ubbidienti refrattari a qualsiasi forma di dissolutezza[774].

In alcuni casi, tuttavia, le istituzioni disciplinari si danno un'organizzazione piramidale che assegna un "capo" a tutti gli altri individui. È il caso degli opifici e delle fabbriche, ove gli operai sono sottoposti ad un rigido e inteso controllo da parte dei sorveglianti lungo tutto il processo di lavorazione; esso riguarda non soltanto la produzione, ma tutto il comportamento generale dei lavoratori, la loro condotta e il loro zelo. Nelle grandi manifatture, diviene, quindi, fondamentale predisporre una nuova categoria di lavoratori: sorveglianti specializzati. Lo stesso vale per l'insegnamento elementare, ove il disordine e la confusione degli allievi rende necessario individuare, tra gli studenti migliori, una serie di ufficiali, intendenti e osservatori, incaricati di sorvegliare il comportamento degli altri[775].

Insomma, mediante un gioco di spazi, di linee, di geometrie e di gradi, la sorveglianza diviene l'ingranaggio immancabile del complesso meccanismo di potere inaugurato dalla società disciplinare: si tratta di un potere che si vanta di essere perfettamente indiscreto – in quanto permea ogni spazio e luogo e non lascia zone d'ombra – e, al contempo, perfettamente discreto – dal momento che funziona come un meccanismo silente e invisibile[776].

### *La sanzione normalizzatrice*

Ogni istituzione disciplinare beneficia di un proprio ristretto sistema di giustizia, con leggi proprie, con specifici comportamenti proibiti, con forme particolari di sanzioni, con proprie istanze di giudizio. I singoli apparati disciplinari stabiliscono quei comportamenti ammessi e quei comportamenti che – nonostante sfuggano ai gradi sistemi punitivi – sono sanzionati, perché giudicati inopportuni in virtù della specifica morale che vige in quell'ambiente. La manifestazione più evidente di tale «infra-penalità» si rinviene

[774] *Ivi*, 189.
[775] *Ivi*, 192.
[776] *Ivi*, 194.

nell'ambiente militare: è obbligatorio salutare i superiori e spegnere la lampada ad una certa ora della sera, si deve tenere un certo decoro e comportarsi onestamente. Parimenti, nell'istituzione scolare è punito qualsiasi gesto o comportamento che dimostri di non tenere in debito conto gli aspetti relativi al tempo (ritardi, assenze), alle attività (interruzione del maestro, negligenza nei compiti), al modo di comportarsi (maleducazione), ai discorsi (chiacchiere durante la spiegazione), al corpo (scarsa igiene, attitudini insolenti)[777]. Il campo del sanzionabile coincide con il campo del non conforme: ogni istituzione stabilisce ciò che è conforme e ciò che non lo è.

Parallelamente, in ogni istituzione disciplinare vige un proprio meccanismo sanzionatorio: oltre ai castighi mutuati dal sistema giudiziario (frusta, ammende, celle di segregazione), essa predilige le punizioni che implicano la correzione dei difetti dell'individuo, passando per l'esercizio: per lo più, le sanzioni consistono nell'apprendimento intensificato e moltiplicato. Così, a titolo esemplificativo, nella scuola, l'alunno che non abbia svolto i compiti, sarà costretto a riscrivere o a imparare a memoria tutta la lezione del giorno successivo[778].

Ciononostante, la punizione costituisce solo un aspetto del Giano Bifronte: più che punire, la società disciplinare cerca di incentivare e gratificare. In questo sistema di addestramento e correzione, il maestro deve rendere le ricompense più appetibili del comportamento scorretto e inopportuno. Così facendo, tale sistema produce l'effetto di estremizzare i comportamenti in poli opposti: bene e male, comportamenti giusti e comportamenti sbagliati[779].

Insomma, tale sistema punitivo è strettamente funzionale all'esigenza della società disciplinare di incasellare e ordinare. Nel gioco della disciplina, si avanza e si conquistano ranghi tramite il meccanismo delle ricompense, mentre si retrocede mediante il meccanismo della punizione[780].

Nella medesima ottica, a differenza di quello giudiziario, il sistema punitivo proprio della società disciplinare è volto non tanto alla repressione o all'espiazione, quanto piuttosto a differenziare gli individui, mediante l'introduzione di una soglia minima di comportamento con cui tutti devono rapportarsi e rispetto alla quale tutti

[777] *Ivi*, 195.
[778] *Ivi*, 197.
[779] *Ivi*, 197.
[780] *Ivi*, 198.

saranno giudicati, nonché a misurare in termini quantitativi ogni modo di agire e a gerarchizzare in termini qualitativi le abilità, le capacità e la natura di ogni individuo. A tal fine, si tracciano linee che segnano le differenze tra l'uno e l'altro individuo, si incasella, si esclude se l'individuo non rispetta determinati *standard:* tutto ciò, con lo scopo ultimo di rendere conformi gli individui ad un certo modello ideale. In definitiva, la sanzione tende a omogeneizzare, categorizzare, normalizzare[781].

Ebbene, da un lato, il potere di normalizzazione costringe all'uniformità e all'omogeneizzazione, dall'altra permette di distribuire i ranghi, individuare i livelli, determinare gli scarti, differenziare le potenzialità di ciascun individuo in virtù della loro utilità. Di conseguenza, il grado di normalità assegnato a ciascuno diviene uno *status,* nel senso che indica l'appartenenza ad un certo corpo sociale i cui membri si somigliano gli uni agli altri[782].

Creando un sistema di uguaglianza formale, si instaura così il potere della Norma (intesa come conformismo), che si affianca ai poteri già esistenti nella società disciplinare: potere della Legge, della Parola, della Tradizione. In definitiva, la disciplina fabbrica un individuo che tende ad essere Normale[783].

### *L'esame, sorveglianza normalizzatrice*

Elemento imprescindibile delle istituzioni disciplinari è costituito dall'esame. Congiungendo le tecniche della sorveglianza gerarchizzata e della sanzione normalizzatrice, costituisce lo strumento per eccellenza che permette di controllare l'individuo, classificandolo, qualificandolo, differenziandolo e, all'occorrenza, punendolo. Si tratta, in altri termini, di una sorveglianza normalizzatrice[784].

---

[781] *Ivi*, 200, che riporta un esempio di tale ideologia: il sistema di classificazione "onorifica" pianificato nella Scuola miliare, ove gli allievi, in base alla loro condotta e alle loro qualità formali, sono ripartiti in classi, ciascuna delle quali individuata da un segno distintivo (il colore della spallina): la classe «dei molto buoni», la classe «dei buoni», la classe «dei cattivi», la classe «vergognosa». Ogni allievo può salire di livello, qualora se ne renda degno oppure scendere di livello, qualora il rendimento e le qualità morali non siano costantemente all'altezza delle aspettative. Questa penalità gerarchizzante produce, così come ideata, un duplice effetto: da un lato, distribuire gli allievi in base alle proprie attitudini e alla propria condotta; dall'altro lato, esercitare su di loro una certa pressione in modo da costringerli ad appiattirsi verso un determinato modello precostituito. In sostanza, tutti devono assomigliarsi.
[782] *Ivi*, 201.
[783] *Ibidem.*
[784] *Ivi*, 202.

Per tale motivo, in ogni apparato istituzionale, l'esame è una specie di cerimonia che riveste particolare importanza. Esso segna il rito di passaggio tra un livello e l'altro, tra un rango e quello successivo[785].

Inoltre, l'esame rende evidente il capovolgersi dell'«economia della visibilità nell'esercizio del potere»: tradizionalmente, è il potere che si manifesta, che si mostra e che, paradossalmente, trova legittimazione nella sua ostentazione, mentre coloro che subiscono il potere rimangono nell'ombra. Al contrario, nella società disciplinare, il potere è invisibile, immobile, ed è proprio l'invisibilità che mantiene in soggezione colui che è sorvegliato, mentre quest'ultimo è pienamente visibile[786]. Si pensi, a titolo esemplificativo, all'organizzazione dell'ospedale, che a partire dalla seconda metà del Settecento diviene un apparato per esaminare: il medico, venuto dall'esterno, entra nell'ospedale per visitare l'ammalato; tali visite divengono sempre più frequenti, fino a diventare delle ispezioni regolari, mentre i malati sono sottoposti ad un potere esaminatore quasi ininterrotto[787].

### 4.1.3. *(Segue):* Una nuova fisica del potere: il panoptismo

Nel corso dei secoli XVII e XVIII, grazie ad un vasto numero di processi storici, economici, giuridico-politici e scientifici[788], i dispositivi disciplinari si moltiplicano attraversando tutto il corpo sociale[789].

La disciplina non si esaurisce né in un'istituzione né tantomeno in un apparato; essa, piuttosto, può essere definita come una modalità di organizzare e di esercitare il

[785] *Ivi*, 207.
[786] *Ivi*, 205.
[787] *Ivi*, 203.
[788] Inizialmente, le discipline cercano di rispondere ad una congiuntura storica ben nota. Difatti, alla vigilia della Rivoluzione francese, in Francia, aumenta drasticamente la popolazione: aumenta la popolazione scolastica, come si moltiplicano anche la popolazione ospedalizzata e il capitale umano impiegato nelle fabbriche. L'aumento demografico porta con sé la problematica di controllare e gestire con urgenza questo continuo flusso umano. Contemporaneamente, si pone il problema di gestire i costi sempre più ingenti dell'apparato produttivo, rispetto al quale si cerca di aumentare anche la produttività (intendendo per produzione non solo la produzione di beni e servizi, ma anche la produzione di sapere, di salute, delle forze armate). La vecchia economia di potere si trova impreparata: né le strutture del potere feudale né i vecchi ingranaggi amministrativi della monarchia, né tantomeno la loro sovrapposizione è in grado di dare una risposta alla molteplicità delle istanze culturali, scientifiche e umane di quegli anni. L'*Ancien Régime* si reggeva, infatti, su strutture instabili, irregolari e lacunose, oltre che economicamente dispendiose. La società deve adeguarsi per non sopperire. Anche il sorgere di un'economia capitalistica ha permesso lo sviluppo di un nuovo metodo di organizzazione del potere, fondato su una tecnologia dell'assoggettamento sottile e calcolata. Per maggiori approfondimenti sulle ragioni storiche che hanno costituito il terreno fertile per il prosperare delle discipline, si veda, in particolare, *ivi,* 237 ss.
[789] *Ivi*, 228.

potere, mediante tutta una serie di procedimenti, di logiche e di livelli di applicazione che sono disserrati da luoghi determinati e chiusi fino a permeare tutto il corpo sociale[790]. In apparenza, le discipline non sono che la risposta ad un problema sociale, le quali però progressivamente si emancipano da esso e tratteggiano un nuovo tipo di società[791].

La rappresentazione plastica di questa nuova fisica del potere è costituita dal *Panopticon* di Bentham[792]. Il modello ideato dal filosofo e giurista sul finire del XVIII secolo è noto: si tratta di un'architettura circolare articolata su più piani, al cui centro si staglia una torretta corredata di grandi finestre che si affacciano verso l'interno; la costruzione periferica contiene al suo interno numerosissime celle tagliate da due finestre: l'una si affaccia verso l'interno, in corrispondenza della finestra della torretta, mentre l'altra, affacciandosi verso l'esterno, è penetrata da un grande fascio di luce. In tal modo, è sufficiente posizionare un sorvegliante nella torre centrale e rinchiudere in ogni cella un malato, un condannato, un operaio, uno scolaro: per effetto del riflesso della luce, il sorvegliante è in grado di vedere i detenuti nelle celle. In ogni cella, ogni individuo è solo, perfettamente individualizzato e sempre visibile dal sorvegliante. Invece, i grandi muri laterali che separano una cella dall'altra impediscono al detenuto di entrare in contatto con gli altri compagni[793].

Per mezzo di un simile apparato architettonico, il dispositivo panottico permette, da un lato, di evitare il sovraffollamento tumultuoso della massa tipico dei luoghi di detenzione, mentre dall'altro, consente al sorvegliante di vedere senza essere visto. In ciò consiste l'effetto principale indotto dal *Panopticon:* il prigioniero è mantenuto in uno stato permanente di visibilità, nella consapevolezza di poter essere osservato, senza che egli sappia di essere sorvegliato effettivamente. Il detenuto è in potenza costantemente e ininterrottamente osservato. È sufficiente ma non necessario la sorveglianza: è sufficiente che egli sappia di essere osservato, ma non è necessario che lo sia effettivamente. La sorveglianza è «permanente nei suoi effetti, anche se è discontinua nella sua azione»: in ciò consiste la perfezione del modello benthamiano. Difatti, il *Panopticon* è incentrato essenzialmente sul principio della visibilità e inverificabilità: il potere esercitato è continuo, ininterrotto, in quanto il detenuto – stagliandosi davanti ai suoi occhi la sagoma del sorvegliante che erompe dalla torretta – ha l'impressione di essere costantemente

[790] *Ivi*, 235.
[791] *Ivi*, 236.
[792] J. BENTHAM, *Panopticon ovvero la casa d'ispezione,* con interventi di M. Foucault e M. Perrot, Marsilio, Venezia, 2009.
[793] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione*, Einaudi, Torino, 2014, 218.

spiato; ma al contempo, il potere è inverificabile, in quanto egli non è in grado di controllare la presenza o l'assenza del guardiano. A tale scopo, infatti, dalla cella il detenuto non può neppure scorgere un'ombra o vedere una sagoma in controluce, perché le persiane alle finestre della torretta glielo impediscono[794].

Il *Panopticon* assicura, così, il funzionamento automatico e deindividualizzato del potere: il dispositivo panottico si regge non tanto sulla persona del sorvegliante, quanto piuttosto su una distribuzione calcolata degli spazi, della luce, delle superfici, degli sguardi. È indifferente chi esercita il potere, così come poco importa del motivo del suo esercizio. Ciò che importa è che il detenuto abbia la costante e inquietante sensazione di essere spiato[795].

Il Panottico è un meccanismo di poteri asimmetrici, volto a sostituire la lugubre cerimonia punitiva, i segni, i marchi e la violenza con la sorveglianza ininterrotta, che più di questi è in grado di costringere il condannato a tenere una buona condotta: colui che è sottoposto a questo gioco di potere lo sa e se ne fa carico; senza alcuno scontro fisico, inscrive in se stesso il potere che lo controlla e non ha altra scelta che divenire obbediente[796].

Tale modello si inscrive perfettamente nell'esigenza della società disciplinare di individuare, incasellare, classificare, organizzare. Innanzitutto, il metodo dell'incasellamento disciplinare tipico del *Panopticon* funziona in base ad uno schema di divisione binaria: pazzo-non pazzo; malato-sano; pericoloso-non pericoloso; virtuoso-non virtuoso[797]. In effetti, esso permette di differenziare: l'ammalato deve essere separato dal sano senza che i miasmi circolino nell'ospedale; gli scolari, che non possono copiare o imitare, sono osservati attentamente e suddivisi in gruppi in base alle attitudini, alla natura, alle capacità; negli operai, si possono notare i tempi che impiegano per svolgere un lavoro e si possono differenziare i salari in base ai risultati[798]. Inoltre, esso si fonda su un modello di assegnazione coercitiva: permette di stabilire chi è il detenuto, come riconoscerlo, come esercitare su di lui un controllo costante e ininterrotto, come giudicarlo, come incasellarlo[799]. Il *Panopticon,* in aggiunta, funziona come un «laboratorio di potere»: esso permette di fare esperimenti sociali e, di conseguenza,

[794] *Ivi*, 219.
[795] *Ivi*, 220.
[796] *Ivi*, 221.
[797] *Ivi*, 217.
[798] *Ivi*, 222.
[799] *Ivi*, 217.

modificare il comportamento dei prigionieri: provare differenti punizioni sui prigionieri e stabilire quella più efficace; insegnare differenti tecniche ad operai e verificare quella migliore; sperimentare diverse tecniche pedagogiche e capire se ognuno può imparare qualsiasi cosa. Infine, lo stabilimento panoptico opera al suo interno anche il controllo dei propri meccanismi di potere: il direttore controlla anche se stesso, in quanto sperimenta su di sé l'efficacia dei legami che ha instaurato e delle capacità che ha messo in campo. Così, il medico che non è stato in grado di arginare i contagi, sarà egli stesso contagiato, il direttore della prigione incompetente sarà il primo destinatario delle rivolte dei detenuti[800].

Il successo del modello panoptico riposa essenzialmente su tre criteri: in base al principio di economicità, esso assicura che l'esercizio del potere sia il meno costoso possibile (sia da un punto di vista economico, in quanto è sufficiente che vi sia un solo sorvegliante, sia da un punto di vista politico, in quanto è un sistema che si autoalimenta, non essendo necessario l'uso della forza e della violenza, bastando la sua discrezionalità e la sua invisibilità); in base al principio di efficienza, esso fa sì che l'esercizio del potere sia il più veloce possibile; in base al principio di efficacia, esso mira a rendere gli effetti di tale potere al massimo della loro intensità ed estensione, senza lacune o difetti[801].

Riesaminando il *Panopticon* di matrice benthamiana, Foucault sostiene che tale modello si sia esteso, nel corso del XVIII secolo, a tutte le istituzioni di potere: sebbene Bentham lo abbia ipotizzato come un meccanismo chiuso su di sé, quale ideale della perfetta detenzione, Foucault ne lumeggia un funzionamento generalizzabile a tutti gli ingranaggi della società. In effetti, il dispositivo panottico è una figura di tecnologia politica che si astrae dall'uso specifico della prigione per applicarsi ai vari canali del potere: ospedali, scuole, prigioni, fabbriche, esercito, case di correzione, asili psichiatrici, stabilimenti di educazione sorvegliata[802]. Esso rappresenta un metodo di esercizio del potere, un modo in cui il potere si organizza, un tipo di inserimento delle persone nello spazio, un tipo di organizzazione gerarchica, con i suoi strumenti e le sue modalità di intervento. In definitiva, ogni volta che si dovrà mantenere sotto sorveglianza una moltitudine di persone, il *Panopticon* potrà essere utilizzato[803].

[800] *Ivi*, 222-223.
[801] *Ivi*, 237.
[802] *Ivi*, 215.
[803] *Ivi*, 224.

In definitiva, tale architettura panottica può vantarsi di essere polivalente, in quanto è in grado di insinuarsi in ogni congiuntura del potere, adattandosi a svolgere qualsiasi funzione (di educazione, di produzione, di terapia, di punizione) e maggiorare tale funzione sfruttando la correlazione diretta tra «il più di potere» e «il più di produzione». In questo caso, l'esercizio del potere non proviene dall'esterno, ma piuttosto è volto a sorvegliare gli ingranaggi dall'interno, in modo sottile e silente[804]. Dunque, tale modello risulta idoneo a «riformare la morale, preservare la salute, rinvigorire l'industria, diffondere l'istruzione, alleggerire le cariche pubbliche, stabilizzare l'economia come sulla roccia, sciogliere, invece di tagliare, il nodo gordiano delle leggi sui poveri; tutto questo con una semplice idea architettonica»[805].

In definitiva, il panoptismo disegna una nuova fisica del potere, ponendosi agli antipodi rispetto a quel sistema di assoggettamento del corpo attuato mediante violenza tipico dell'*Ancien Régime:* fino al XVIII secolo, il sovrano dispiega sul corpo del condannato tutta la sua forza materiale e il castigo sembra eguagliare, se non superare, il delitto compiuto nella sua essenza selvaggia; dal XVIII secolo in poi, invece, l'anatomia politica sottesa al modello panottico assume le sembianze di un potere permanente, di una sorveglianza onnipresente, in grado di guardare tutto a patto di non essere mai guardata[806].

### 4.1.4. *(Segue):* La nascita della prigione, luogo di sorveglianza per antonomasia

Il *Panopticon* di Bentham – luogo di sorveglianza e di osservazione, nonché di conoscenza e di individualizzazione – ha trovato la sua più compiuta e perfetta realizzazione nella prigione[807]. Contrariamente a quello che si potrebbe pensare, infatti, la prigione non è un elemento endogeno nel sistema penale – come abbiamo visto, nell'epoca dei Lumi i riformatori avevano ipotizzato tutt'altra tipologia di pena – ma è piuttosto la logica prosecuzione dei meccanismi propri della società disciplinare. Siffatta eterogeneità rispetto al sistema penale, tuttavia, non ha impedito che i meccanismi della prigione penetrassero nel tessuto della giustizia punitiva[808].

[804] *Ivi*, 225.
[805] J. BENTHAM, *Panopticon,* in *Works,* ed. Bowring, tomo IV, 1843, 65.
[806] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione*, Einaudi, Torino, 2014, 233.
[807] *Ivi*, 272.
[808] *Ivi*, 280.

Se è vero che a cavallo dei secoli XVII e XVIII le raffinate tecniche disciplinari, come modalità concreta di esercizio del potere, hanno avuto larghissima diffusione in tutto il corpo sociale, è pur vero che il tema del *Panopticon* ha potuto materializzarsi solo nelle istituzioni penitenziarie[809]: tramite la prigione si traduce «nella pietra l'intelligenza della disciplina»[810].

Il dispositivo panottico, infatti, a partire dagli anni 1830-1840, ispira la gran parte delle planimetrie delle prigioni[811]. In effetti, sorge l'esigenza che le prigioni siano progettate come macchine azionate da un solo motore[812], con numerose celle in cui si troveranno i detenuti e una torretta centrale dalla quale un osservatore permanente sarà in grado di controllare contemporaneamente detenuti e guardiani. Queste necessità si possono tradurre in un'architettura dalle numerose varianti: innanzitutto, il classico *Panopticon* ideato da Bentham nella sua forma più rigorosa, ma anche il semicerchio o la pianta a croce o la disposizione a raggi[813]. L'utopia che guida i vari progetti di prigione è sempre la stessa: tutta la prigione deve essere costruita in modo tale che dalla sala centrale di ispezione il sorvegliante sia in grado di operare un controllo continuo, ininterrotto, generale; tale sorveglianza sarà stata perfetta se dalla torretta il direttore sarà stato in grado di guardare senza essere visto dai detenuti; «uno sguardo senza volto» deve costantemente monitorare non solo i detenuti nelle loro celle, ma anche i guardiani di ogni piano incaricati di controllare i detenuti[814].

A cavallo dei due secoli, il *Panopticon* penitenziario, già modalità di esecuzione della pena, funge contemporaneamente da luogo di studio degli individui puniti, secondo una duplice prospettiva: certamente, da un lato, i detenuti sono costantemente sorvegliati; dall'altro lato, è necessario che di ogni detenuto sia annotato e registrato tutto ciò che riguarda la sua condotta, il suo comportamento, le sue credenze morali, il suo progressivo miglioramento[815]. Si comprende bene, allora, che la prigione diviene anche un «sistema di documentazione individualizzante e permanente»: nel corso del XVIII secolo, in Francia, è reso obbligatorio il c.d. "resoconto morale" del detenuto, vale a dire un documento da cui risulti l'osservazione del detenuto e che riporti informazioni che

[809] *Ivi*, 272-273.
[810] C. LUCAS, *De la réforme des prisons,* tomo I, 1838, 69.
[811] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione*, Einaudi, Torino, 2014, 272-273.
[812] L. P. BALTARD, *Architectonographie des prisons,* 1829, 4-5.
[813] M. FOUCAULT, *Sorvegliare e punire: nascita della prigione*, Einaudi, Torino, 2014, 273.
[814] *Ivi*, 274.
[815] *Ivi*, 272.

trascendono le circostanze del crimine, ma che riguardano piuttosto la storia della sua vita, la sua organizzazione, la sua educazione e posizione sociale. Si fa strada l'idea che il delinquente è legato al delitto commesso da una serie di relazioni complesse (carattere, abitudini, educazione, pulsioni, istinti). L'introduzione di questa inchiesta biografica, all'apparenza banale, ha segnato un nuovo importante approdo nella storia della giustizia criminale, perché mette al centro della modello penitenziario la persona prima del delitto compiuto e al di fuori di esso[816].

Ad ogni modo, dentro la prigione, il direttore è tenuto, oltre che a sorvegliare, anche a conoscere il detenuto: se la decisione del giudice deve applicare la legge e ha come suo perno il delitto commesso, la pratica penitenziaria deve prelevare dal detenuto un sapere che funga da principio regolatore della sua permanenza in prigione[817].

Ebbene, la prigione aspira a divenire un apparato disciplinare onnicomprensivo, da diversi punti di vista: innanzitutto – molto di più della scuola, della fabbrica o dell'esercito, che sono istituzioni specializzate – l'istituto penitenziario deve farsi carico di ogni aspetto della vita dell'individuo, dal suo addestramento fisico alla sua dignità morale, dalle sue attività quotidiane al lavoro. Inoltre, esso è una istituzione chiusa, che presuppone una disciplina incessante, finché il suo obiettivo – la rieducazione del condannato – non sia stato portato a compimento. In aggiunta, la prigione mira ad essere, oltre che individualizzante, anche totalizzante, perché costringe il detenuto a

[816] *Ivi*, 277.

[817] *Ivi*, 267-271 e 274-275, ove si sottolinea che la prigione aspira a divenire uno «strumento di modulazione della pena», nel senso che, sin dalla sua nascita, l'istituzione carceraria rivendica il diritto – concesso fino agli ai secoli XIX e XX solamente in forma frammentaria – di abbreviare o prolungare la pena a seconda delle circostanze, come condizione di buon funzionamento della prigione e di efficacia della pena quale strumento di rieducazione del condannato: in base a tale ideologia, se fosse fissata a livello giudiziario una volta per tutte, senza possibilità di modulazione, la rischierebbe di privarsi del suo valore correttivo. Tant'è che numerosi giuristi propongono delle misure di "libertà preparatoria" o "supplementi afflittivi" quando la pena concretamente fissata dal giudice, rispettivamente, ecceda il tempo necessario per la riqualificazione del detenuto ovvero, all'opposto, non produca i risultati sperati: si veda, a tal proposito, A. BONNEVILLE, *Des libérations préparatoires,* 1846, 6. Senza pretesa di esaustività sul tema, basti qui ricordare che, alla vigilia della Rivoluzione francese, da più parti si sottolineava che la pena dovesse adattarsi alla trasformazione «utile» del condannato, con la conseguenza che la giusta pena dovesse variare non solo in funzione del delitto commesso e delle sue circostanze, ma anche in funzione delle necessità di emendamento dell'individuo punito, oggetto di trasformazione permanente. Si arriva, dunque, ad un principio, formulato dall'avvocato e giurista C. Lucas – riformatore del sistema penitenziario – già allora molto dibattuto e che ancora oggi si fa fatica ad accettare senza riserve: il sistema penitenziario vuole emanciparsi dalle rigide maglie del sistema propriamente giudiziario. Detto diversamente, il sistema carcerario, oltre alla sua autonomia amministrativa, rivendica «una parte della sovranità punitiva». Di tal guisa, la sentenza del tribunale non è che un pre-giudicare, in quanto le attitudini morali e la capacità di cambiamento del detenuto non possono essere valutate che alla prova. In ciò si apprezza il fondamentale ruolo svolto dal guardiano nella prigione panottica.

un'educazione totale. Essa, dunque, «porta alla intensità massima tutte le procedure che si trovano negli altri meccanismi disciplinari»[818].

Certamente, non bisogna trascurare che quando, a cavallo dei secoli XVII e XVIII, la detenzione diviene nel Codice penale francese la pena per eccellenza, la forma-prigione esiste già nell'apparato giudiziario (sebbene confinata a pena di certi delitti o pena sostitutiva), nel senso che l'apparato giudiziario reperisce un meccanismo di coercizione già elaborato altrove e lo eleva a forma generalizzata di pena; tuttavia, ciò che qui preme sottolineare è il motivo di tale transizione al modello della detenzione penale, a discapito di modelli che pure erano stati proposti dai riformatori illuministi dell'epoca[819]. Invero, la prigione si inscrive perfettamente in quelle procedure elaborate per ripartire nello spazio gli individui, per distribuirli, classificarli, addestrare il loro corpo, ricavandone un'utilità maggiorata dalla combinazione calcolata delle forze. In definitiva, i meccanismi disciplinari colonizzano anche l'apparato giudiziario[820].

È inutile negare che, nei primi anni del XIX secolo, si ha ancora coscienza della sua estraneità rispetto al precedente impianto di espiazione della pena; tuttavia, la prigione appare così intimamente legata al funzionamento della società disciplinare che è in grado di far cadere nell'oblio tutte le altre tipologie di pena che pure i riformatori illuministi avevano proposto e che apparivano comunque valide. Ancora oggi, sebbene non perfetta, la detenzione appare «la detestabile soluzione, di cui non si saprebbe fare a meno».[821]

Il successo e la solidità del sistema carcerario, che peraltro arriva con poche modificazioni fino ai giorni nostri, riposano su un duplice fondamento. Da una parte, in esso si rinviene un fondamento giuridico-economico, in quanto si fonda sulla forma della privazione di libertà – bene che appartiene a tutti nello stesso modo e cui tutti sono profondamente legati – e, in più, la detenzione consente di quantificare esattamente la pena in termini di giorni, mesi, anni[822]. Dall'altro lato, tuttavia, sin dall'inizio, la prigione non è semplice privazione della libertà, ma aspira a ricoprire il ruolo di motore di trasformazione degli individui; il suo fondamento tecnico-disciplinare si appunta dunque

[818] *Ivi*, 257.
[819] Si tratta dell'archetipo disegnato dai giuristi riformatori: si veda, *amplius,* il paragrafo §4.1.1 e la nota n. 65, che riassume i tre diversi modelli esistenti alla vigilia della Rivoluzione francese.
[820] *Ivi*, 251.
[821] *Ivi*, 252.
[822] La pena della detenzione, in sostanza, sottrae all'uomo ciò che ha di più caro: il tempo. Dunque, essa ha un contenuto egalitario, molto più dell'ammenda, in quanto la perdita di libertà ha lo stesso valore per tutti. Inoltre, il tempo può essere facilmente monetizzato: ogni delitto può essere pagato mediante frazioni di tempo.

nella circostanza che, sin dal principio, alla prigione fu attribuita la funzione di emendamento del condannato: privato il detenuto della sua libertà e del suo tempo, rinchiuso nella sua cella, addestrato, riconciliato con le idee di ordine, moralità e rispetto, riprodotti in uno spazio chiuso tutti i meccanismi propri della società disciplinare, il condannato torna nella società finalmente educato[823].

In definitiva, a cavallo dei secoli XVII e XVIII, il corpo marchiato, bruciato, arso vivo e polverizzato del supplizio lascia il posto al corpo del prigioniero, che – tramite i raffinati meccanismi del potere disciplinare – si cerca di rendere altrettanto sottomesso e docile senza l'uso della violenza[824].

## 4.2.Dalla biopolitica alla psicopolitica: la sorveglianza sulla mente

Mentre il potere sovrano tipico dell'*Ancien Régime* si estrinseca in un potere di vita o di morte in mano al re, agli albori del XVII secolo, il potere disciplinare si manifesta come una «scrupolosa amministrazione dei corpi» e una «pianificazione contabile della

[823] *Ivi*, 252-254, ove si sottolinea che sin dai Codici penali francesi del 1808 e 1810, la detenzione non ha mai coinciso con la semplice privazione di libertà. Perché il condannato potesse tornare in società emendato, sono stati previsti precisi meccanismi di ricodificazione dell'esistenza dell'individuo: essenzialmente, l'isolamento e il lavoro. Innanzitutto, l'isolamento dei detenuti – sia rispetto al mondo esterno sia rispetto agli altri detenuti – è stato letto come un dispositivo di riforma: mediante l'isolamento, sono recise tutte le sue relazioni con quel fascio di fili complessi (altri condannati, istinti, ambiente negativo) che hanno condotto l'individuo in prigione; inoltre, per mezzo della riflessione e dei rimorsi che esso suscita, il condannato è messo nella condizione di dialogare con se stesso, senza interferenze esterne, da cui può trarre la forza per un positivo emendamento; soprattutto, la solitudine dolorosa crea le condizioni necessarie perché il detenuto possa essere totalmente sottomesso al potere che si esercita su di lui: per tale via viene assicurata non solo la sorveglianza sui suoi movimenti, ma specialmente la sorveglianza dei suoi pensieri e della sua anima. In particolare, il modello di Auburn si fonda sull'isolamento notturno e sulla comunicazione esclusivamente con i guardiani, con la conseguenza che «gli individui sono isolati nell'esistenza morale, […] non potendo la comunicazione avvenire che in senso verticale». Invece, il modello di Filadelfia, in cui l'isolamento è assoluto, si fonda sulla convinzione che il detenuto debba essere riqualificato non tanto dalla legge e dal timore della punizione, cioè da un potere esterno, ma piuttosto dal lavoro della sua coscienza, cioè un potere interiore. Ad ogni modo, in linea generale, il lavoro accompagna l'isolamento per sei giorni a settimana, mentre la domenica è consacrata alla preghiera e alla meditazione solitaria. E così trascorrono le settimane, i mesi, gli anni. Il prigioniero familiarizza con il lavoro, principale mezzo di reinserimento nella società, e con le soddisfazioni che ne derivano. Nonostante il malcontento della popolazione per il lavoro retribuito in carcere, la risposta data dall'amministrazione penitenziaria è sempre la stessa: il lavoro in prigione non deve essere letta come attività di produzione di beni o servizi, ma piuttosto deve essere inteso come un mezzo che genera effetti positivi nella meccanica umana. Esso si afferma sempre più come criterio di ordine e disciplina: occupando la giornata del detenuto, gli si danno delle regole che verranno poi riprodotte nella società esterna, allontana i pensieri di rivolta e di agitazione, si trasforma un uomo, che da violento e impulsivo lo si rende attivo e propositivo. Il salario non assume la forma di retribuzione per una prestazione eseguita, perchè non è altro che un ingegno per rendere l'individuo propenso al lavoro e alla disciplina, insegna ai malfattori il senso della proprietà, nonché l'attitudine al risparmio, alla previdenza e la predisposizione al futuro. Soprattutto, il lavoro insegna ai detenuti il rispetto della gerarchia, la sottomissione individuale ed è in grado di costruire un rapporto di potere in senso verticale.

[824] *Ivi*, 279.

vita»[825]; ad ogni modo, entrambe le tipologie di potere attuano una coercizione sul corpo che fabbrica il soggetto d'obbedienza[826]. Le tecniche disciplinari, tuttavia, non hanno accesso agli strati più profondi della psiche: nel *Panopticon* di Bentham, il sorvegliante controlla i detenuti dall'esterno, osservandone i movimenti e i comportamenti, ma non realizza una reale manipolazione dei suoi pensieri e bisogni intimi[827].

Per tale motivo, la biopolitica – tecnica di governo su cui si fonda la società disciplinare – entra in crisi con l'affermarsi del regime neoliberale: essa si limita al controllo minuzioso del corpo, ma non ha alcun accesso allo "psicoprogramma" del singolo e della collettività[828].

A differenza di quanto profetizzato da Karl Marx, il filosofo sudcoreano con cattedra all'Università di Berlino Byung-Chul Han, nella sua *"Psicopolitica"*[829] ritiene il capitalismo industriale non abbia condotto ad una società comunista, ma che – sulla soglia del XX secolo – si sia evoluto in neoliberalismo e in capitalismo finanziario, entrambi connotati da forme di produzione immateriali[830]. In questa nuova articolazione del potere, il lavoratore non lotta contro un'opposta classe sociale, ma cerca di sfruttare se stesso – il proprio tempo e le proprie potenzialità – per costruire la propria impresa immateriale. Per tale via, la lotta di classe si è evoluta in una lotta interiore contro se stessi. Si è fatta strada l'idea che ognuno di noi, in quanto progetto, è capace di «un'autoproduzione illimitata»: l'individuo non può permettersi di fallire e se fallisce, se non si sfrutta appieno, si ritiene responsabile e indirizza la sua aggressione non verso l'esterno, ma verso l'interno[831].

A cavallo dei secoli XX e XXI, l'uomo non lavora più per soddisfare i propri bisogni, ma per sentirsi libero; l'imprenditore di se stesso si trova intrappolato in un

[825] *Ivi*, 121.
[826] B.-C. HAN*, Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 29.
[827] *Ivi*, 31.
[828] *Ibidem.*
[829] Nel suo saggio *"Psicopolitica",* così come anche negli altri suoi saggi che sono serviti alla presente analisi per tracciare la parabola che va dalla biopolitica alla psicopolitica (quali *"La società della trasparenza"* e *"Nello sciame"*), è evidente che il filosofo sudcoreano Han sia rimasto legato alla tradizione lirica tipica dell'Estremo Oriente: sebbene egli abbia studiato filosofia e letteratura a Berlino insieme con il filosofo e sociologo Habermas, Han ha mantenuto il linguaggio onirico e disincantato tipico della sua terra d'origine, senza però rinunciare a schiettezza e perspicacia. Han descrive la società odierna senza mezzi termini, ma appare al tempo stesso laconico e sfuggente.
[830] *Ivi*, 13-14.
[831] *Ivi*, 14-16.

aggrovigliato nodo gordiano, in cui sfrutta la propria libertà con l'illusione che il lavoro gli restituisca libertà; invece, diventa servo del lavoro e di se stesso[832].

Il regime neoliberale tende a sfruttare non solo il tempo (si pensi all'individualità-genetica, votata al cumulo e alla capitalizzazione del tempo, tipica della società disciplinare), ma l'intera persona, tutte le sue risorse personali e tutta la sua attenzione[833]. Le tecniche di controllo neoliberale si appuntano sempre più sull'auto-ottimizzazione del tempo e delle capacità cognitive; ogni pensiero negativo deve essere convertito in positività; non c'è più spazio per l'ozio e per il riposo fine a se stesso. Ogni attività, ogni gesto, ogni rapporto deve essere funzionale al lavoro e alla *performance.* La psiche è manipolata al punto che il soggetto si lascia sottomettere dalla cultura della positività: non c'è tempo per pensare, per interiorizzare; non c'è spazio per debolezze ed errori. Il Super-Io lotta incessantemente contro se stesso in nome dell'efficienza. Addirittura il dolore – sentimento negativo per eccellenza – può essere sfruttato, nella misura in cui l'insoddisfazione può fungere da molla per migliorare la propria vita[834].

Dunque, quale forma di mutazione del capitalismo, il neoliberalismo non pone più al centro il corpo e tutto ciò che è biologico, ma si interessa quasi esclusivamente della psiche. Nel corso dei secoli XX e XXI – dominati da forme di produzione immateriali e incorporee – accanto ai beni materiali, si iniziano a produrre programmi, *software* e, soprattutto, informazioni. Allo scopo di accrescere la produttività, il potere non si interessa più di tutto ciò che è corporale, come nella società biopolitica, ma inizia a sfruttare e ottimizzare i processi psichici o mentali[835].

---

[832] *Ivi*, 16.

[833] Non sono infrequenti, nella società digitale, *workshop* motivazionali e corsi di *automanagement* organizzati nel fine settimana, che promettono un incremento dell'efficienza. Soprattutto nella società americana, si parla di "guarire" dalle proprie debolezze e blocchi interiori per poter avere accesso ad una nuova vita. Han dice: «Guarire non è altro che uccidere»: nella cultura della positività tossica, l'anima umana muore sotto il peso dell'efficienza. Per un approfondimento, si veda B.-C. HAN, op. cit., 39-42.

[834] *Ivi*, 39-41.

[835] *Ivi*, 34. Il filosofo sudcoreano ricorre a due metafore tratte dal mondo animale per descrivere, rispettivamente, gli abitanti della società disciplinare e della società del controllo neoliberale: i detenuti negli ambienti di internamento descritti da J. Bentham e M. Foucault possono essere paragonati alla talpa, nella misura in cui essa si muove in un ambiente chiuso e controllato, essendo *ab externo* ripartito e classificato in spazi pre-installati; tuttavia, anche quando lavora in modo disciplinato e ordinato, la talpa non potrà mai superare un certo livello di produttività. Per tale motivo – con l'affermarsi di nuove forme di produzione post-industriali, immateriali e interconnesse – il regime disciplinare che si sviluppa a partire dal XVII secolo si trasforma, a partire dal XX secolo, in un regime neoliberale, incarnato dal serpente, che mal sopporta le restrizioni e gli ambienti chiusi e si muove in spazi nuovi e sempre più aperti. La talpa rappresenta il lavoratore, sottoposto al potere disciplinare del datore di lavoro, laddove il serpente rappresenta l'imprenditore, che scopre il mondo e si fa da sé. L'immagine del serpente, tuttavia, inevitabilmente evoca anche una sensazione negativa: la colpa, che la psicopolitica digitale utilizzano come

Ecco, allora, che sulla soglia di III millennio, il corpo docile e sottomesso di matrice foucaultiana lascia spazio alla psicopolitica[836].

Mentre il sistema disciplinare è un regime biopolitico, incentrato sul corpo, la società del controllo neoliberale è un regime psicopolitico, in quanto si organizza come un'"anima", ponendo al centro dei suoi interessi la motivazione, l'emulazione, il progetto, lo spirito d'iniziativa, la *performance,* l'ottimizzazione delle azioni e dei pensieri[837].

Già il filosofo francese Bernard Stiegler paventava la possibilità che il biopotere, così minuziosamente descritto da Foucault anche dal punto di vista storico e geografico, non fosse adeguato a descrivere la forma di potere che caratterizza l'epoca contemporanea. Egli, tuttavia, poneva ancora al centro dello psicopotere l'industria telecratica – contrapposta alla tecnica del leggere e dello scrivere di Kant – ritenendo la televisione il dispositivo psicotecnico per eccellenza, nella misura in cui è capace di controllare il flusso delle informazioni[838].

Compiendo una fuga in avanti, il filosofo Han – ritenendo che, nell'epoca attuale, la televisione sia un «modello critico-culturale obsoleto, non più adatto alla rivoluzione digitale» – pone al centro del cambiamento di paradigma sociale e culturale i *media* propriamente digitali, vale a dire *Internet* e i *social media,* nonché la loro struttura comunicativa, a cui imputa il passaggio dalle tecnologie di potere alle tecnologie del Sé. A differenza dell'analisi foucaultiana, che contrappone in maniera dualistica le tecnologie del dominio individuale alle tecniche di potere e di dominio[839], Han suggerisce che il regime di dominio neoliberale si serve della tecnologia del Sé, da intendersi come l'ottimizzazione permanente delle proprie risorse individuali: è il soggetto neoliberale, imprenditore di se stesso, a prendere le deleghe del proprio controllo, guidato dal

---

mezzo di dominio (non a caso, come si dirà nel proseguo della presente trattazione, il soggetto che si ribella a questa forma di potere, che non è in grado di sfruttare appieno le risorse, è un soggetto depresso).
Per un maggiore approfondimento sul tema, si veda B.-C. HAN, op. cit., 27-28.

[836] *Ivi*, 34.

[837] *Ivi*, 28.

[838] L. DE FIORE, *Big data e psicopolitica: ancora e sempre fatti versus interpretazione? Una riflessione filosofica sul presente futuro dei big data,* in *Forward,* novembre 2016, consultabile in https://forward.recentiprogressi.it/it/rivista/numero-4-big-data/articoli/big-data-e-psicopolitica-ancora-e-sempre-fatti-versus-interpretazione/.

[839] A Foucault si deve, tuttavia, l'anticipazione del nesso tra tecnologia del potere e tecnologia del sé: in M. FOUCAULT, *Sull'origine dell'ermeneutica del sé: due conferenze al Dartmouth College,* a cura di MF/Materiali foucaultiani, Cronopio, Napoli, 2012, 39-40, si legge che – allo scopo di studiare la genealogia del soggetto nella civiltà occidentale – bisogna esaminare non solo le tecniche di dominio, ma anche le tecnologie del sé, prendendo in considerazione il rapporto tra queste due tecniche. Difatti, per un verso, occorre «considerare i punti in cui le tecnologie di dominio degli individui gli uni sugli altri fanno ricorso a processi attraverso cui l'individuo agisce su di sè», mentre per altro verso, occorre «considerare i punti in cui le tecniche di sé sono integrate in strutture di dominio e di coercizione».

desiderio di *performance* e dalla chimera del successo; mentre nel XVII secolo è il regime disciplinare a sottomettere e manipolare l'individuo, imponendo esercizi e prescrivendo manovre, nella società neoliberale è l'individuo che sfrutta «volontariamente ed entusiasticamente» le proprie risorse interiori con lo scopo di incrementare l'efficienza e le capacità performative[840].

Tale forma di potere non ha alcuna presa sul corpo, ma si appunta sulla psiche: la sorveglianza non è scomparsa dalla società, ma ha soltanto cambiato sede e modificato i propri connotati, presentandosi come un potere immanente la nostra cultura, senza un volto riconoscibile né incolpabile, sottraendosi a ogni visibilità e sfruttando la libera scelta[841].

Nella psicopolitica di matrice neoliberale, il potere abbandona la sfarzosa festa punitiva con cui si manifesta nell'*Ancien Régime* o la rigida necessità di individuare, incasellare, classificare e organizzare che connota la società disciplinare del XVII secolo e agisce silenziosamente, deponendo un modello di potere violento e negativo e offrendosi come libertà. Laddove il potere disciplinare assume una forma proibitiva – perdendosi l'individuo in un dedalo di obblighi e divieti, di costrizioni e privazioni – il modello neoliberale del potere spinge l'individuo ad essere attivo, motivato, energico ed entusiasta della propria vita, credendosi libero. Ecco, allora, tutta l'intelligenza e la duttilità con cui si manifesta il potere a partire dal XX secolo: mediante *Internet* e i *social media* – complice un gioco di piaceri e di soddisfazioni immediate – l'individuo è portato a sottomettersi da sé al rapporto di dominio. Siffatto «potere intelligente, benevolo» non sottomette, ma fa sì che l'uomo si senta libero; non è un potere repressivo, ma permissivo; non limita, ma seduce; non impone divieti, non si oppone alla volontà del soggetto, ma lo asseconda; non si fonda sul silenzio e sull'isolamento, ma invita l'individuo a comunicare continuamente, ad esprimere i suoi bisogni, preferenze, a condividere i propri frammenti di vita, a raccontare, sfruttando le emozioni positive e le gioie immediate che ne derivano[842].

Dunque, in questa nuova fisica del potere, il controllo digitale passa attraverso lo sfruttamento della libertà: l'uomo del XXI secolo non si sente un soggetto sottomesso, ma piuttosto un "progetto libero", che scopre se stesso e che si reinventa in modo

[840] [840] B.-C. HAN*, Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 37-39.
[841] *Ivi*, 25.
[842] *Ivi*, 24.

continuo[843]. Egli, tuttavia, non è consapevole di essersi legato a catene ancora più forti, difficili da spezzare: guidato dalla smania di successo e ammaliato dall'esigenza di apparire invincibile, si sottomette a costrizioni interiori e ad obblighi che si è autoimposto, tendendo all'ottimizzazione delle risorse interiori[844].

Paradossalmente, in tale contesto, non pare peregrina l'idea che attualmente questa libertà, che si oppone concettualmente all'obbligo, è essa stessa fonte di doveri e di costrizioni. Il «soggetto di prestazione», che si pensa libero, è in realtà servo di se stesso: egli è al contempo servo e padrone. Sparisce il dualismo tipico della dialettica hegeliana tra servo e padrone: qui non vi è nessun uomo in carne ed ossa che obbliga il servo a lavorare, mentre egli gode solamente. Al contrario di quanto afferma Hegel, il servo non si rende libero per mezzo del lavoro, ma diviene egli stesso schiavo del lavoro[845]; egli lavora per affrancarsi dal rapporto di soggezione che lo lega al padrone, ma poi diviene schiavo di quella sensazione di libertà. La sua libertà è soltanto apparenza. Egli sfrutta se stesso al massimo grado, divenendo imprenditore di se stesso, ma il lavoro diviene totalizzante e alienante[846].

Inoltre, il soggetto, impregnato della cultura neoliberale fin nelle sue fibre più dure, è incapace di relazionarsi con gli altri in modo libero e disinteressato: ogni azione

[843] L'individuo studiato dal filosofo Martin Heidegger è il contadino, cioè il soggetto sottoposto alla legge (νόμος, in greco antico) della terra. Al contrario, l'individuo della società neoliberale si sente un progetto in continuo divenire, che ottimizza il proprio tempo e se stesso. Per descrivere il passaggio dal soggetto al progetto, il filosofo e scrittore Vilém Flusser usa queste parole: «Noi non siamo più soggetti di un mondo oggettivo dato, bensì progetti di mondi alternativi. Dalla servile posizione soggettiva ci siamo alzati alla andatura eretta del progettare». A tal proposito, si veda V. FLUSSER, *La cultura dei media,* a cura di A. Borsari, Bruno Mondadori, Milano, 2004, 236. Come sottolineato in B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 67 ss. mentre l'ordinamento terraneo, studiato da Heidegger, poggia sulla terra, cioè un elemento materiale stabile e fermo, ed è circoscritto da confini, muri e fortezze, l'ordinamento digitale è caratterizzato dalla flessibilità e, in senso negativo, dalla instabilità e, dunque, potrebbe essere paragonato al mare, sempre in movimento. Per tale motivo, mentre il contadino dell'ordinamento terraneo ha un carattere fermo e deciso, l'*homo digitalis,* in continuo divenire, è instabile e incerto. Allo stesso modo, Spirito, azione, pensiero e verità sono le categorie che descrivono l'ordinamento terraneo; al contrario, operazione, efficienza, calcolo e trasparenza sono categorie che appartengono all'ordinamento digitale. Nella società psicopolitica, l'azione lascia spazio all'operazione: quando l'*homo faber* agisce, ha bisogno di pensare, così come anche di indugiare e dubitare. Il pensiero e il dubbio, tuttavia, rallentano l'efficienza tipica dell'operazione. Difatti, all'operazione, che procede lineare, è estraneo il pensiero: è abolita qualsiasi sorpresa, interruzione o deviazione. Anche la Verità appare una categoria ormai superata: la Verità è innestata dalla tensione negativa con la falsità e presuppone il dualismo bene-male; la Verità presenta una struttura narrativa. Tale concetto può essere meglio compreso alla luce di quanto diremo, nel proseguo della presente trattazione, nel paragrafo §4.2.2, a proposito della società dell'esposizione.

[844] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 9.

[845] *Ibidem.*

[846] *Ivi*, 11.

– anche apparentemente libera, come l'emozione, il gioco, il riposo, la comunicazione – deve raggiungere il massimo rendimento[847].

A differenza di quanto profetizzato dal filosofo e scrittore Vilém Flusser[848] – che immaginava un futuro nel quale l'*homo digitalis* avrebbe maneggiato non più oggetti ma informazioni immateriali – il digitale ha inaugurato non l'epoca dell'ozio, bensì l'epoca della prestazione. Contrariamente alla visione di Flusser, infatti, anche il gioco e il tempo libero devono obbedire alle regole della società della prestazione e dell'efficienza[849].

In generale, infatti, una linea netta separa l'ozio dal *negotium:* l'ozio inizia laddove finisce il lavoro. Il tempo dell'ozio è Altro rispetto al lavoro. Invece, nel sistema neoliberista della prestazione, tutto il tempo che abbiamo a disposizione deve essere trasformato in tempo di lavoro: il tempo va ottimizzato e sfruttato fino all'osso; la pausa non è altro che una fase del lavoro, finalizzata alla rigenerazione delle forze da convertire in forza-lavoro. Contrariamente a quanto avveniva nel passato, in cui il luogo di lavoro e i luoghi del non-lavoro erano separati fisicamente, con la conseguenza che anche il tempo di lavoro e il tempo libero erano tempi alternativi, nell'epoca contemporanea, in molte professioni, i dispositivi digitali hanno aperto la possibilità di lavorare in ogni luogo e in ogni momento: la libertà di lavorare ovunque si è rovesciata nell'obbligo di lavorare ovunque[850]. Nella società liquida[851], ove nulla assume contorni nitidi e ben definiti, anche il lavoro è divenuto fluido per via dei dispositivi digitali. Così, non è più possibile sottrarsi al lavoro. Anche qui la libertà assume i contorni della costrizione[852].

La società digitale si basa sul contare e sul calcolare: difatti, la parola "digitale" deriva da "*digitus"*, dita. In effetti, su *Facebook* si contano "gli amici"; su Instagram si contano le simpatie sottoforma di "mi piace"; tutto viene trasformato in dati e numeri che possano essere calcolati. Solo ciò che si può contato esiste. Come vedremo meglio nel proseguo[853],

---

[847] *Ibidem.*
[848] Secondo il filosofo e scrittore Vilém Flusser, l'uomo del futuro non avrebbe più avuto bisogno delle mani per lavorare e maneggiare gli oggetti, perché la società neoliberale sarebbe stata dominata da beni immateriali quali informazioni e dati. Nell'utopia flusseriana, l'*homo faber,* che crea per mezzo delle mani, avrebbe lasciato il posto all'*homo ludens,* incapace di agire e lavorare con le mani; le mani dell'individuo si sarebbero atrofizzate a causa del diffondersi dei dispositivi digitali e avrebbero lasciato spazio all'«uomo che gioca con le dita, senza mani». Per un maggiore approfondimento, si veda V. FLUSSER, *La cultura dei media,* a cura di A. Borsari, Bruno Mondadori, Milano, 2004, 205.
[849] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 48-49.
[850] *Ivi*, 50-51.
[851] Il sociologo Zygmunt Bauman parla di "modernità liquida": si veda, a tal proposito, Z. BAUMAN, *Modernità Liquida,* Laterza, Roma, 2020.
[852] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 50-51.
[853] Si veda, *amplius,* in questo Capitolo, il paragrafo § 4.2.3, a proposito dei *big data.*

i dispositivi digitali non sono in grado di raccontare alcunché. In questo senso, allora, si può dire che l'*homo digitalis* «gioca con le dita», perché conta e calcola, ma non è più in grado di raccontare del Sé[854].

Non stupisce, allora, che le malattie della nostra epoca siano la depressione e la sindrome di *burnout.* In una società che reprime i veri bisogni dell'uomo e «la forza educativa del dolore»[855], l'individuo è esautorato, represso, non è più libero di mostrare le sue debolezze[856] e, inevitabilmente, crolla sotto il peso di una colpa atavica: quella di essere umano.

Ecco, dunque, la domanda che pone il filosofo Han: *siamo sicuri di essere liberi*? Ma soprattutto, *vogliamo davvero essere liberi*?[857]

Seppure in modo laconico e talvolta lacunoso – tratteggiando i contorni sfumati della società neoliberale e delle sue dinamiche relazionali ma, contemporaneamente, lasciando spazio a ulteriori riflessioni – nella sua *"Psicopolitica",* Han arriva alla fatale conclusione secondo la quale, nella società contemporanea, crediamo di essere liberi, ma non lo siamo: possiamo soltanto scegliere tra le tante offerte che ci vengono proposte[858].

### 4.2.1. *(Segue):* La dittatura della trasparenza: ciascun individuo sorveglia l'altro

Senza dubbio, in questo mutamento del modo in cui il soggetto è investito dai rapporti di potere[859], ha assunto un ruolo centrale l'avvento di *Internet,* e soprattutto di *smartphone* e *social media*. Difatti, mentre i prigionieri del *Panopticon* di matrice benthamiana erano isolati nelle loro celle e non erano autorizzati a parlare tra di loro – assurgendo il silenzio a fonte di catarsi e di emendamento – nel Panottico digitale, i cittadini sono spronati a comunicare tra di loro e a condividere incessantemente la propria vita sui *social network;* essi sono talmente intrisi della cultura neoliberale che avvertono tale costrizione come una libertà di espressione. In ciò si sostanzia l'intelligenza e l'efficacia del nuovo potere: la condivisione non è imposta da un soggetto esterno, ma

[854] *Ivi*, 51-52.
[855] F. NIETZSCHE, *Al di là del bene e del male. Preludio a una filosofia dell'avvenire,* Giunti-Demetra, Firenze-Milano, 2006, 187.
[856] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 40-42.
[857] *Ivi*, 16.
[858] *Ivi,* 25.
[859] In questo passaggio, si evoca M. FOUCAULT, *Sorvegliare e punire: nascita della prigione,* Einaudi, Torino, 2014, 27.

risponde a un bisogno interiore; grazie ad un «autodenudamento volontario», ciascuno di noi divulga i propri dati personali e fa circolare informazioni su se stesso[860].

Lo *smartphone*, dunque, diviene il dispositivo di devozione per antonomasia, perché trasforma ogni bisogno interiore, ogni esigenza, ogni desiderio più recondito in informazione tracciabile e, di conseguenza, controllabile; i *social media* diventano un rosario di cui il *like* è l'*amen* digitale e *Facebook* (letteralmente, adunanza) è la sua Chiesa. Il soggetto, senza alcun obbligo apparente, immette in rete tutti i dati e le informazioni che lo riguardano, senza preoccuparsi di chi sa cosa, quando e in che modo l'ha saputo[861]; l'informazione circola in modo incontrollato sul *web*[862]; cliccando *like* sui *social network* l'individuo si lascia sedurre dalla sua benevolenza e, abbassando tutte le difese, lascia che i suoi pensieri consci e inconsci si disvelino al mondo[863]. Lo *smartphone,* allora, si trasforma in uno strumento di sottomissione e di manipolazione.

Parimenti, i *big data* consentono di estrapolare informazioni dai nostri *click* e in tal modo elaborano previsioni sul comportamento umano; dalla previsione individuale, è poi possibile tracciare previsioni che trascendono il singolo individuo e che riguardano il comportamento collettivo[864]: tramite l'analisi dei dati raccolti sul *web* si può tracciare non solo lo "psicoprogramma individuale", ma anche quello collettivo e, a seconda del livello di consapevolezza dell'individuo, lo "psicoprogramma dell'inconscio". Tramite i *big data,* che generano informazioni controllabili che rivelano l'*Es* di memoria freudiana[865], la psicopolitica sfrutta l'inconscio di ognuno di noi, portandoci ad avvertire bisogni indotti che crediamo nostri, anticipando la formazione della volontà e plasmando, senza la nostra consapevolezza (ma sfruttando la nostra libertà) la mente[866]. I *big data* trasformano la decisione libera in una decisione preannunciata, conducendo alla morte della volontà[867].

[860] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 18-19.
[861] *Ivi,* 21.
[862] *Ivi,* 18-22.
[863] *Ivi,* 25-26, che si riferisce alla nostra epoca definendola «il *capitalismo del like»,* con riferimento al quale opera la seguente raccomandazione: «*Protect me from what I want».*
[864] *Ivi,* 22.
[865] *Ivi,* 75-76.
[866] *Ivi,* 31.
[867] *Ivi,* 22.

In definitiva, anziché corpi docili, il «*capitalismo del like*» fabbrica menti dipendenti[868].

Il filosofo Han sostiene che le forze di mercato neoliberali abbiano favorito la fine dello spazio prospettico caratteristico del *Panopticon* e il passaggio – già profetizzato dal sociologo e filosofo Jean Baudrillard, sebbene in termini parzialmente differenti[869] – ad un panottico del tutto diverso, cioè aprospettico[870].

Come già evidenziato, nella psicopolitica neoliberale – complici sofisticati e complessi algoritmi, *smartphone, social media* e soprattutto *big data* – scompare completamente la distinzione tra centro e periferia, fondamentale per la realizzazione della sorveglianza dispotica nel *Panopticon* di Bentham. Mentre nella società disciplinare il controllore sorveglia dalla propria torretta le celle dei detenuti – e tale sistema di potere può essere esteso a fabbriche, manicomi, ospedali, esercito, scuole –, i quali non sono in grado di vedere a loro volta il sorvegliante, nel Panottico digitale del XXI secolo, non vi è ottica prospettica: in un'epoca in cui ognuno sorveglia l'altro, il sorvegliante è ovunque e la trasparenza è multilaterale[871]. Nel sistema aprospettico che si sta sviluppando nell'epoca contemporanea, non vi è alcun occhio centrale in grado di «vedere senza essere visto»[872], anzi gli occhi sono dappertutto[873]. Inoltre, mentre i detenuti del *Panopticon* sono consapevoli di essere soggiogati dall'uomo della torretta, gli abitanti della società del controllo psicopolitico credono di essere liberi e, involontariamente, collaborano alla creazione e al mantenimento dello spazio aprospettico, connettendosi sui *social network* e comunicando massivamente tra loro. Mediante la iper-comunicazione, dunque, si realizza la società della trasparenza. Nondimeno, la grande particolarità della nuova tecnica di controllo neoliberale risiede nella volontarietà della condotta: ciascun individuo – guidato da esibizionismo e ambizioni personali – immette volontariamente i propri dati personali sul *web,* libero da qualsivoglia costrizione esterna. La riservatezza e l'intimità cedono il passo al desiderio interiore di denudarsi senza pudore[874].

---

[868] *Ivi,* 24.
[869] Il sociologo e filosofo Jean Baudrillard – al quale era ancora sconosciuta la rivoluzione digitale – sviluppa la tesi della fine dello spazio prospettico, ricollegandola al *medium* televisivo: si veda J. BAUDRILLARD, *Agonie des Realen,* Marve Verlag, Berlino, 1978, 48.
[870] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 76.
[871] *Ivi,* 77.
[872] J. BENTHAM, *Panopticon ovvero la casa d'ispezione,* con interventi di M. Foucault e M. Perrot, Marsilio, Venezia, 2009, Lettera V, 46.
[873] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 77-78.
[874] *Ibidem*.

Si attua, così, il passaggio da una sorveglianza estrinseca, realizzata dal guardiano del *Panopticon,* ad una sorveglianza intrinseca ai meccanismi stessi della società, in cui *ciascuno di noi, credendosi libero, controlla l'altro* e si uniforma al suo comportamento[875].

Nell'epoca della psicopolitica digitale – in cui beni immateriali quali dati e informazioni si trasformano in profitto e in cui, all'opposto, ogni segreto, riservatezza e interiorità costituiscono un ostacolo alla capitalizzazione – la trasparenza produce l'effetto per il quale ciascuno sorveglia l'altro, da cui deriva, a sua volta, un effetto di conformità senza violenza né coercizione[876]. Il controllo totale è preludio del livellamento di ogni pensiero e desiderio[877]. Nella società della iper-comunicazione, nessuno è davvero libero di essere diverso, perché sente costantemente il peso del giudizio altrui.

Il controllo totale si pone su un piano completamente antitetico rispetto alla fiducia, che necessità di libertà d'azione. Come il popolo, se ripone fiducia nei suoi governati, non sente il costante bisogno di supervisione, di controllo e di consultazioni costanti su ogni loro singola azione[878], all'opposto, in un'epoca dominata dalla trasparenza, il popolo non ha fiducia dei propri governati. La fiducia, infatti, implica degli spazi bui: se tutto è illuminato e chiaro, non v'è bisogno di fiducia. La trasparenza elimina in radice qualsiasi bisogno di fiducia: la fede è possibile solo ove risiede il non-sapere. Il popolo domanda trasparenza proprio quando si è esaurita la fiducia. Ecco, allora, che la società della trasparenza affonda le sue radici nella sfiducia e nel sospetto: in una società in cui l'onestà e la sincerità sono chimere, la trasparenza si impone quale nuovo imperativo categorico[879].

Peraltro, mentre il progetto di Bentham nasceva dall'esigenza di una società rinnovata dal punto di vista morale[880], l'imperativo della trasparenza è guidato

---

[875] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 21. Peraltro, tale società della trasparenza è stata, forse per la prima volta, ipotizzata anche dal futurista David Brin, che – davanti al mutamento delle tecniche di controllo – auspica quantomeno una democratizzazione della sorveglianza. Infatti, l'utopia briniana di una "società trasparente" affonda le sue radici nell'esigenza di eliminare ogni asimmetricità del potere tra l'alto e il basso. In D. BRIN, *The Transparent society: Will Technology Force Us to Choose Between Privacy and Freedom?,* Perseus Books, New York, 1998, 14, egli domanda: «Possiamo sopportare di vivere esposti alla sorveglianza, con i nostri segreti svelati, se in cambio otteniamo noi stessi delle luci con le quali possiamo illuminare chiunque?».

[876] *Ivi,* 21.

[877] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 79.

[878] R. SENNETT, *Rispetto. La dignità umana in un mondo di diseguali,* a cura di G. Turnaturi, il Mulino, Bologna, 2004, 125-126.

[879] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 79-80.

[880] J. BENTHAM, Prefazione a *Panopticon ovvero la casa d'ispezione,* con interventi di M. Foucault e M. Perrot, Marsilio, Venezia, 2009, 33, ove Bentham si attende, quali principali effetti della sorveglianza

unicamente da logiche economiche: chi si auto-denuda, rinunciando alla riservatezza e all'intimità, consegna se stesso allo sfruttamento in vista di un successo anzitutto economico. L'abitante della società del controllo neoliberale è incapace di formare una comunità e sacrifica i più alti valori etici in vista del soddisfacimento di propri bisogni personali. Anche la comunicazione e la condivisione di contenuti si colorano di puro egoismo: per l'uomo imprenditore di se stesso, la socialità non è altro che elemento costitutivo del processo produttivo e, di conseguenza, del profitto. L'abitante della società della trasparenza è «l'*homo sacer* del panottico digitale»[881].

A differenza dello stato di sorveglianza disegnato da Orwell, nel Panottico digitale la tortura è sostituita da *tweet* e *post* su *Facebook* e *Instagram*; il Ministero della Verità lascia il posto alla trasparenza e all'autodeterminazione informativa. Lo *smartphone* sostituisce il Grande Fratello di orwelliana memoria; il Grande Fratello non estorce informazioni con la violenza e la tortura, ma mostra tutta la sua benevolenza con *like* e commenti; non c'è carestia, ma massima prosperità. Nel *Panopticon* di Bentham, i prigionieri – nonostante non conoscano il volto del sorvegliante – si sentono osservati e costretti ad agire in modo conforme. Invece, nell'epoca contemporanea, nessuno si sente osservato e intimidito, eppure – per mezzo delle informazioni che circolano in rete – appare chiaro che *ognuno sorveglia l'altro*[882].

Pertanto, nella psicopolitica, il potere benevolo fa sì che l'uomo si senta libero in modo tale da riprodurre dentro di sé meccanismi di sottomissione: il soggetto non è consapevole del proprio asservimento al potere, il rapporto di dominio è per lui invisibile[883]. Si collabora insieme, involontariamente, per la realizzazione e il mantenimento dello sguardo panottico[884]. In questo senso, libertà e sfruttamento

realizzata nel *Panopticon,* una «morale riformata», nonché una «salute preservata», «l'istruzione diffusa», «il nodo gordiano delle leggi d'assistenza pubblica non tagliato, ma sciolto».

[881] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 81-82. Qui il riferimento è al maggiore progetto filosofico che ha visto impegnato per oltre un ventennio Giorgio Agamben, composto ora da nove libri raccolti in un unico volume: G. AGAMBEN, *Homo sacer. Edizione integrale. 1995-2015,* Quodlibet, Macerata, 2018: I Sezione (*Il potere sovrano e la nuda vita*), II Sezione (II, 1. *Iustitium. Stato di eccezione;* II,2. *Stasis. La guerra civile come paradigma politico;* II, 3. *Horkos. Il sacramento del linguaggio;* II, 4. *Oikonomia. Il Regno e la Gloria*; II, 5. *Opus Dei. Archeologia dell'ufficio*), III Sezione (*Auschwitz. L'archivio e il testimone*), IV Sezione (IV, 1. *Altissima povertà;* IV, 2. *L'uso dei corpi*).

[882] B.-C. HAN*, Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 46-50.

[883] *Ivi,* 24.

[884] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 83.

coincidono[885]. L'abitante del panottico digitale è carnefice e, al contempo, vittima di se stesso[886].

### 4.2.2. *(Segue):* La dittatura del positivo e dell'esposizione

La società della trasparenza è, anzitutto, una società del positivo[887].

Le cose acquistano trasparenza quando è eliminata ogni Negatività, ogni angolo spigoloso, cioè quando esse sono livellate e stirate. Nell'articolazione neoliberale della società, tutti i processi decisionali sono sottoposti ad un obbligo di trasparenza, con lo scopo di standardizzarli e di accelerarli[888].

Nella società dell'iper-comunicazione, che necessita di una condivisione sempre più veloce, la Negatività e l'alterità o la resistenza dell'Altro rallentano «la piatta comunicazione dell'Uguale»[889]. Anche il linguaggio trasparente è un linguaggio meccanico, privo di ambiguità e di segreti. Nonostante a rigor di termini l'opacità sia la caratteristica distintiva di ogni linguaggio e di ogni comunicazione[890], la società della trasparenza esige uniformità. L'imperativo categorico dell'uniformità rinuncia alla diversità[891].

Eppure, l'essenza umana è per natura impenetrabile: ogni uomo ha bisogno di propri spazi di diversità e di ecletticità, ove possa soggiornare in Sé, lontano dall'Altro. L'essere umano ha bisogno, per ritornare in se stesso, di un luogo nascosto ove manifestare spontaneità, creatività, libertà: tutte caratteristiche che non ammettono trasparenza. Addirittura, secondo Sigmund Freud, l'uomo non può essere trasparente neppure per se stesso, perché l'*Es* si nasconde all'*Io* – esiste, dunque, una crepa tra l'*Io* e l'*Es*. In definitiva, è impossibile realizzare l'auto-trasparenza, motivo per il quale non è pensabile una trasparenza intersoggettiva[892]. Proprio le ambiguità e le tortuosità

[885] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma,2017, 38.
[886] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 83.
[887] *Ivi,* 9.
[888] *Ivi,* 10.
[889] *Ibidem.*
[890] W. v. HUMBOLDT, *La diversità delle lingue,* a cura di D. Di Cesare, Laterza, Roma-Bari, 2000, 51, ove il linguista e filosofo tedesco Wilhelm von Humboldt scrive: «Nessuno pensa, con una parola, precisamente ed esattamente la stessa cosa che pensa un altro, e l'ancor piccola diversità si trasmette, come un cerchio sull'acqua, in tutta la lingua. Ogni comprendere è perciò sempre un non-comprendere […]»
[891] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 11.
[892] *Ivi,* 12.

dell'animo umano alimentano le relazioni intersoggettive: la delicatezza dell'uomo si esprime al massimo grado quando è in grado di rispettare, anche nel rapporto più intimo, «la proprietà privata interiore», la quale pone un argine alla conoscenza da parte dell'Altro rivendicando «il diritto al segreto»[893].

L'obbligo di trasparenza imposto dalla società contemporanea, invece, chiede all'individuo di rinunciare a questa delicatezza d'animo e di soffocare ogni alterità. La società della trasparenza non tollera segreti e lacune nell'informazione; ogni meandro della mente deve essere illuminato[894].

La società del positivo, rinnegando la negatività, disconosce la triade dialettica hegeliana, che attraversa i tre momenti dell'idea «in sé e per sé» (tesi), dell'idea «fuori di sé» (antitesi) e dell'idea che «ritorna in sé» o idea «pura» (sintesi)[895]. Secondo Hegel, lo Spirito si fa "potenza" solo quando «guarda in faccia il negativo e soggiorna in esso»[896]: il positivo necessita del negativo per divenire Spirito, anzi è la negatività dell'Altro che lo tiene in vita[897]. Al contrario, chi non attraversa la negatività dell'Altro, chi rimane fermo in sé non può divenire Spirito. Lo Spirito è una forza lenta, proprio perché ha bisogno di passare attraverso e di soggiornare nel negativo. La *Fenomenologia dello spirito* di Hegel descrive la forza generatrice di tutto ciò che è Altro, cioè di tutto ciò che è negativo[898]. La società della trasparenza, invece, rifiuta ogni complessità, nella misura in cui sarebbe un ostacolo alla velocità[899]: per tale ragione, la società contemporanea descrive piuttosto una «*fenomenologia del mi piace*»[900].

Nella società della trasparenza, non si agisce più per negatività e divieti, ma per stimoli positivi[901]. I sentimenti negativi non sono tollerati; la sofferenza e il dolore rinnegati e disimparati[902]. Eppure, secondo Nietzsche, l'anima umana è resa grande dal negativo, dal dolore, dalle sventure; sopportato e attraversato il dolore, la forza umana ne

[893] G. SIMMEL, *Sociologia,* Edizioni di Comunità, Torino, 1998, 308-309.
[894] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 15.
[895] G. W. F. HEGEL, *Enciclopedia delle scienze filosofiche in compendio,* a cura di B. Croce, Laterza, Roma-Bari, 1994, par. 18.
[896] G. W. F. HEGEL, *Fenomenologia dello spirito,* Bompiani, Milano, 2000, 87.
[897] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 69.
[898] *Ivi,* 70.
[899] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 15.
[900] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 70.
[901] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 46-50.
[902] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 17.

esce rinnovata; il dolore è forza creatrice dell'essenza[903]. Al contrario, le nuove tecniche del controllo neoliberale tendono a limitare la diversità, l'estraneità, l'Altro. Ogni sofferenza e ogni passione – figure della negatività – devono essere evitate in nome dell'autosufficienza e dell'efficienza. Non a caso, nella società contemporanea, l'eccesso di positività si manifesta, a livello patologico, come disturbi psichici, quali la depressione, la stanchezza, l'esaurimento. L'uomo del neoliberalismo ha disimparato ad attraversare il dolore e, allora quando lo incontra, non è preparato a gestirlo[904].

È emblematico della società del positivo il *like* di *Facebook,* così come è indicativo il fatto che la piattaforma americana si sia rifiutata di introdurre, correlativamente, il tasto per il *dislike:* perfettamente integrato, e anzi propulsore della logica della positività tossica che permea la nostra società, *Facebook* non ha introdotto il pulsante *dislike*, in quanto consapevole che la negatività non possa essere commercializzata e monetizzata. Difatti, un'espressione di disgusto da parte della comunità di Facebook arresterebbe la comunicazione e lo scambio di dati tra gli utenti e, di conseguenza, l'azienda registrerebbe una perdita del valore economico dei dati[905].

Ciononostante, la società del positivo non è in grado di convincere l'uomo avveduto che l'iper-comunicazione e l'iper-informazione possano eliminare l'intrinseca opacità che anima il mondo. Anzi, la ricerca spasmodica del positivo rende evidente che la società contemporanea manca di Verità, di essenza. In un'epoca in cui regna la falsità, la Verità è una negatività; un insieme di informazioni non fa verità, se manca loro un senso[906].

La società della trasparenza è, inoltre, una società dell'esposizione[907].

Nella società della trasparenza, le cose – divenute ormai merci – non esistono se non sono esposte, con la conseguenza che il loro "valore cultuale" abdica a favore di un valore di esposizione, in quanto il valore delle cose aumenta se vengono viste da altri individui. L'opposto accade, secondo il filosofo Walter Benjamin, agli oggetti di culto: è sufficiente che «le cose che stanno al servizio del culto» esistano, mentre non è necessario che siano esposte alla vista di altri: anzi, il loro "valore cultuale" aumenta quando sono

[903] F. NIETZSCHE, *Al di là del bene e del male,* in *Opere complete,* a cura di G. Colli e M. Montinari, Adelphi, Milano, 1968, vol. VI, tomo II, 134.
[904] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 17.
[905] *Ivi,* 20.
[906] *Ibidem.*
[907] *Ivi,* 22.

nascoste nella negatività dell'isolamento (il lemma latino *secretus* assume proprio il significato di "separato", "isolato")[908].

Nella società neoliberale, invece, il «puro esserci» cede il passo al valore dell'esposizione: tutto ciò che non è mostrato, tutto ciò che riposa in sé, tutto ciò che non è pubblicizzato non esiste. L'obbligo di trasparenza induce il soggetto capitalista a mostrare tutto ciò che possiede, a discapito di ciò che è, con il fine ultimo di suscitare interesse[909]. Per tale via, nella società dell'esposizione, ogni individuo pubblicizza e vende se stesso. Ogni cosa è denudata e svestita del suo essere per mostrarsi all'esterno. L'articolazione neoliberale della società riduce tutto al valore di esposizione: tutto ciò che è esterno è più importante di ciò che è interno; ciò che appare è più importante dell'essenza. L'invisibile non esiste e, qualora esista, non ha alcun valore [910].

L'imperativo categorico dell'esposizione costringe, così, alla bellezza e al *fitness* a tutti i costi, perché anche il corpo diviene un oggetto da mostrare. Anche il corpo è esposto e, così, sfruttato. I modelli di oggi (si pensi agli *influencer* di *Instagram*) non hanno alcun valore interiore, ma si sforzano di creare un paradigma di esposizione: essi sono stati creati dalla società dell'esposizione e contribuiscono ad alimentarla[911].

In aggiunta, nella società dell'esposizione, «non è più possibile essere il proprio volto»: l'obbligo di esposizione, figlio della società della trasparenza, ci priva della possibilità di essere essenza vera e ci costringere ad essere ciò che *dobbiamo* mostrare all'esterno per pubblicizzare la nostra immagine. In ciò risiede la violenza dell'esposizione: la società contemporanea rinnega tutto ciò che non si sottomette alla visibilità e ignora tutto ciò che non è visibile[912].

In definitiva, la società dell'esposizione rifiuta tutto ciò che emana complessità e profondità, in quanto la complessità costituisce un ostacolo all'iper-comunicazione[913]. La comunicazione cui siamo abituati (si pensi ai messaggi scambiati su *WhatsApp*) è veloce, perché l'uomo imprenditore di se stesso non ha tempo per gli abissi dell'anima umana.

[908] *Ivi,* 22-23.
[909] *Ibidem.*
[910] B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 25-27.
[911] *Ibidem.*
[912] *Ibidem.*
[913] *Ivi,* 28.

Al contrario, l'essenza ha bisogno di tempo, è lenta: ed è per questo che essa costituisce un ostacolo all'iper-comunicazione, votata unicamente alla velocità. Così, la trasparenza genera un «vuoto di senso»[914].

Ebbene, le fotografie immesse in rete (*Facebook, Instagram, Snapchat*) divengono oscene, nel senso che hanno ormai rinunciato ad ogni complessità, ad ogni valore intrinseco, ad ogni riflessione ulteriore. Esse mancano di ogni opacità che avrebbe però bisogno di un esame attento, cioè di tempo di stare con se stessi. Ogni sensazione è planata in superficie; non riesce a raggiungere alcuna profondità. Ogni negatività, ogni angolo spigoloso è limato per raggiungere la massima velocità e, di conseguenza, la massimizzazione del profitto[915].

In definitiva, quella creata dalla psicopolitica neoliberale è una società della trasparenza in cui, però, manca ogni Verità.

### 4.2.3. *(Segue):* Il ruolo dei *big data:* l'individuo è panottico di se stesso

Lo sviluppo dei *big data* ha inaugurato un Secondo Illuminismo: mentre il Primo Illuminismo è stato dominato dalla statistica, salutata all'epoca come la scienza in grado di liberare il sapere dalla mitologia, perché fondata su cifre e condotta su base numerica, nell'età contemporanea tutto si è trasformato in dati e informazioni. Tale rivoluzione dei dati – il c.d. Dataismo – è dominata dalla trasparenza[916]: come si legge sul *New York Times,* l'uomo ha oggi la possibilità di raccogliere una grandissima quantità di dati immessi sul *web.* Tutto ciò che può essere quantificato deve essere quantificato: tali dati rappresentano una «lente trasparente e affidabile» che ci consente di avere accesso ai pensieri di natura ideologica ed emotiva degli individui[917].

Dal momento che nel regime neoliberale ogni *click* – e cioè ogni pensiero, ogni riflessione, ogni desiderio più recondito – si trasforma in dati e in informazioni, la sorveglianza digitale è molto più efficace rispetto alla sorveglianza attuata nel *Panopticon* benthamiano: mentre nel dispositivo panottico, legato all'ottica prospettica, sono possibili angoli ciechi, ove i detenuti possano sottrarsi all'occhio del sorvegliante, la sorveglianza

[914] *Ibidem*.
[915] *Ibidem.*
[916] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 67.
[917] *New York Times* del 04.02.2013.

digitale – in quanto aprospettica – non consente luoghi ove l'individuo possa rifugiarsi. Per tale motivo, la sorveglianza digitale si impossessa di ogni pensiero, desiderio, di ogni emozione, rendendo possibile una sorveglianza psicopolitica dell'individuo[918].

Il Dataismo è una nuova ideologia che conduce ad un «totalitarismo digitale», ad un annientamento di tutto ciò che è segreto o nascosto, per cui – secondo il filosofo Han – sarà necessario un Terzo Illuminismo, che porti alla luce il fatto che il Secondo Illuminismo ha ridotto l'uomo ad una nuova schiavitù[919].

Difatti, la psicopolitica neoliberale ha inaugurato una nuova forma di violenza: si tratta di una violenza molto più silente rispetto a quella che si mostrava nell'*Ancien Régime* come potere di vita o di morte del re o rispetto a quella che coincideva con l'ordine e l'incasellamento nella società disciplinare. È la violenza della trasparenza[920].

La tecnica di potere neoliberale è in grado di insinuarsi nella quotidianità di ognuno di noi: il fenomeno culturale del *quantifield self*, che ha sempre più seguaci nel mondo, si illude che tramite la tecnologia e i numeri si possa arrivare ad una profonda conoscenza del Sé. La fede sconfinata nella misurabilità e quantificabilità della vita fa sì che, sempre più comunemente, gli sportivi si dotino di *smartwatch* che registrano i dati dell'allenamento, la temperatura corporea, il numero di battiti cardiaci, il tasso glicemico, le calorie consumate o assunte; che gli appassionati di cinema si dotino di *app* in grado di contare e tenere traccia del numero di film guardati; ognuno di noi ha sullo *smartphone* almeno un'applicazione che tenga traccia del conto in banca o dei tragitti percorsi; sono controllate anche le condizioni mentali, gli stati d'animo e tanto altro ancora. Mediante dispositivi integrati nell'abbigliamento o nello *smartphone* si può tenere traccia praticamente di tutto[921]. Indubbiamente, la quantità di dati processati è potenzialmente infinita.

Ogni ricerca sul *web* e ogni *click* sul nostro *smartphone* o *computer* vengono salvati e registrano le nostre abitudini di consumo, il nostro stile di vita, i nostri momenti di riposo e di lavoro: ecco, allora, che l'identità umana si proietta su *Internet* come identità digitale. I siti *web* sanno di noi più di quanto possiamo immaginare e, forse, più di quanto sappiamo di noi stessi. Passando per l'*Internet della persona,* il c.d. *web 2.0,* l'*Internet*

[918] B.-C. HAN*, Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 66-67.
[919] *Ivi,* 69.
[920] *Ivi,* 70.
[921] *Ivi,* 72-73.

*delle cose (*c.d. *Internet of Things*), il c.d. *web 3.0*, monitora e registra ogni interazione tra i dispositivi connessi e, per il suo tramite, la persona[922]. Dunque, l'individuo è costantemente sorvegliato dai dati che, consapevolmente o inconsapevolmente, immette sul *web*[923].

I dati così raccolti sono talvolta pubblicati e mostrati sui *social network:* ecco, allora, che il soggetto del regime neoliberale sorveglia costantemente l'altro e contemporaneamente sorveglia se stesso. Come soggetto che si spoglia di ogni segreto e che incessantemente si confronta con l'altro, l'individuo della società psicopolitica è sorvegliante e detenuto di se stesso: «Il soggetto digitalizzato, interconnesso è *panottico di se stesso»,* dice il filosofo Han[924].

Nondimeno, mentre nel *Panopticon* di matrice benthamiana i sorveglianti non hanno davvero accesso a ciò che i detenuti sperano e desiderano, i *big data* registrano tutto e ricordano tutto: in ciò risiede la straordinaria efficacia del Dataismo. Mentre la biopolitica fa presa sul corpo, questa nuova microfisica del potere – sfruttando i *big data* – è in grado di instillarsi in profondità nella psiche dell'individuo, di ricordare ciò che l'individuo fa o pensa o desidera e, mediante l'analisi dell'andamento dei comportamenti passati, è addirittura in grado di prevedere le sue azioni future. La psicopolitica digitale, dunque, si insinua nel processo psichico dell'uomo e, di fatto, anticipa la formazione della volontà, determinando la fine della volontà[925].

---

[922] ORACLE, *Che cos'è l'IoT?,* consultabile in https://www.oracle.com/it/internet-of-things/what-is-iot/.

[923] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 74. Nel proseguo del suo saggio sulla Psicopolitica, Han suggerisce che i *big data* hanno creato, prima di tutto, un *business* economico senza precedenti nella storia: i dati personali sono commercializzati e, peraltro, hanno un alto valore economico proprio in virtù della circostanza che sono in grado di fare previsioni sui comportamenti futuri degli utenti. Ad esempio, l'azienda statunitense di analisi di *big data* Acxiom possiede i dati personali di più di 300 milioni di cittadini statunitensi, dai quali ricava elevati profitti. Allora, si comprende bene (ma neanche troppo) come i dati personali siano classificati in un catalogo e poi venduti: gli individui con un basso valore di mercato sono classificati come "*waste*", cioè spazzatura, mentre coloro che hanno un elevato coefficiente economico (in pratica, gli individui più attivi dal punto di vista digitale) sono etichettati come "*shooting star*". È come se i *big data* avessero creato nuove categorie sociali. Ebbene, in questa nuova articolazione del potere, compare un *Ban-opticon (Bannoptikum),* termine tratto da Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella moderna liquidità,* Laterza, Roma-Bari, 2015, versione e-book. Mentre nel *Panopticon,* i sorveglianti controllano i movimenti dei detenuti dall'alto della loro torretta, nel *Ban-opticon* gli individui sono identificati, catalogati in classi (coloro che sono "rifiuti" vengono separati da coloro che sono "utili") e, alcuni di essi, esclusi (*to ban:* escludere).

[924] *Ivi,* 73.

[925] *Ivi,* 74-75, che, con riferimento a tale aspetto dei *big data,* a sua volta richiama V. MAY-ER-SCHONBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think,* Hougthon Mufflin, Londra, 2013, 203. In particolare, Han sostiene che, anche nelle elezioni statunitensi, verrebbero sfruttati i *big data,* in quanto da diverse fonti verrebbe raccolta una grande quantità di dati, che poi sarebbero incrociati tra di loro mediante algoritmi estremamente sofisticati, per tracciare

Come abbiamo già accennato, i *big data* sono, inoltre, capaci di tracciare lo "psicoprogramma collettivo": tramite algoritmi altamente sofisticati, i dati e le informazioni raccolti sono incrociati e analizzati, in modo da tracciare l'andamento complessivo dei desideri e pensieri collettivi. Per mezzo dell'analisi di modelli collettivi di comportamento, dunque, la psicopolitica di matrice neoliberale sarebbe in grado di accedere all'inconscio collettivo, appropriarsi del comportamento della massa su un piano che trascende la coscienza[926].

Altrettanto indubbiamente, tuttavia, il *quantifield self* e il Dataismo non sono in grado di rispondere a questa domanda: *Chi sono io?* Per quanto possano essere sconfinati i dati raccolti sulla vita di un individuo, per quanto precisa possa essere la previsione dei suoi comportamenti, i numeri non sono comunque in grado di raccontare nulla del Sé. Il Sé emerge da un racconto della propria vita e soprattutto dalla comprensione della propria storia. Per tale motivo, la rivoluzione dei dati è «pura tecnica di autocontrollo» che nulla racconta della nostra etica e della nostra Verità[927].

Dal momento che i *big data* si fondano su tecniche induttive e di inferenza probabilistica[928], cioè sulla probabilità e regolarità statistiche, il comportamento umano diviene prevedibile. Il Dataismo e il *quantified self* sono in grado di prevedere correlazioni tra un comportamento e l'altro. La correlazione, tuttavia, non è in grado di *comprendere* e di *spiegare perché*: essi non sono in grado di spiegare perché un individuo si comporta in un certo modo, sono soltanto in grado di prevedere comportamenti, agendo sul piano della probabilità causale. La causalità, però, non rappresenta il più alto livello del sapere: i *big data* non hanno nulla a che vedere con il concetto e con lo Spirito[929].

Le correlazioni mettono in evidenza specialmente ciò che è statisticamente probabile: i *big data* analizzano soprattutto i modelli comportamentali della massa. Per tale via, tutto diventa conforme: la trasparenza e l'informazione costringono l'uomo alla conformità. Calcolando valori medi, i *big data* producono l'effetto di livellare tutto. Tutto ciò che è

profili estremamente precisi dei votanti. Si parla, in tal caso, di *micro-targeting,* in grado di fare previsioni precise sul futuro comportamento del ceto elettorale.

926 B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 77.

927 *Ivi,* 72.

928 A tal proposito, si veda, *amplius,* il paragrafo §1.2.1 nel Capito Primo, con riferimento ai *big data.*

929 *Ivi,* 83.

unico, tutto ciò che è episodico non ha valore. La storia, tuttavia, è scritta dagli eventi unici: se così è, i *big data* non sono neppure in grado di vedere il futuro[930].

### 4.2.4. *(Segue):* Dalla folla allo «sciame digitale» incapace di uno Spirito comune

In un periodo caratterizzato da grandi mutamenti sociali e politici – complici non solo i processi di industrializzazione, di modernizzazione e di urbanizzazione, ma anche la diffusione delle idee socialiste, che porta con sé violenti scioperi in tutta Europa – lo psicologo e antropologo francese Gustave Le Bon presagiva, con una connotazione certamente negativa, che nel futuro la società sarebbe stata governata dalle folle. La massa si sarebbe insinuata nell'organizzazione del potere, portando alla distruzione totale del potere regio e alla crisi della civiltà[931]. Per Le Bon, le "masse" sono animate da uno spirito collettivo che agisce guidato da un «senso di potenza invincibile»[932].

Gustave Le Bon descrisse il passaggio dal XIX secolo al XX secolo. Il filosofo Byong-Chul Han, nel suo saggio "*Nello sciame. Visioni del digitale*" sostiene che l'epoca contemporanea è parimenti caratterizzata da un nuovo sovvertimento sociale, dovuto oggi alla rivoluzione digitale: ancora una volta, le masse aspirano a rovesciare il precedente rapporto di potere e di dominio per fondare un nuovo ordine sociale. Nel XXI secolo, tuttavia, la folla ha assunto piuttosto le sembianze di uno «sciame digitale» privo di uno Spirito comune e incapace di intonare una sola voce[933].

Lo sciame digitale vanta caratteristiche distintive – che il filosofo Han prova a dipingere a sottili pennellate – rispetto alla folla, protagonista degli studi che hanno occupato di Le Bon. Innanzitutto, per quanto connotata da tratti negativi, la folla ha un'anima, uno Spirito che la guida. La massa assume un'uniformità di pensiero e di comportamento che è sintesi, e non somma, delle caratteristiche dei singoli. Coloro che compongono la massa perdono la propria individualità a favore dell'interesse comune; sono animati da un senso di unità e sono in grado di divenire un *Noi* e di intonare una sola voce. Tra di essi vige un tacito accordo per il quale l'uno si confonde e si plasma

---

[930] *Ivi,* 89-90.
[931] G. LE BON, *Psicologia delle folle,* Edizioni Clandestine, Marina di Massa, 2013, 2-5.
[932] I. COLONNA (a cura di), *La psicologia delle folle. Gustave Le Bon, 1895,* consultabile in https://www.unisalento.it/documents/20152/224009/Le+Bon-LaPsicologiadelleFolle.pdf/a1b11f49-dc1b-45a7-a797-8fd81aadb416?version=1.0.
[933] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 22.

nell'altro. Progressivamente, l'uomo della folla diviene Nessuno, dissolvendosi nella moltitudine[934].

Al contrario, lo «sciame digitale» è composto da uomini con una personalità spiccatamente individualista. L'*homo digitalis* non è in grado di sacrificare il proprio benessere sull'altare del benessere comune; egli rimane Qualcuno – e lavora incessantemente per diventare Qualcuno, sfruttando anche se stesso, il proprio corpo e le proprie capacità personali – anche quando fa parte di un gruppo. È incapace di abdicare se stesso – la propria volontà, il proprio tempo, i propri interessi – in favore di uno Spirito comune. I confini tra sé e l'Altro sono sempre ben visibili. L'abitante del Panottico digitale è anonimo, perché si nasconde dietro uno schermo e dietro l'evanescenza del pensiero comune, ma non è capace di diventare Nessuno[935].

Inoltre, mentre la folla si riunisce in luoghi chiusi, ove gli individui possano parlarsi e conoscersi, l'*homo digitalis* abita uno spazio completamente diverso: l'isolamento della propria casa. L'individuo della società contemporanea si illude di connettersi al mondo tramite *Internet*, ma in realtà resta isolato dal mondo, dai suoi drammi e dai suoi piaceri, sedendo comodamente sulla poltrona della propria camera. Gli individui che compongono lo «sciame digitale» si radunano sporadicamente, come negli *smart mobs,* ma più che ad uno tsunami capace di travolgere tutto assomigliano a insetti volatili, assai instabili e disordinati, incapaci di farsi un'anima sola per un interesse comune. A differenza della folla, che – anche quando animata da ideali bassi – sa marciare verso un'unica direzione, la moltitudine dell'epoca neoliberale non sviluppa energia positiva e non è in grado di costituire un'alternativa al potere costituito. E, così come rapidamente si è formata, rapidamente sparisce[936].

In definitiva, gli abitanti del *web* «danno vita a un peculiare *assembramento senza riunione*, a una *massa senza spiritualità*, senza anima o spirito»[937].

Similmente, anche le *shitstorms*[938]*,* evoluzione patologica della moltitudine, non sono in grado di mettere in discussione i rapporti di potere, in quanto gli individui – in

[934] *Ivi,* 23.
[935] *Ivi,* 23-24.
[936] *Ivi,* 25.
[937] *Ivi,* 24.
[938] Con il termine "*shitstorm*" si intende il fenomeno diffuso sul *web,* soprattutto nei *blog* o sui *social network,* di discussione attorno a temi di dominio pubblico, in cui spesso persone comuni si scagliano contro altre persone utilizzando un linguaggio violento e dispregiativo. Nel 2012, il termine "*shitstorm*" è stato eletto in Germania come vocabolo dell'anno da una commissione di linguisti tedeschi appositamente nominati. Si veda, a tal proposito, B.-C. HAN, op. cit., 99. Come sottolineato dal filosofo Han, tale

evidente stato di eccitazione – si limitano ad attaccare persone precise e a discutere su temi privi di sostanza politica e sociale[939].

Analizzando la società neoliberale da un altro punto di vista, i *media* digitali si differenziano dai *media* classici perché "de-medializzano" la comunicazione, nel senso che non si avvalgono di intermediari. I *media* elettronici, come la radio o la televisione, sono costruiti come un anfiteatro in cui vi è un centro da cui promanano notizie, per cui è possibile solamente una comunicazione unilaterale. Viceversa, nei *media* digitali – soprattutto nei *blog* e nei *social network* come *Facebook o Twitter* – non vi è un centro unico, ma gli utenti recepiscono e, al contempo, diffondono informazioni, dando vita ad una comunicazione multilaterale. L'*homo digitalis* non si accontenta più di essere passivo recettore di informazioni, ma aspira a crearle attivamente, perchè vuole essere presente direttamente sul luogo di irradiazione della notizia e vuole presentare direttamente il proprio punto di vista senza l'aiuto di intermediari[940].

Allora, si capisce come anche la democrazia rappresentativa sia entrata in crisi, in quanto l'uomo della società contemporanea richiede una sempre maggiore partecipazione attiva in tutti i processi decisionali[941].

Per altro verso, è vero che le informazioni sono aumentate in modo incontrollato: questo «frastuono comunicativo» causa una crisi dello Spirito. Lo Spirito, infatti, è alimentato dal silenzio – cioè dall'incontro con il Sé – che non è facile da riprodurre in una società iper-comunicativa, iper-creativa e iper-produttiva[942].

---

fenomeno dilagante in tutta Europa rende plasticamente evidente che viviamo in una società in cui non vige più rispetto reciproco. Come risulta chiaro dalla sua etimologia, il rispetto impone una distanza (rispettare: distogliere lo sguardo); invece, nella società contemporanea, la comunicazione digitale ha ridotto le distanze spaziali, con la conseguenza che l'*homo digitalis* si sente nella posizione di poter rinunciare alle distanze interpersonali. L'uomo del panottico digitale esprime una posizione su qualsiasi aspetto, anche privato. Tale commistione tra sfera pubblica e privata è particolarmente evidente sui *social network.* Per un approfondimento sul tema, si veda B.-C. HAN, op. cit., 11-17.

[939] *Ivi,* 25.

[940] *Ivi,* 29-31.

[941] *Ivi,* 31.

[942] *Ivi,* 35, ove Han dice che «il silenzio è medium dello spirito». In un altro luogo, il filosofo sudcoreano, rifacendosi a Jean Paul Sartre, critica aspramente – bollandole come "oscene" – l'iper-creatività, l'iper-produzione e l'iper-comunicazione, che sfrecciano via al di là dello scopo. Secondo Sartre, infatti, è osceno il corpo che è ridotto a pura carne, spogliato di ogni Spirito e di ogni narrazione interna: allo stesso modo, secondo Han, è oscena la nostra società che spinge ogni cosa al di là di quanto necessario: è una società che procede per addizione e non per narrazione. In nome della trasparenza, la società del XXI secolo – ripudia ogni gesto e rituale che sia narrativo: solo il processore può essere completamente trasparente, perché procede per addizione. Al contrario, i rituali e le cerimonie sono processi narrativi, che hanno bisogno del proprio tempo e del proprio spazio. Divenuta ormai una società dell'accelerazione, la società della trasparenza rifiuta ogni tensione narrativa e ogni immaginazione, perché ha preso solo a contare. Questo passaggio dalla narrazione al conteggio è riprodotto nella distinzione tra memoria umana e memoria

Il cerchio si chiude: gli individui del regime neoliberale sono troppo impegnati allo sfruttamento di se stessi, all'ottimizzazione permanente delle proprie risorse individuali, alla *performance,* a creare entusiasticamente la migliore versione di sé per condividere il proprio mondo interiore con l'Altro e costruire, per tale via, una folla capace di un agire comune. Nell'epoca contemporanea, il sentimento comune è la solitudine: l'*homo digitalis,* sopraffatto dal Super-Io interiore, illudendosi di entrare maggiormente a contatto con l'Altro tramite la riduzione delle distanze*,* ha finito per non sapersi più unire con gli altri in una folla[943].

### 4.2.5. *(Segue):* La comunicazione digitale allontana dall'Altro

Quando comunichiamo, paradossalmente, la componente verbale è molto limitata: la gestualità, le espressioni facciali, i movimenti del corpo, la tensione nella posizione che assumiamo e lo sguardo dicono di noi molto più delle parole. Nella comunicazione, la multidimensionalità della percezione umana, cui concorrono tutti i sensi, difficilmente può ingannare quanto le parole[944].

La rivoluzione digitale, invece, ci sta progressivamente allontanando dal Reale e, di conseguenza, dall'Altro: oramai, possiamo scambiare informazioni e comunicare nella comodità delle nostre case, per cui – nel quadro dell'esigenza di sfruttare tutto il tempo a disposizione e tutte le capacità personali – la comunicazione è divenuta sempre più impersonale. Lo *smartphone*, in particolare, gioca un ruolo essenziale: quando parliamo con l'Altro, soprattutto tramite *app* di messaggistica, spariscono il suo volto e il suo corpo, così come spariscono nella comunicazione la gestualità, la mimica facciale, le pause tra un argomento e l'altro, gli occhi. Nella comunicazione, l'*homo digitalis* immagina più di

---

informatica: la memoria informatica opera e procede in modo meramente additivo, cioè diacronico, accatastando, l'uno vicino all'altro, dati e informazioni, laddove la memoria umana opera un incessante riordinamento e una riscrittura continua di tutto ciò che vede e ricorda; dunque, mentre la memoria informatica è un ammasso disordinato di immagini e di dati, la memoria umana racconta una storia. Si veda, a tal proposito, B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014, 52 ss.

[943] B.-C. HAN*, Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 27. Nelle pagine precedenti, Han si pone in aperto contrasto con i filosofi Michael Hardt e Antonio Negri, i quali, in *Moltitudine: guerra e democrazia nel nuovo ordine imperiale,* Rizzoli, Milano, 2004, partendo da categorie storicamente superate, ritengono che la globalizzazione abbia generato due forze contrapposte: da un lato, l'Impero, cioè un centro di potere capitalistico decentrato, dall'altro lato, la moltitudine, cioè una classe, capace di uno Spirito comune, che si contrappone al dominio dell'Impero. Secondo Han, i due omettono di considerare che nell'epoca contemporanea non è più possibile fare un discorso di classe, in quanto l'ordine politico non è oggi dominato da una classe sociale che sfrutta gli individui dell'altra classe sociale, perché ognuno sfrutta se stesso, divenendo allo stesso tempo padrone e servo.

[944] *Ivi,* 36-37.

quanto ha mai fatto nel passato; tramite lo schermo dello *smartphone*, ciascuno vede la propria immagine riflessa e parla con nessuno se non con se stesso[945].

Lo *smartphone*, al contempo, elimina ogni Negatività. Nel nome dell'efficienza e della velocità, la comunicazione con l'Altro è sempre più breve e le parole sempre più semplificate. Lo *smartphone*, infatti, ripudia quelle forme comportamentali che esigono ampiezza temporale, eliminando tutto ciò che richiede tempo. Non a caso, su *Facebook,* il pulsante "mi piace" non richiede altre parole: ci siamo, dunque, abituati a pensare in modo dualistico, quasi binario, con un appiattimento generale di tutte le sfumature della Realtà. Questa semplificazione delle parole, figlia della compressione del tempo, comporta anche una semplificazione del pensiero: l'*homo digitalis* si è disabituato a pensare in maniera complessa. I dispositivi digitali, in definitiva, stanno indebolendo «la capacità di rapportarsi alla negatività» e, si potrebbe aggiungere, alle infinite sfumature di pensiero[946].

Secondo Sartre, l'Altro è in ogni luogo – intendendo per l'Altro ogni cosa esistente[947]. Sicuramente, in passato, tramite lo sguardo, l'Altro era capace di destare più Negatività, più resistenza rispetto ad oggi. Nell'epoca contemporanea, invece, l'*homo digitalis* rifugge l'Alterità – lo sguardo dell'Altro – per restare nella sua "*confort zone"* e non interrogarsi. Come sottolineato dal filosofo Han, «la comunicazione digitale è una comunicazione *povera di sguardo*»[948].

Si pensi, in rappresentanza di tutte le piattaforme di comunicazione, a *Skype*: sicuramente, la videochiamata ci ha restituito la possibilità di restare a contatto anche con persone lontane; ciononostante, residua comunque una distanza tra chi comunica. Difatti, se si guarda l'obiettivo della videocamera non è possibile guardare l'Altro e se si guarda l'immagine riflessa dell'Altro, l'Altro capisce che si sta guardando sulla parte superiore o inferiore del PC: vi è comunque un'asimmetria dello sguardo, che ci comunica l'assenza dell'Altro[949].

---

[945] *Ivi,* 36-37.
[946] *Ivi,* 37-38.
[947] In J. P. SARTRE, *L'essere e il nulla. La condizione umana secondo l'esistenzialismo,* Il Saggiatore, Milano, 2008, 304 si legge: «Senza dubbio, ciò che manifesta più spesso uno sguardo è la convergenza verso di me di due globi oculari. Ma uno sguardo può anche essere dato da un fruscio di rami, da un rumore di passi seguiti da silenzio, dallo sbattere di un'imposta, dal leggero movimento di una tenda».
[948] B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015, 38-39.
[949] *Ivi,* 39, che a sua volta cita uno dei più importanti quotidiani della Germania, *Suddeutsche Zeitung Magazine,* dicembre 2013.

Similmente, nell'epoca di *Facebook,* l'immagine del profilo non è un volto, ma è una faccia (*face*) privata di ogni interiorità e di ogni storia. L'immagine del profilo ambisce ad essere l'Altro, ma non restituisce in chi guarda la sua interiorità, le sue emozioni, la sua paura, il suo vissuto. Quel volto fotografato ed esposto all'attenzione di tutti rappresenta soltanto l'immagine che vogliamo dare di noi, l'ultimo rifugio dell'apparenza e dell'appiattimento emotivo della società. L'esibizione del Sé elimina ogni diversità. La faccia non è più l'Altro che mi guarda e mi rapisce, ma rappresenta soltanto un'immagine piatta del contorno del viso[950].

Difatti, nell'epoca contemporanea, questo delirio dell'ottimizzazione non ha risparmiato neppure le immagini: si ottimizza il tempo, si ottimizzano le proprie capacità e si ottimizzano le immagini. Anche la produzione eccessiva di fotografie e immagini – resa possibile dalle enormi potenzialità dei dispositivi digitali – può essere interpretata come fuga dal Reale[951]. Le immagini sono usate per far sembrare la realtà – percepita evidentemente come imperfetta – più viva, più accattivante, priva di negatività – in una parola, perfetta[952]. Tramite le immagini, *l'homo digitalis,* congela il tempo e si oppone al divenire[953]. La riproduzione falsata della realtà porta alla scomparsa di tutto ciò che è diverso, imperfetto, stravagante e reale. Le belle foto eliminano la Realtà e producono l'effetto di disabituare l'*homo digitalis* alla diversità[954].

## 4.3.Le tecniche di riconoscimento facciale: verso una sorveglianza sulle emozioni?

### 4.3.1. *(Segue):* Il fenomeno dell'*affective computing* e i sistemi di riconoscimento delle emozioni umane

Non è una novità che, nell'ambito del *marketing,* gli operatori economici sfruttino le emozioni e le più profonde e intime afferenze umane con lo scopo di indirizzare i comportamenti economici degli individui. Non sorprende, allora, che a partire dagli anni

[950] *Ivi,* 41.
[951] *Ivi,* 45.
[952] *Ivi,* 42-43.
[953] *Ivi,* 45, ove il filosofo rinviene nella differenza tra l'immagine analogica e l'immagine digitale una metafora del nostro tempo, che rifugge dalla negatività e dal divenire. In particolare, le fotografie analogiche, come tutte le cose, sono sottoposte allo scorrere del tempo: anche la carta delle fotografie è deperibile e, dunque, anche se fissata su altri supporti, è mortale come qualsiasi altro organismo vivente. Al contrario, le fotografie digitali sono immuni dallo scorrere del tempo e, quindi, dalla negatività del tempo: non bisogna più preoccuparsi del crescere e dell'invecchiare, della nascita e della morte. L'immagine digitale è sempre uguale a se stessa: essa «non sboccia né risplende, perché nello sbocciare è iscritta la negatività dell'appassire, nello splendore la negatività dell'ombra».
[954] *Ivi,* 42-43.

Sessanta del secolo scorso siano stati finanziati e condotti studi scientifici sulle emozioni umane[955].

Come abbiamo avuto modo di anticipare[956], nel campo del riconoscimento facciale, si sta sviluppando il c.d. *affective computing,* vale a dire tecniche di analisi delle emozioni che si dichiarano capaci di captare e decifrare le emozioni umane[957], le quali possono essere impiegate in svariati ambiti: dal campo medico (ad esempio, per aiutare le persone affette da autismo a implementare capacità emotive) all'ambito commerciale (ad esempio, per rilevare le preferenze e la predisposizione all'acquisto dei consumatori)[958], dalle attività di polizia (si pensi alle tecniche di interrogatorio) allo svolgimento dei colloqui di lavoro[959].

Il primo progetto di ricerca in materia è costituito dal progetto *Facial Action Coding System* (FACS), elaborato dallo psicologo Paul Ekman della University of California. In particolare, esso si basava sullo studio e sulla successiva rielaborazione dei sei emozioni di base, indicate come universali e immutabili a prescindere dal contesto culturale e sociale degli individui analizzati: rabbia, disgusto, paura, felicità, tristezza e sorpresa[960]. Nelle intenzioni di Ekman, lo studio di tali emozioni – combinate con altri elementi fisico-emozionali, come gli impercettibili movimenti dei muscoli facciali – avrebbe dovuto consentire di costruire un paradigma generale del modo in cui gli individui comunicano le proprie emozioni[961]. Ciononostante, diversi studi[962] evidenziano che, in realtà, gli individui manifestano le proprie emozioni – comprese quelle qualificate come "universali" – a seconda della propria cultura, del proprio contesto sociale, della situazione e addirittura delle circostanze, per cui lo stesso individuo potrebbe esprimere

---

[955] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 515.
[956] Tale argomento è stato anticipato, a proposito dell'Intelligenza Artificiale, nel Capitolo Primo, paragrafo §1.2.1.
[957] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 43-44; R. V. PICARD, *Affective computing,* MIT Press, Cambridge, 1997.
[958] G. LUGLI, M. RIANI (a cura di), *Espressioni ed impronte facciali nel marketing,* Giappichelli, Torino, 2018.
[959] AI NOW INSTITUTE, *AI Now Report 2019,* dicembre 2019, 50 ss.
[960] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 43; AI NOW INSTITUTE, AI *Now Report 2018,* dicembre 2018, 14; E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 517.
[961] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 517.
[962] L. F. BARRETT ET AL., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements,* in *Psychological Science in the Public Interest,* 20, 1, 2019, 46 ss.

la stessa emozione in modi diversi. Inoltre, la stessa espressione facciale potrebbe esprimere in modo variabile una o più emozioni complesse[963].

L'intuizione di fondere i risultati ottenuti in campo psicologico sull'analisi delle emozioni con i progressi delle scienze computazionali si deve agli studi di Rosalind Picard e del gruppo di ricercatori del MIT Media Lab, che possono considerarsi gli ideatori e fondatori del fenomeno dell'*affective computing*[964]. Secondo tale progetto di ricerca – che si fondava su intenti altamente etici[965] – una volta studiate, le emozioni umane possono essere codificate e calcolate[966].

Alcune *Big Tech,* come Microsoft, IBM e Amazon, e altre società di *marketing* non si sono lasciate sfuggire l'occasione di utilizzare gli studi sull'*Emotional AI* per scopi eminentemente capitalistici, con l'intento di massimizzare i profitti, e nel tempo hanno creato algoritmi di riconoscimento facciale che si basano soprattutto sugli studi dello psicologo Ekman[967].

In particolare, l'azienda *Smart Eye* ha acquistato *Affectiva*[968] – l'azienda fondata dagli stessi ricercatori del MIT Media Lab – ed è oggi divenuta l'impresa *leader* nelle operazioni di tracciamento e codificazione delle emozioni umane. Mentre *Affectiva* era nata con i medesimi intenti etici e sociali che animavano le ricerche della Picard, negli

---

963 G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 43-44.

964 Il fenomeno dell'*affective computing,* infatti, ha trovato terreno fertile a seguito dell'implementazione dei sistemi di Intelligenza Artificiale capaci di analizzare e schematizzare le emozioni umane. Per questo motivo, si parla anche di *Emotion AI* o di *Emotional AI.* Sul sito del gruppo di ricerca *Emotional AI Lab,* consultabile su *emotionalai.org,* si legge: «Il termine "*emotional AI"* si riferisce a quelle tecnologie che utilizzano l'*affective computing* (lett. calcolo delle emozioni) e l'Intelligenza Artificiale per percepire, conoscere e interagire con la vita emotiva umana».

965 R. PICARD, *Affective Computing,* in *MIT Media Laboratory Perceptual Computing Section Technical Report,* n. 321, 1995 evidenzia che i criteri di analisi e progettazione dei sistemi volti a studiare e codificare le emozioni umane vantano una vocazione fortemente etica e sociale, in quanto volti a migliorare la qualità di vita delle persone e a superare le difficoltà pratiche che talune persone incontrano nella vita quotidiana. Ad esempio, l'*affective computing* poteva essere utilizzato per aiutare i bambini disabili a superare barriere cognitive ed emozionali ovvero a migliorare le relazioni sociali in ambito professionale. L'Autrice, tuttavia, in R. PICARD, *Affective Computing,* Cambridge, 1997 non manca di considerare che tali studi – sebbene nati per perseguire scopi virtuosi – potrebbero essere utilizzati in maniera distorta e negativa, con lo scopo di influenzare e condizionare le esigenze economiche degli individui ad esclusivo vantaggio degli operatori economici che utilizzano questi sistemi computazionali.

966 E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 518.

967 G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, 43; AI NOW INSTITUTE, AI *Now Report 2018,* dicembre 2018, 14.

968 *Affectiva,* creata dalla ricercatrice Rana el Kaliouby, allieva della Professoressa Picard, può vantarsi di aver creato il fenomeno del c.d. *Emotional AI* e del c.d. *Human Perception AI.* Si stima che siano quasi 5 milioni i video facciali degli utenti raccolti in tutto il mondo. Il sito dell'azienda è consultabile su *affectiva.com.*

ultimi anni risulta evidente il mutamento di prospettiva dei progetti presentati dall'azienda – talvolta in collaborazione con aziende del calibro di Google – spesso rivolti allo sviluppo di nuove applicazioni per *smartphone*[969].

Altro progetto, egualmente innovativo e altamente pericoloso per l'intrusività nella vita delle persone, è stato realizzato dall'azienda *Emoshape,* società che tramite i sistemi di riconoscimento delle emozioni mira ad analizzare le emozioni umane allo scopo di fornire agli utenti servizi sempre più personalizzati in base alle loro emozioni[970].

Ancor più inquietante è l'esperimento condotto da *Facebook* dal titolo "*contagio emotivo*", condotto in occasione delle elezioni politiche di medio termine negli Stati Uniti[971]. Basandosi sulle attività di *scanning* condotte su una platea di oltre 61 milioni di persone, nel 2010 *Facebook* mise a disposizione di una parte degli utenti un'icona che mostrava dove si trovasse il seggio elettorale più vicino, mentre ad altri utenti non era mostrato nulla. Osservando i dati sulla distribuzione geografica del voto, tale esperimento mise in luce la correlazione esistente tra l'icona e gli utenti che erano andati a votare. In quel caso, la *Big Tech* aveva "semplicemente" convinto le persone ad andare a votare, ma – sulla base del successivo esperimento condotto nel 2014 – è risultato evidente che per *Facebook* sarebbe possibile capire l'orientamento politico dei suoi utenti e convincere quelli più indecisi a votare per questo o quel candidato[972]. Gli scenari che si potrebbero dischiudere sarebbero devastanti.

Al contempo, sono stati finanziati progetti di ricerca finalizzati a creare modelli predittivi dei comportamenti umani, allo scopo di studiare (e guidare) le scelte economiche degli individui: anche in questo caso il movimento dei muscoli facciali, la mimica facciale, le espressioni di gioia o di rabbia, da elementi impercettibili e irrilevanti, si sono trasformati in terreno di studio[973].

---

[969] Come sottolineato in E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 522, è stata recentemente lanciata l'applicazione "*AffdexMe*" sugli *smartphone* Android, che – sebbene, si avverte, si trovi in una fase ancora embrionale e potrebbe non essere affidabile – si dichiara capace di rilevare e analizzare le sei principali espressioni facciali analizzate anche da Ekman: rabbia, disgusto, paura, felicità, tristezza e sorpresa: si veda il sito https://affdexme.it.softonic.com/mac.

[970] *Ibidem.*

[971] AA. VV., *A 61-million-person experiment in social influence and political mobilization*, in *Nature,* vol. 489, 2012, 295 ss.

[972] IL POST, *Facebook può influenzare un'elezione?* in *Il Post,* 7 maggio 2016, consultabile sul sito https://www.ilpost.it/2016/05/07/facebook-puo-influenzare-unelezione/.

[973] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 519, che sottolinea che anche la Commissione

Quanto ai fini perseguiti, dunque, si è definitivamente consumato il passaggio da scopi eminentemente etici e sociali, volti a migliorare la vita relazione ed emotiva dell'individuo, a scopi di previsione dei comportamenti umani con l'intento di indirizzare le scelte economiche dell'utente digitale[974]: come è stato efficacemente sottolineato «[i] territori intimi del sé, come la personalità e le emozioni, vengono accaparrati come comportamenti osservabili e trasformati in ricchi depositi di *surplus* predittivo»[975].

A tutto ciò si aggiunga che risulta ormai chiaro, alla luce degli studi sperimentali condotti dalla *behavioral Law & Economics,* che il comportamento dell'individuo solo raramente è orientato alla massimizzazione del suo vantaggio economico, mentre spesso è influenzato da disposizioni caratteriali (ad esempio, la propensione al rischio), da suggestioni emotive (si pensi al c.d. effetto *framing,* in base al quale il soggetto opera scelte differenti a seconda del modo in cui il problema gli venga presentato), a cui si devono oggi aggiungere le suggestioni pubblicitarie e le pratiche commerciali cui è costantemente sottoposto, nonché le reti parentali e clientelari e, ovviamente, il «bisogno»[976].

Sfruttando le debolezze umane, dunque, i sistemi di riconoscimento delle emozioni hanno inaugurato un nuovo capitolo del mercato digitale, volto a realizzare «nuovi mezzi di modifica del comportamento umano»[977].

Si comprende bene, allora, come siffatti sistemi di riconoscimento delle emozioni – che hanno trovato una prima (ma inefficace e forse ingenua) formulazione normativa nella Proposta di Regolamento sull'IA della Commissione europea[978] – sono diventati

europea ha finanziato il progetto SEWA (*Automatic Sentiment Analysis in the Wild*) per sviluppare algoritmi capaci di leggere l'emozione provata dall'individuo quando vede un contenuto digitale.

[974] *Ibidem.*

[975] Così scrive S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma, 2019, 305.

[976] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 523. Risultano ormai superate la teoria economica neoclassica e la successiva teoria giuseconomica. Per un'analisi più approfondita, si veda R. VIALE, *Quale mente per l'economia cognitiva,* in R. VIALE (a cura di), *Le nuove economie: dall'economia evolutiva a quella cognitiva: oltre i fallimenti della teoria neoclassica,* Milano, 2005; D. KAHNEMAN, A. TVERSKY, *«Prospect Theory»: An Analysis of Decision under Risk,* in *Econometrica,* 1979, 33 ss.; A. GENTILI, *Il ruolo della razionalità cognitiva nelle invalidità negoziali,* in *Riv. Dir. Civ.,* 2013, 1123.

[977] S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma, 2019, 309.

[978] Ne abbiamo parlato diffusamente nel Secondo Capitolo, nel paragrafo §2.2, evidenziando al contempo le criticità formulate dall'EDPB e dall'EDPS e dal Garante per la protezione dei dati personali nel paragrafo §2.2.3.

pericolose forme di intrusione della vita reale delle persone[979]. Notevoli sono le criticità per la tutela della persona umana. Tali sistemi di codificazione delle emozioni, infatti, sono in grado di penetrare l'animo umano, inficiando le più intime capacità volitive e psicologiche dell'uomo e condizionandone le scelte e i comportamenti. Ad essere messa a dura prova è, quindi, non solo l'autonomia privata della persona[980], ma l'essenza umana nella sua dimensione più intima.

I condizionamenti che avvengono *online* sulla psiche degli individui agiscono a livello inconscio, plasmando e dirigendo le azioni dei singoli nel mondo reale. Alla luce dei tanti e vari progetti volti a implementare i sistemi di riconoscimento delle emozioni, appare chiaro che le emozioni umane potrebbero costituire il mezzo attraverso il quale raggiungere il fine economico delle grandi aziende di *marketing*[981].

Ma cosa ci impedisce di pensare che, se oggi i *Big Tech* studiano le emozioni umane per lanciare un'applicazione sugli *smartphone Android*, domani potrebbero manipolare le emozioni per altri (deplorevoli) fini? Se oggi *Facebook* è in grado di convincere sessanta mila persone ad andare a votare, che cosa potrebbe accadere domani, qualora decidesse di sfruttare le emozioni degli utenti per indirizzarli a votare per un determinato candidato politico?

### 4.3.2. *(Segue):* L'emozione quale mezzo di controllo psicopolitico dell'individuo: l'uomo non dovrebbe rivendicare il suo «diritto al tempo futuro»?

Come rilevato dal filosofo Han nella sua *"Psicopolitica",* nell'articolazione neoliberale della società, anche le emozioni sono vendute e consumate. È proprio con l'affermarsi di nuove forme di produzione post-industriali, immateriali e interconnesse, che l'emozione acquista particolare significato, perché ciò che conta non è tanto il valore d'uso di una cosa quanto il suo valore emotivo o cultuale[982].

Da un lato, questa «congiuntura dell'emozione» deriva dall'esigenza di creare maggiori bisogni e, di conseguenza, un maggiore stimolo all'acquisto. Nell'epoca

[979] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 519.
[980] *Ivi,* 520.
[981] *Ivi,* 523.
[982] B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016, 55.

contemporanea, in effetti, non acquistiamo più oggetti, ma l'emozione che quell'oggetto ci suscita: mentre le cose da consumare sono finite, le emozioni possono essere consumate all'infinito. La società neoliberale ha creato un nuovo campo di consumo: l'emotività[983].

Nella società disciplinare, ove ogni cosa è individuata, incasellata, classificata e organizzata, tutto deve funzionare, l'emozione rappresenta piuttosto un intralcio[984]. Al contrario, nella società neoliberale, le emozioni sono utili, perché devono essere sfruttate appieno per creare nuovi bisogni.

Da un altro punto di vista, l'emozione costituisce un mezzo di produzione del neoliberalismo. Questa nuova fisica del potere, infatti, ricorre alle emozioni nella misura in cui esse costituiscono preziose risorse per conseguire una maggiore produttività. Ad un certo stadio di produzione, la razionalità – che costituisce l'elemento maggiormente rappresentativo della società disciplinare – si scontra con i suoi limiti. All'improvviso, l'uomo che deve sottostare a rigide costrizioni e regole non trova più la motivazione necessaria per produrre. Invece, l'emotività, che si accompagna alla sensazione di libertà – entrambe elementi della società neoliberale – diventa il vero motore di produzione, in quanto restituisce all'individuo l'illusione di essere artefice del proprio destino e «progetto libero». Sentirsi liberi significa proprio poter esprimere le proprie emozioni. La tecnica di potere neoliberale insinua, e al contempo sfrutta, questa sensazione di libertà nell'esprimere le proprie emozioni[985].

Come abbiamo detto nei paragrafi precedenti, il regime neoliberale tende a sfruttare non solo il tempo, ma l'intera persona, tutte le sue risorse personali e tutta la sua attenzione[986]. Le tecniche di controllo neoliberale si appuntano sempre più sull'auto-ottimizzazione; non c'è spazio per il Negativo, ogni pensiero negativo deve essere convertito in positività; anche il dolore deve essere sfruttato, in quanto l'insoddisfazione e il dolore devono fungere da molla per il miglioramento della propria vita[987]. Ecco, allora, che l'individuo sfrutta anche le proprie emozioni e la temporanea motivazione che esse comportano per creare la propria impresa immateriale e sentirsi all'apice del successo.

[983] *Ivi,* 57.
[984] *Ivi,* 57.
[985] *Ivi,* 55-56.
[986] *Ivi,* 39-42.
[987] *Ibidem.*

La razionalità è caratterizzata da oggettività, universalità e persistenza, laddove l'emozione è soggettiva, veloce, volatile. La razionalità si accompagna a costanza, durevolezza e regolarità, mentre l'emozione è instabile e imprevedibile. L'economica neoliberale incorpora anche l'emozione nel processo di produzione e, anzi, favorisce la velocità della trasformazione emotiva per fare pressione verso l'accelerazione[988].

Inoltre, l'emozione è ormai divenuta elemento costitutivo nell'interazione comunicativa. Le emozioni costituiscono la «materia prima» nella comunicazione e nella gestione d'impresa. Anche il *manager* dei nostri giorni, più che un *manager* razionale, assomiglia ad un *trainer* motivazionale, in quanto deve essere in grado di motivare e stimolare i lavoratori su un piano pre-riflessivo e semi-cosciente[989]

In definitiva, da svariati punti di vista, anche l'emozione diviene utile nell'epoca neoliberale. La psicopolitica digitale si impossessa delle emozioni dell'individuo, in modo tale da insinuarsi nella sua psiche e nelle sue afferenze più intime e profonde e controllare l'uomo nella sua totalità. Attraverso l'emozione, la società contemporanea è in grado di influenzare l'uomo su un piano pre-riflessivo, agendo senza la sua consapevolezza e insinuandosi nel suo inconscio. Così, anche l'emozione si rivela un «medium estremamente efficace del controllo psicopolitico dell'uomo»[990].

Tramite i sistemi di riconoscimento facciale, le tecniche di analisi delle emozioni più intime e profonde dell'uomo si insinuano nella vita della persona, inscrivendosi in un processo di graduale perdita del c.d. diritto al futuro di ogni individuo[991].

Ebbene, è come se in ambito digitale la formulazione "io voglio volere" – cioè la rivendicazione dell'uomo al c.d. diritto al futuro – abbia perso di consistenza, intendendo il tempo futuro non già come una mera conseguenza del passato, ma come ambito di espressione della volontà di ogni singolo, ove i progetti futuri appartengono alla decisione libera e incondizionata di ognuno[992]. Il diritto al futuro si è trasformato in un «orpello dai tratti antichi»[993].

---

[988] *Ivi,* 56-57.
[989] *Ivi,* 58-59.
[990] *Ibidem.*
[991] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 539.
[992] Secondo Hannah Arendt, la volontà è «il nostro organo spirituale di un futuro per principio indeterminabile e pertanto foriero di novità»: H. ARENDT, *La vita della mente,* Il Mulino, Bologna, 2009.
[993] E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 539.

L'individuo deve essere libero di emozionarsi, di sperare, di scegliere il proprio futuro e anche di sbagliare; anche l'errore fa parte dell'architettura della libertà umana. Al contrario, i sistemi di riconoscimento delle emozioni sono in grado di condizionare e plasmare i comportamenti dell'utente in ambito digitale, ma tali scelte si rifletteranno inevitabilmente anche nello spazio Reale. Siffatti sistemi sono capaci di incanalare le scelte dell'uomo verso gli obiettivi economici e di *marketing* di pochi, per adesso limitandosi ad indurre l'individuo ad acquistare un bene anziché un altro, ovvero a selezionare un servizio piuttosto che un altro; ma in futuro, tale eterodeterminazione delle scelte dei singoli potrebbe dischiudere scenari di gran lunga peggiori, traducendosi in un pericoloso condizionamento di massa[994].

In altri termini, si tratta di sistemi di condizionamento endogeni che inducono nell'individuo bisogni che egli crede suoi e che rischiano di compromettere negativamente l'essenza umana[995]. Ebbene, dinanzi a siffatti sistemi di riconoscimento delle emozioni, che privano l'individuo del pieno dominio sulle sue emozioni e sulle più intime afferenze psicologiche, si può ancora sostenere che l'uomo è libero di volere?[996]

La sensazione è che, a seguito della rivoluzione tecnologica *in fieri*, l'*homo digitalis* stia perdendo lentamente, ma inesorabilmente, il proprio diritto al tempo futuro[997].

E allora, al di là dello strumento regolatorio prescelto, il diritto ha il dovere di ricollocare la tutela dell'individuo al centro delle trame del mercato digitale, per evitare di cadere nel drammatico errore di trasformare l'individuo da fine a mezzo[998]. Bisogna sostenere con forza che al centro delle scelte politiche e giuridiche debba essere sempre collocato l'uomo, con le sue debolezze e le sue passioni[999], nel rispetto della sua dignità e dei suoi diritti.

---

994 E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022, 543 e 550.
995 *Ibidem.*
996 *Ivi,* 539.
997 *Ivi,* 549.
998 *Ivi,* 527.
999 N. RANGONE, *Il contributo delle scienze cognitive alla qualità delle regole,* in *Mercato concorrenza regole,* 2012, 163: «[…] l'esigenza di porre al centro dell'attenzione dei decisori pubblici le persone reali, con le loro passioni, indicazioni, preferenze, debolezze».

## 4.4.L'incontro con l'Altro

Il tratto distintivo della cultura contemporanea è rappresentato dall'immediatezza: si parla, per l'appunto, di "compressione spazio temporale"[1000] per indicare lo spazio e il tempo che, in forza del progresso tecnologico, appaiono sempre più compressi, accorciati, ristretti[1001]: ogni esperienza deve essere vissuta in fretta, con l'unico obiettivo di prepararsi per l'evento successivo. Di conseguenza, anche il rapporto con l'Altro è teso a rimanere su un piano superficiale ed a consumarsi rapidamente. Secondo il sociologo e filosofo Bauman, infatti, la conoscenza dell'Altro è immediata, esteriore, nel senso che si indirizza alla sua superficie, nell'accezione più estetica del termine[1002]. Se infatti l'immediatezza fornisce, da un lato, l'illusione di una maggiore accessibilità agli altri e a se stessi, dall'altro lato, preclude lo sviluppo di legami stabili, basati sull'esperienza diretta e reale e non filtrati dal mondo "virtuale"[1003]. L'esperienza con l'Altro è ormai perlopiù ridotta alla connessione virtuale: l'Altro rappresenta qualcuno con cui rimanere costantemente connessi, pur rimanendo fisicamente isolati e distanti gli uni dagli altri.

La presenza dell'Altro «si è disciolta e smaterializzata nella rete»[1004]: essere sempre in contatto, senza vicinanza fisica, è la condizione normale delle relazioni odierne. Nella società contemporanea, infatti, assistiamo ad un cambiamento del significato stesso di relazione.

Il crescente e smisurato utilizzo, in ogni contesto, di strumenti tecnologici – quali, ad esempio, gli *smartphone* e i *social network* – che si frappongono tra le persone e il loro modo di relazionarsi, dà l'idea di quanto le forme di interazione siano al centro di un profondo cambiamento sociale. Nella società contemporanea, i nuovi mezzi di comunicazione hanno influenzato il rapporto con l'Altro, riducendolo spesso ad un'immagine statica, priva di ogni qualità emotiva e personale[1005]. Ciononostante, la relazione è pur sempre «tratto costitutivo dell'esistenza personale»[1006] e implica sempre «l'uscire da se stessi per incontrare l'altro nella sua diversità»[1007]. Le semplici

[1000] D. HARVEY, *La crisi della modernità. Riflessioni sulle origini del presente*, Il Saggiatore, Milano, 1993.
[1001] C. MUSCELLI, *L'altro e il tempo dell'immediatezza*, in *Rivista di estetica*, 56/2014, 35-53.
[1002] Z. BAUMAN, *La società dell'incertezza*, Il Mulino, Bologna,1999, 121.
[1003] C. MUSCELLI, *L'altro e il tempo dell'immediatezza*, in *Rivista di estetica*, 56/2014, 35-53.
[1004] *Ibidem.*
[1005] F. TINNIRELLO, *La perdita dell'alterità nella finzione social*, in *Il Chiasmo*, Treccani, 23 marzo 2018.
[1006] A. BELLINGRERI, *Imparare ad abitare il mondo. Senso e metodo della relazione educativa*, Mondadori Università, Milano, 2015.
[1007] R. G. ROMANO, *Il bisogno di relazione nell'era digitale*, in *Pensa Multimedia Editore*, Anno XVIII – n. 3 – ottobre 2017.

connessioni e i meri scambi virtuali, quindi, non appaiono sufficienti allo stabilirsi di una relazione o di un reale confronto e dialogo con l'Altro[1008].

Come ben sintetizzato dal filosofo Sergio Givone, «nella proliferazione delle immagini oscene, l'altro non è più persona, ma solo corpo, nuda vita», scrive, «E allora la vita dell'Altro, l'Altro, è il nulla»[1009]. L'Altro, nella società contemporanea, viene sostituito da una rappresentazione svuotata del contatto con il volto altrui. Secondo il filosofo ebreo Lévinas, però, «il volto è l'unico canale di fruizione della comunicazione e del dialogo con l'Altro-da-me: un altro essere umano, con una differente realizzazione dell'esistenza»[1010].

In particolare, il pensiero occidentale è caratterizzato, oggi più che mai, da una concezione dell'Altro come "prolungamento dell'io"[1011], negandone di conseguenza l'unicità e l'alterità. In un'ottica di contrapposizione, invece, secondo la prospettiva di Lévinas, «al mito di Ulisse che ritorna ad Itaca vorremmo contrapporre la storia di Abramo che lascia per sempre la sua patria per una terra ancora sconosciuta»[1012]. Secondo il filosofo, infatti, Ulisse rappresenterebbe l'ideale dell'uomo che, nella ricerca di se stesso, ripone la fiducia esclusivamente nelle proprie forze; Abramo, al contrario, sarebbe l'emblema dell'uomo in grado di "uscire da sé" e riporre la propria fiducia nell'Altro[1013]. Proprio il prevalere della figura di Ulisse su quella di Abramo, per Lévitas, sarebbe la causa dell'esaltazione dell'individualismo e del soggettivismo nella civiltà occidentale[1014].

Da tale concezione, inoltre, discenderebbe come conseguenza un atteggiamento di possesso e di dominio da parte degli uomini, causa di violenze e ingiustizie[1015]. Secondo Lévinas, il modo per salvarsi da tale destino è quello di «trovare all'uomo una parentela diversa da quella che lo lega all'essere – il che permetterà, forse, di pensare questa

[1008] R. G. ROMANO, *Il bisogno di relazione nell'era digitale*, in *Pensa Multimedia Editore*, Anno XVIII – n. 3 – ottobre 2017.
[1009] *Ibidem*.
[1010] *Ibidem*.
[1011] V. GIANMASTIANI, *La relazione con l'Altro: L'Abramo di Levinas e il Socrate di Arendt*, in *Dialegesthai – Rivista telematica di filosofia*, 31 luglio 2022.
[1012] E. LÉVINAS, *La traccia dell'Altro*, Pironti, Napoli, 1979, 30.
[1013] R. VINCO, *Ripartire dal volto dell'Altro. Spunti di riflessione sul pensiero di Emmanuel Lévinas*, in *Esperienza e teologia 4*, 1997.
[1014] *Ibidem.*
[1015] *Ibidem.*

differenza tra me e l'altro, questa disuguaglianza, in un senso assolutamente opposto all'oppressione»[1016].

All'umanesimo dell'essere, Lèvinas contrappone l'umanesimo «dell'altro uomo»[1017] e, in particolare, lega la rinascita dell'etica all'incontro dell'uomo con il «volto dell'Altro»[1018]. Tutto il pensiero del filosofo, quindi, è incentrato proprio sul riconoscimento dell'alterità e sul primato dell'Altro rispetto all'Io[1019] quale base per il fondamento e il riconoscimento dell'etica.

Lèvinas riuscì a sfuggire ai campi di sterminio tedeschi, ma non fu risparmiato dall'esperienza nei campi di concentramento francesi. Tale vissuto influenzò profondamente il pensiero del filosofo: nei campi di Auschwitz, si annullò qualsiasi base etica, in quanto ogni uomo venne ridotto ad un numero e privato del proprio nome e cognome[1020]. Tuttavia, proprio in tale condizione, l'uomo ha potuto riconoscere e rivendicare la più antica delle verità, ossia la «preziosità dell'uomo singolo e concreto»[1021]. L'obiettivo di Lèvinas, allora, è proprio quello di restituire ad ogni uomo la propria dignità, attraverso un'etica della responsabilità, ossia il riconoscimento dell'Altro come «divinità» e «trascendenza»[1022].

Per Lèvinas, l'Altro, e in particolare, il suo volto, è infatti la rilevazione di una trascendenza: l'Altro è l'uomo biblico, lo straniero, il povero[1023]. Ed è solo attraverso l'incontro con tali volti che l'uomo riuscirebbe a rimettere in primo piano l'etica.

### 4.5. L'Altro come fine e non come mezzo

Se per Lèvinas la riscoperta dell'etica sta nell'incontro con la diversità e nel riconoscimento del volto altrui, invece nella rete non c'è spazio per l'Altro: secondo il filosofo Giorgio Agamben «fa parte della barbarie tecnologica che stiamo vivendo la cancellazione dalla vita di ogni esperienza dei sensi e la perdita dello sguardo,

[1016] E. LÉVINAS, *Altrimenti che essere o al di là dell'essenza*, Jaka Book, Milano, 1995, 219-220.
[1017] E. LÉVINAS, *Umanesimo dell'altro uomo*, Il Melangolo, Genova, 1985.
[1018] *Ibidem.*
[1019] R. VINCO, *Ripartire dal volto dell'Altro. Spunti di riflessione sul pensiero di Emmanuel Lévinas*, in *Esperienza e teologia 4*, 1997.
[1020] *Ibidem*.
[1021] *Ibidem*.
[1022] E. TROTTA, *Il volto dell'Altro. L'umanesimo di Emmanuel Lèvinas*, in f*ilosofiaenuovisentieri2012*, 26 aprile 2020.
[1023] R. VINCO, *Ripartire dal volto dell'Altro. Spunti di riflessione sul pensiero di Emmanuel Lévinas*, in *Esperienza e teologia 4*, 1997.

durevolmente imprigionato in uno schermo spettrale»[1024]. Su *internet*, il dialogo e il confronto e, quindi, il rapporto con l'Altro è ridotto a commenti e "*like*" decontestualizzati, in cui l'essenza di ognuno diventa astratta e codificata in una identità digitale che spesso ha poco a che fare con la realtà e si colloca al di fuori della storia autentica dell'individuo[1025].

Con l'abbattimento dei confini tipico della società contemporanea, infatti, si verifica un cambio di paradigma sociale in cui la relazione si va a confondere con l'omologazione e qualsiasi dissenso diviene vietato in nome del *politically correct*, legittimando disuguaglianze e marginalizzazione[1026]. La relazione, quindi, da luogo di confronto e accettazione delle diversità, evolve in strumento di «dominio e di addomesticamento ideologico»[1027].

Non è un caso, in tal senso, che le fragilità delle relazioni umane appaiono come un fenomeno sempre più generalizzato ed attuale[1028]: nella società tecnologica odierna, la persona, ispirata da diffidenza ed individualismo, non è più preparata a vivere la relazione nella sua pienezza[1029].

Secondo il filosofo e psicologo Umberto Galimberti, nel deserto relazionale contemporaneo «fa la sua comparsa il gesto, soprattutto quello violento, che prende il posto di tutte le parole che non abbiamo scambiato né con gli altri per istintiva diffidenza, né con noi stessi per afasia emotiva»[1030]. Difatti, se la rete, da una parte, aiuta e facilita il mantenimento di relazioni, specie a distanza, dall'altra incide e trasforma il modo stesso di intendere la relazione, non più intesa «come capacità di accogliere l'altro con le sue diversità e di vivere insieme, ma ricercata come forma di autorealizzazione e di felicità personale». Di conseguenza, «[d]a evento duale, la relazione è diventata un evento personale, posto a cavallo tra la sfera del privato e quella del pubblico»[1031]. Sarebbe però un errore confondere l'iper-connettività e la sensazione di essere sempre insieme agli altri con l'incontro umano dello stare in relazione con gli altri, attraverso una presenza

[1024] G. AGAMBEN, *Requiem per gli studenti*, in *Diario della crisi – IISF*, 22 maggio 2020.
[1025] M. RUSSO, *L'uomo dai mille volti nell'era digitale*, in *Culture digitali*, 16 giugno 2019.
[1026] R. G. ROMANO, *Il bisogno di relazione nell'era digitale*, in *Pensa Multimedia Editore*, Anno XVIII – n. 3 – ottobre 2017.
[1027] *Ibidem*.
[1028] *Ibidem.*
[1029] *Ibidem*.
[1030] U. GALIMBERTI, *L'ospite inquietante. Il nichilismo e i giovani*, Feltrinelli, Milano, 2007, 49.
[1031] R. G. ROMANO, *Il bisogno di relazione nell'era digitale*, in *Pensa Multimedia Editore*, Anno XVIII – n. 3 – ottobre 2017.

fisica[1032]. Eppure, appare sempre più concreto il pericolo di sottrarsi alle relazioni sociali "reali", specie tra i giovani, per prediligere quelle virtuali caratterizzate da un minore impegno umano.

Tuttavia, se è solo dall'incontro con l'Altro – inteso come il diverso da noi – che si può accedere alla conoscenza di se stessi e alla conoscenza del mondo, allora sarebbe utile, se non necessario, accogliere il pensiero di Lèvinas e uscire da questi spazi virtuali, per incontrare l'Altro nella sua vera essenza e accoglierlo nella sua diversità.

Anche per la filosofa ebrea Hannah Arendt, la socievolezza rappresenterebbe «il più alto fine per gli uomini non nel senso di un obiettivo da raggiungere nel susseguirsi progressivo delle generazioni, ma in quanto principio intrinseco della stessa natura umana»[1033].

Hannah Arendt, pensatrice del Novecento, fu profondamente influenzata dal filosofo Kant e, in particolare, dalla terza formulazione dell'imperativo categorico di quest'ultimo: «[a]gisci in modo da considerare l'umanità, sia nella tua persona, sia nella persona di ogni altro, sempre anche al tempo stesso come scopo, e mai come semplice mezzo»[1034]. Secondo Kant, infatti, ogni essere umano dovrebbe considerare l'Altro come fine, ponendosi come limite alla possibilità di prendere decisioni egoistiche, cioè quelle che non considerino l'Altro[1035]. Influenzata da tale pensiero, la filosofa Arendt presentò una delle sue tesi fondamentali, e cioè l'idea che «la forma più elevata di agire, quella che esprime al massimo grado la dignità della condizione umana, non è, come pare ovvio per l'epoca moderna, il fare produttivo, bensì l'agire politico, in cui si passa da un atteggiamento individualistico, per quanto rivolto a entità sublimi, come la verità o la bellezza o a valori materiali, come il denaro, a uno di relazione, si vive cioè il mondo che ci circonda non come materia da usare e manipolare, ma come il luogo della partecipazione»[1036]. Anche per Hannah Arendt, quindi, la forma più elevata di agire è quella relazionale, vale a dire il modo in cui la persona interagisce e fonda la sua vita di relazione.

---

[1032] Z. BAUMAN, E. MAURO, *Babel*, Laterza, Roma-Bari, 2015.
[1033] H. ARENDT, *Lectures on Kant's political philosophy*, Chicago: University of Chicago Press, 1970, 73-74.
[1034] I. KANT, *Fondazione della metafisica dei costumi*, Rusconi, 1785, 143-145.
[1035] G. PILI, *Capire la "Fondazione della metafisica dei costumi" di Kant*, in *Scuola Filosofica – Rivista online*, 18 marzo 2018.
[1036] H. ARENDT, *Vita activa. La condizione umana*, Bompiani, Milano, 2017.

Nelle correnti di pensiero del Novecento, quindi, si esplora e ci si interroga sul concetto di "Altro" e tali riflessioni trovano trasposizione in particolare nell'esistenzialismo di Foucault, Sartre e Lèvinas.

Proprio quest'ultimo insisterà sull'importanza dell'Altro «non come rappresentazione di noi stessi, ma nella sua diversità»[1037]. Accogliere l'Altro, secondo Lèvinas, significa accettare l'essenza altrui, sentirsi partecipi della sua vita, responsabili della sua felicità e infelicità[1038].

Si introduce, quindi, il concetto di etica della responsabilità, in cui lo scopo dell'incontro con l'Altro non è ridotto alla conoscenza, ma è fondato su un rapporto di responsabilità reciproca[1039]. Secondo il filosofo francese, il vero valore fondante l'etica non è la libertà ma la responsabilità: solo attraverso l'incontro con il volto altrui, l'uomo riesce ad assoggettare il proprio Io e a porre la responsabilità su un piano prioritario rispetto alla libertà[1040].

In definitiva, Lévinas consegna alla filosofia contemporanea una "filosofia dell'Altro" in sostituzione della "filosofia del Medesimo"[1041]. Quest'ultima – che conduce a pensare l'umanità partendo dal Sé – privilegia le istanze autonome e individualiste dell'uomo, foriere di violenze e guerre[1042]. Invero, sarebbe proprio a partire dalla responsabilità dell'Io di fronte al volto dell'Altro che si troverebbe l'essenza della pace[1043]: «il volto dell'Altro, senza-difesa, è al contempo la tentazione di uccidere e l'appello alla pace. Il "Tu non ucciderai" è la responsabilità dell'uno-per-l'altro, l'impossibilità di lasciarlo solo di fronte al mistero della morte, dunque, la capacità di vivere e morire per l'altro, prendersene cura, mettersi al servizio dello straniero, dell'orfano, della vedova. La pace con Altri giunge fino a tanto: è tutta la gravità dell'amore del prossimo»[1044].

---

[1037] A. M. PACILLI, *L'incontro tra l'Io e l'Altro: l'incontro tra Filosofia e Psicologia*, in *Nel Futuro – Web magazine di informazione e cultura*, 13 febbraio 2017.
[1038] E. TROTTA, *Il volto dell'Altro. L'umanesimo di Emmanuel Lèvinas*, in *filosofiaenuovisentieri2012*, 26 aprile 2020.
[1039] *Ibidem*.
[1040] M. T. PACILÈ, *Quale pace per il nuovo millennio? Lèvinas e la responsabilità infinita,* in *Heliopolis – Culture civiltà politica* – Anno XV, Numero 2 – 2017.
[1041] *Ibidem*.
[1042] *Ibidem*.
[1043] *Ibidem*.
[1044] E. LÉVINAS, *Totalità e Infinito*. *Saggio sull'esteriorità*, Jaca Book, Milano, 1980, 24.

### 4.6. Il principio di responsabilità quale principio cardine dell'etica

Anche per il filosofo Hans Jonas la responsabilità costituisce il principio cardine dell'etica.

Nato in Germania nei primi anni del Novecento, il filosofo tedesco di origine ebraica è autore di una delle opere più importanti sul rapporto tra responsabilità e tecnologia: egli, nel suo *"Il Principio di responsabilità. Un'etica per la civiltà tecnologica"* ritiene l'uomo responsabile non solo nei confronti dell'Altro – inteso come soggetto che convive nel presente – ma anche, e soprattutto, nei confronti degli esseri umani che verranno[1045]. In tal senso, l'etica di Jonas è un'etica del presente e del futuro. Infatti, in contrapposizione all'imperativo kantiano «[a]gisci in modo tale che la tua massima possa valere come legge universale»[1046], manchevole di reciprocità tra presente e futuro, Jonas esprime il proprio imperativo: «Agisci in modo tale che le conseguenze della tua azione siano compatibili con la permanenza di un'autentica vita umana sulla terra»[1047].

Dunque, secondo Jonas, in base all'etica della responsabilità, l'essere umano dovrebbe tener conto, nelle proprie scelte e nelle proprie azioni, anche dell'Altro che non può far valere le proprie ragioni, perché non presente. Rivolge, quindi, uno sguardo al mondo futuro e alle generazioni prossime, in quanto le azioni umane di oggi si ripercuotono inevitabilmente anche nel domani, influenzando il futuro e l'esercizio dei diritti e delle libertà dell'umanità che verrà[1048].

L'etica di Jonas, quindi, è un'etica della responsabilità per la civiltà tecnologica e della sua potenziale potenza distruttiva. In particolare, è fondamentale che la filosofia, e in particolare l'etica, desti maggiore attenzione alla tecnologia, nella misura in cui essa riguarda qualsiasi aspetto della vita e dell'uomo[1049]. Il pensatore, dunque, ritiene necessario procedere ad una normativizzazione della tecnologia, affinché venga indirizzata verso un uso positivo. La tecnologia, infatti, si sostanzierebbe in un potere e, come ogni altro potere, essa è in grado «sia di fare male che di fare bene»[1050].

---

[1045] Il DODO, *L'etica della responsabilità in Hans Jonas*, in *Il Dodo pensiero*, 30 novembre 2019.
[1046] I. KANT, *Critica della ragion pratica. Testo tedesco a fronte*, Laterza, Bari-Roma, 1997.
[1047] H. JONAS, *Un'etica per la civiltà tecnologica,* Einaudi, Torino, 1990.
[1048] *Ibidem*.
[1049] *Ibidem.*
[1050] *Ibidem*.

# CONCLUSIONE

Quanto detto finora ci accompagna nel cuore della presente tesi: i sistemi di riconoscimento facciale e l'avanzamento tecnologico devono essere intesi quali strumenti per il controllo e la sorveglianza o, invero, finalizzati all'ampliamento delle libertà e dei diritti?

Nonostante la percezione legata all'innovazione tecnologica sia strettamente correlata a quella di progresso e di "miglioramento del mondo"[1051], abbiamo già sottolineato come, invero, tali applicazioni effettuino una vera e propria intrusione nella vita degli individui, attraverso un controllo sociale[1052] che rende incapace l'individuo di scegliere secondo le proprie volontà, con profondi riflessi sulle libertà individuali e collettive. Nella società contemporanea, il binomio "*privacy e sicurezza*" parrebbe lasciare il posto a quello di "*sorveglianza e sicurezza*"[1053]: il lento riconoscimento, da parte di numerosi Stati, del diritto alla *privacy* quale diritto fondamentale[1054] è messo in costante discussione, a volte in misura impercettibile, dal diritto alla sicurezza.

La società della trasparenza, «continuamente monitorata, tenuta sotto osservazione, implacabilmente registrata»[1055], trasforma i soggetti in un «docile oggetto di poteri altrui, che non sono soltanto quelli delle diverse agenzie di sorveglianza, che esercitano un controllo su ogni comportamento classificato come appartenente a una delle tante possibili forme di devianza»[1056]. Invero, nella società dei dati, la persona diventa essa stessa l'oggetto dei nuovi poteri: questi ultimi, attraverso la tecnologia, cercano non solo di sottoporre l'individuo ad un sempre più intrusivo controllo, ma anche di delinearne accuratamente i profili e le identità al fine di estrarre il maggior numero di informazioni

[1051] E. SADIN, *Critica della ragione artificiale. Una difesa dell'umanità*, Luiss University Press, Roma, 2019, 17.
[1052] N. COULDRY, *The Costs of Connection. How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford University Press, 2019.
[1053] G. FIORIGLIO, *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos* 2-2014.
[1054] G. FIORIGLIO, *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, Bononia University Press, Bologna, 2008.
[1055] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, 30.
[1056] *Ivi*, 26. A tal proposito, una celebre citazione del documentario *"The social dilemma"* ci offre lo spunto per un'importante riflessione: «se non stai pagando per il prodotto allora il prodotto sei tu» (J. ORLOWSKI, *The social dilemma* (2020), documentario Netflix).

da offrire al mercato per finalità economiche[1057]. L'essere umano, quindi, si trasforma da soggetto a oggetto, alla *mercé* delle logiche economiche e di mercato.

Lo sviluppo tecnologico, tuttavia, non deve essere esclusivamente demonizzato: l'avanzamento tecnologico, infatti, ha permesso e permette una più ampia collettivizzazione e l'abbattimento dei confini della conoscenza e della partecipazione dei cittadini[1058].

Di fatto, non ci troviamo di fronte a strumenti non conosciuti o conoscibili per loro natura, ma a tecnologie create dagli uomini per controllarne altri, che possono assurgere a «*tecnologie della libertà*» o «*tecnologie del controllo*»[1059]. In senso più ampio, come osservato da Bruno Montanari, riprendendo Carl Schmitt, «non è la tecnologia, come tale, ad essere divenuta un potere a sé stante, poiché la natura del potere è tale che può appartenere solo all'uomo e non ad una certa entità inanimata; essa, tuttavia, tiene in scacco l'uomo, perché si frappone alla relazione umana, impedendo agli uomini di guardarsi direttamente negli occhi, fino a rendere inumano il contesto umano»[1060].

La tecnologia, infatti, è definita come neutra, nel senso che può essere utilizzata sia per scopi benevoli che pericolosi: il nodo centrale sta proprio nel gestire i sistemi che la tecnologia ci consegna all'interno di un perimetro normativo che ne vieti gli usi pericolosi e, al tempo stesso, ne incoraggi lo sviluppo etico[1061].

Come analizzato approfonditamente nel presente elaborato, l'Unione europea – ma anche singoli stati, associazioni, aziende, organizzazioni e privati – ha stabilito dei principi e delle regole fondamentali per la gestione di siffatti strumenti tecnologici. Tuttavia, ciò potrebbe non essere sufficiente soprattutto in ragione del crescente affidamento delle responsabilità decisionali nelle "mani" degli algoritmi: alcune decisioni prese dalle Intelligenze Artificiali non appaiono prevedibili e predicabili dall'uomo[1062],

[1057] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, 26.
[1058] S. RODOTÀ, *Tecnopolitica*, *La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 2004.
[1059] *Ibidem*.
[1060] B. MONTANARI, *La fragilità del potere. L'uomo, la vita, la morte*, Mimesis, Milano-Udine, 2013, 138.
[1061] G. FIERRO, *AI per la sicurezza: le tecnologie di visione AI-Powered*, in *AI4Business*, 14 ottobre 2022.
[1062] M. M. MOLLICONE, *Il rischio dell'intelligenza artificiale applicata. Modelli di allocazione a confronto*, in *Actualidad Jurídica Iberoamericana*, Nº 18, febbraio 2023, 2108-2133.

in quanto l'algoritmo (nel caso di c.d. IA forti[1063]) decide in autonomia in base a quanto appreso nel tempo.

Orbene, potendo i sistemi di riconoscimento facciale assurgere sia a strumenti di progresso e miglioramento della qualità della vita sia a strumenti di compromissione dei diritti e di disumanizzazione della società, il tema principale appare, oggi più che mai, quello di definire un'etica dell'intelligenza artificiale. Tali applicazioni, infatti, hanno acceso un profondo dibattito proprio per la potenziale finalità di sorveglianza sulle persone[1064] e quindi del riflesso sui diritti fondamentali.

Oltre che per scopi di sicurezza, tali tecnologie di riconoscimento facciale sono sempre più utilizzate anche dai privati per finalità varie. Un esempio di applicazione delle TFR si rinviene nel *neuromarketing* per l'analisi del comportamento in risposta a determinate immagini interattive al fine di prevedere le preferenze dei consumatori. Uno tra i primi esperimenti nel campo del *neuromarketing* è stato quello condotto dalla Disney[1065] che, attraverso le tecniche di riconoscimento delle emozioni, ha tentato di "interpretare" lo stato emotivo dei telespettatori, durante una proiezione di un film, al fine di coglierne le diverse sfumature emotive e analizzarne il grado di apprezzamento partendo dalla lettura del viso[1066].

Tuttavia, come abbiamo sottolineato scomodando il filosofo Lèvinas, il volto umano assume un'importanza particolare, non solo in quanto capace di identificarci e di rilevare una serie di informazioni che ci qualificano – quali tratti identificativi, condizioni di salute, fascia di età, identità di genere[1067] – ma in quanto rappresentazione di una parte unica di ogni individuo e quale zona più espressiva del corpo: con i suoi 40 muscoli, il volto permette di rendere visibile *alla sensibilità umana* qualsiasi sfumatura emozionale. Non a caso, per Marco Tullio Cicerone il volto è l'immagine dell'anima[1068].

Dunque, in un mondo governato dagli algoritmi, i sistemi di riconoscimento facciale possono sostituire l'uomo?

---

[1063] E. HAHANA, *The AI Utility Levels Schema – Building an AI Classification*, in Https://law.stanford.edu/2022/04/02/the-ai-utility-levels-schema-building-ai-classification/.
[1064] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio*?, in *Diritto penale e uomo (DPU)*, 19 maggio 2021.
[1065] Per un maggiore approfondimento si veda D. COLDEWEY, *This facial recognition system tracks how you're enjoying a movie*, in *TechCrunch*, 26 luglio 2017.
[1066] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio*?, in *Diritto penale e uomo (DPU)*, 19 maggio 2021.
[1067] G. FIERRO, *AI per la sicurezza: le tecnologie di visione AI-Powered*, in *AI4Business*, 14 ottobre 2022.
[1068] M. T. CICERONE, *De Oratore*, Utet, Torino, 2017.

Secondo Lévinas, nel momento in cui si riconosce un individuo, dal suo volto si percepisce la sua anima: nel momento in cui io riconosco un volto, immediatamente si instaura in me un dovere di responsabilità. È il riconoscimento del volto che impone una responsabilità dell'Altro. Dunque, nel momento stesso in cui due individui si riconoscono come tali, partendo dal loro volto, si instaura un rapporto di c.d. *mutual responsibility.*

In un momento storico in cui tutto è divenuto liquido, e cioè possibile, è difficile immaginare strumenti giuridici in grado di prevedere e regolare esattamente tutte le infinite variabili del possibile: secondo Jonas, l'unico principio che può guidare l'uomo è il principio di autoresponsabilità.

Ebbene, se per i più importanti pensatori del Novecento l'etica sta nell'incontro con l'Altro e nel riconoscimento del suo volto, può una macchina – attraverso un *calcolo* – cogliere il viso nella sua autenticità ed espressività? Può un *software* rispettare il principio di responsabilità che si fonda proprio sul riconoscimento dell'Altro a partire dal volto? Si può chiedere ad un *software* di vedere l'Altro sempre come fine e mai come mezzo? Può un sistema di riconoscimento facciale, anche quando progettato dall'uomo nel rispetto di tutti i principi prescritti dalla legge, *calcolare* l'anima? La tecnologia è in grado di vedere in quel volto non un oggetto, ma un soggetto portatore di emozioni, di storia e di vita?

# BIBLIOGRAFIA


A. AGOSTINI, *Biometria e privacy: i presunti nemici a confronto,* Edis, Bologna, 2006.

A. ANJOS, S. MARCEL, *Counter-measures to photo attacks in face recognition: a public database and a baseline, International Joint Conference on Biometrics,* 2011.

A. BELLINGRERI, *Imparare ad abitare il mondo. Senso e metodo della relazione educativa*, Mondadori Università, Milano, 2015.

A. BERTILLON, *La photographie judiciaire: avec un appendice sur la classification et l'identification antropométrique,* Gauthier-Villars, Parigi, 1980.

A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy,* EPC LIBRI, Roma, 2002.

A. BONNEVILLE, *Des libérations préparatoires,* 1846.

A. CARRUGGIA, *Il ministro Piantedosi: «Più polizia nelle stazioni»* in *Governo Italiano, Ministero dell'Interno,* consultabile su https://www.interno.gov.it/it/stampa-e-comunicazione/interventi-e-interviste/ministro-piantedosi-piu-polizia-nelle-stazioni.

A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019.

A. DI CORINTO, *Ecco i database rubati a Facebook. Che cosa possono farne gli hacker,* in *Repubblica,* 15 febbraio 2021.

A. GENTILI, *Il ruolo della razionalità cognitiva nelle invalidità negoziali,* in *Riv. Dir. Civ.,* 2013, 1123.

A. KACHUR et AL, *Assessing the big five personality traits using real-life static facial images,* in *Nature Scientific Reports 10,* Article number: 8487, 2020.

A. M. PACILLI, *L'incontro tra l'Io e l'Altro: l'incontro tra Filosofia e Psicologia*, in *Nel Futuro – Web magazine di informazione e cultura*, 13 febbraio 2017.

A. MALRAUX, *La condition humaine,* Editions Gallimard, 1933.

A. MANTELERO, *La gestione del rischio,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

A. PRATOLINI, *Il Garante Privacy su Clearview AI: capire la sanzione per l'uso dei dati biometrici,* 16 marzo 2022, Industry News, consultabile su

https://blog.didomi.io/it/il-garante-privacy-su-clearview-ai-capire-la-sanzione-per-luso-dei-dati-biometrici.

A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo,* Il Saggiatore, Milano, 2019.

AA. VV, *Artificial Intelligence and life in 2030 – One hundred year study on artificial intelligence,* Stanford University, settembre 2016.

AA. VV., *A 61-million-person experiment in social influence and political mobilization*, in *Nature,* vol. 489, 2012.

Agendadigitale.eu [2021], *Controllo remoto degli studenti, vizio di tanti: il Garante non sanzioni solo Bocconi*, 30 settembre 2021, consultabile su https://www.agendadigitale.eu/sicurezza/privacy/controllo-remoto-degli-studenti-tanti-peccano-il-garante-non-sanzioni-solo-bocconi.

AGENZIA PER L'ITALIA DIGITALE, *Libro Bianco sull'intelligenza Artificiale al servizio del cittadino,* 21 marzo 2018.

AI NOW INSTITUTE, AI *Now Report 2018,* dicembre 2018.

AI NOW INSTITUTE, *AI Now Report 2019,* dicembre 2019.

B. MONTANARI, *La fragilità del potere. L'uomo, la vita, la morte*, Mimesis, Milano-Udine, 2013.

B.-C. HAN, *La società della trasparenza,* Nottetempo, Roma, 2014.

B.-C. HAN, *Nello sciame. Visioni del digitale,* Nottetempo, Roma, 2015.

B.-C. HAN, *Psicopolitica: il neoliberalismo e le nuove tecniche del potere,* Nottetempo, Roma, 2016.

C. CALDAROLA, *L'intelligenza artificiale: l'ombra sulla specie umana in un pianeta dominato dalla tecnica? O l'alba di una nuova umanità?,* in A. F. AURICCHIO, G. RICCIO, U. RUFFOLO, *Intelligenza artificiale tra etica e diritti: prime riflessioni a seguiti del Libro Bianco dell'Unione europea,* Bari, Cacucci, 2020.

C. DEL KASHMIR, *The Secretive Company That Might End Privacy as We Know It*, 18 gennaio 2020, New York Times, consultabile su https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

C. FIORE [2023], *Garante privacy: sanzionata una società per il trattamento dei dati biometrici dei propri lavoratori,* Diritto al Digitale, 13 aprile 2023, consultabile su https://dirittoaldigitale.com/2023/04/13/trattamento-dati-biometrici/.

C. FOGLIA, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019.

C. IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017.

C. LUCAS, *De la réforme des prisons,* tomo I, 1838.

C. MUSCELLI, *L'altro e il tempo dell'immediatezza*, in *Rivista di estetica*, 56/2014.

C. PALMIERI, *Intelligenza Artificiale, il nuovo quadro normativo europeo,* in *Altalex,* 17 agosto 2021, consultabile in https://www.altalex.com/documents/news/2021/05/20/intelligenza-artificiale-nuovo-quadro-normativo-europeo.

Città di Lecce, *Telecamere di videosorveglianza: il Garante chiude l'istruttoria preliminare*, 1 dicembre 2022, consultabile su https://www.comune.lecce.it/news/dettaglio/2022/12/01/telecamere-di-videosorveglianza-il-garante-chiude-l-istruttoria-preliminare.

CNIL, *Riconoscimento facciale: sanzione di 20 milioni di euro contro CLEARVIEW AI*, 20 ottobre 2022, consultabile su https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai.

CNIPA, *Linee guida per le tecnologie biometriche,* 8 ottobre 2004, in www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI – GARANTE EUROPEO PER LA PROTEZIONE DEI DATI, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),* 18 giugno 2021.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida 4/2019 sull'articolo 25 GDPR – Protezione dei dati fin dalla progettazione e per impostazione predefinita*, versione 2.0, 20 ottobre 2020.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione,* 3 ottobre 2017, emendate il 6 febbraio 2018.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Endorsement* 1/2018, 25 maggio 2018.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video,* 2.0, 29 gennaio 2020.

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nell'ambito delle forze dell'ordine,* 12 maggio 2022.

COMMISSIONE EUROPEA, *Allegati della Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione,* {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, 21 aprile 2021.

COMMISSIONE EUROPEA, *Call for a High-Level Expert Group on Artificial Intelligence,* 9 marzo 2018.

COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un'agenda digitale europea*, (COM(2010)245 definitivo), 19 maggio 2010.

COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e social europeo e al Comitato delle Regioni, Creare fiducia nell'Intelligenza Artificiale antropocentrica,* (COM(2019) 168 final), 8 aprile 2019.

COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa,* (COM(2018) 237 final), 25 aprile 2018.

COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, Piano coordinato sull'Intelligenza Artificiale,* (COM(2018) 795 final), 7 dicembre 2018.

COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA RICERCA E INNOVAZIONE, GRUPPO EUROPEO PER L'ETICA DELLE SCIENZE E DELLE NUOVE TECNOLOGIE, *Statement on artificial intelligence, robotics and "autonomous" systems,* 9 marzo 2018.

COMMISSIONE EUROPEA, *Libro Bianco sull'Intelligenza Artificiale – Un approccio europeo all'eccellenza e alla fiducia,* (COM/2020/65 final), 19 febbraio 2020.

COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, Relazione,* (COM(2021) 206 final), 21 aprile 2021.

Comune di Arezzo, *La Polizia Municipale di Arezzo protagonista del progetto pilota di sperimentazione Sicurezza sulla strada: occhiali "speciali" in dotazione agli agenti*, Comunicato stampa del 10 Novembre 2022, consultabile su https://www.comune.arezzo.it/notizie/polizia-municipale-arezzo-protagonista-del-progetto-pilota-sperimentazione-sicurezza-sulla.

CORDIS, *Il Gruppo europeo di etica delle scienze e delle nuove tecnologie si rinnova e guarda al futuro,* consultabile in https://cordis.europa.eu/article/id/16849-a-revitalised-european-group-on-ethics-and-new-technologies-eyes-the-future/it.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), C-283-11, *Sky Österreich GmbH contro Österreichischer Rundfunk*, 22 gennaio 2013.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), C-311/18, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, 23 luglio 2020.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González,* 13 maggio 2014.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite C-293-12 e C-594, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.,* 8 aprile 2014.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite C-581-10 e C-629-10, *Emeka Nelson e altri contro Deutsche Lufthansa AG e TUI Travel plc e altri contro Civil Aviation Authority*, 23 ottobre 2012.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite C-92-09 e C-93-09, *Volker und Markus Schecke GbR* (C-92/09) *e Hartmut Eifert* (C-93/09) *contro Land Hessen*, 9 novembre 2010.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), cause riunite n. C-362-14, *Maximillian Schrems c. Data Protection Commissioner,* 6 ottobre 2015.

CORTE DI GIUSTIZIA (GRANDE SEZIONE), causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, 23 luglio 2020.

CORTE DI GIUSTIZIA (IV SEZIONE), causa C-212/13, 11 dicembre 2014.

CORTE DI GIUSTIZIA (IV SEZIONE), causa C-291, *Schwarz c. Stadt Bochum,* 17 ottobre 2013.

CORTE DI GIUSTIZIA (IV SEZIONE), causa C-343-09, *Afton Chemical,* 8 luglio 2010.

CORTE DI GIUSTIZIA (V SEZIONE), causa C-101-12, *Herbert Schaible v. Land Baden-Württemberg,* 17 ottobre 2013.

CORTE EDU, *A.-M.V. c. Finlandia*, 14 novembre 2019.

CORTE EDU, *Buckley c. Regno Unito,* 29 settembre 1996.

CORTE EDU, *Khan c. Regno Unito,* 12 maggio 2000.

CORTE EDU, *P.G. and J.H. v. the United Kingdom,* 25 settembre 2001.

CORTE EDU, *Paradiso e Campanelli c. Italia*, 24 gennaio 2017.

CORTE EDU, *Peck v. The United Kingdom,* 28 gennaio 2003.

CORTE EDU, *Piechowicz c. Polonia*, 17 aprile 2012.

CORTE EDU, *Rotaru c. Romania,* 4 maggio 2000.

CORTE EDU, *S. e Marper c. Regno Unito,* 4 dicembre 2008.

CORTE EDU, *Silver e altri c. Regno Unito,* 25 marzo 1983.

CORTE EDU, *Z. c. Finlandia*, 3 dicembre 1996.

COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, aprile 2013, in https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81.

COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Practical guide on the use of personal data in the police sector*, febbraio 2018.

COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO

AUTOMATIC PROCESSING OF PERSONAL DATA, CONVENTION 108, *Guidelines on Facial Recognition,* T-PD (2020)03rev4, 28 gennaio 2021.

D. COLDEWEY, *This facial recognition system tracks how you're enjoying a movie*, in *TechCrunch*, 26 luglio 2017.

D. DI MALTA, *Clearview AI, sanzione privacy importante ma danni irreversibili*, 10 marzo 2022, Agendadigitale.eu, consultabile su https://www.agendadigitale.eu/sicurezza/privacy/clearview-ai-sanzione-privacy-importante-ma-danni-irreversibili/.

D. HARVEY, *La crisi della modernità. Riflessioni sulle origini del presente*, Il Saggiatore, Milano, 1993.

D. KAHNEMAN, A. TVERSKY, *«Prospect Theory»: An Analysis of Decision under Risk,* in *Econometrica,* 1979.

D. LESLIE, *Understanding bias in facial recognition technologies: an explainer,* in *The Alan Turning Institute,* 2020.

D. POLETTI, M. C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione,* in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* Giuffrè Francis Lefebvre, Milano, 2019.

E. BROUWER, *Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection, in European public law*, 26, 1, 2020.

E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio*?, in *Diritto penale e uomo (DPU)*, 19 maggio 2021.

E. HAHANA, *The AI Utility Levels Schema – Building an AI Classification*, 2 aprile 2022, in Https://law.stanford.edu/2022/04/02/the-ai-utility-levels-schema-building-ai-classification/.

E. LÉVINAS, *Altrimenti che essere o al di là dell'essenza*, Jaka Book, Milano, 1995.

E. LÉVINAS, *La traccia dell'Altro*, Pironti, Napoli, 1979.

E. LÉVINAS, *Totalità e Infinito*. *Saggio sull'esteriorità*, Jaca Book, Milano, 1980.

E. LÉVINAS, *Umanesimo dell'altro uomo*, Il Melangolo, Genova, 1985.

E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali,* in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019.

E. M. IANCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale,* in *Giustizia civile,* 2022.

E. MORDINI, *The ethical and social Implications of Biometricsì Technologies,* in *Biometrics: Biometrics; Enhancing Security or Invading Privacy? Proceedings of the Irishi Council For Bioethics' Conference,* 26 novembre 2008, Dublic.

E. R. BROUWER, *Eurodac: Its Limitations and Temptations, in European Journal of Migration and Law*, 4, 2, 2002, 231 ss.; F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer, Berlin-Heidelberg, 2012.

E. SACCHETTO, *Riconoscimento facciale, l'approccio italiano è in antitesi alla Ue: i nodi,* in *Network Digital 360, Agenda Digitale,* 7 dicembre 2022, consultabile in https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-lapproccio-italiano-e-in-antitesi-alla-ue-i-nodi/.

E. SADIN, *Critica della ragione artificiale. Una difesa dell'umanità*, Luiss University Press, Roma, 2019.

E. SANNA, *Le garanzie di sicurezza e autenticità delle informazioni in rete; in particolare del mandato informatico di pagamento,* in *Riv. Giur. Sarda, 2001,* fasc. 1, 311.

E. TROTTA, *Il volto dell'Altro. L'umanesimo di Emmanuel Lèvinas*, in f*ilosofiaenuovisentieri2012*, 26 aprile 2020.

EUROPEAN COMMISION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Commettee on Citizen's Freedoms and rights, Justice and Home Affaire (LIBE),* 2005 in http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), *Privacy anda Data protection by design – from policy to engineering,* 2014.

F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* Zanichelli, Bologna, 2019.

F. CASCETTA, M. DE LUCCIA, *Sistemi di identificazione personale*, in *Mondo digitale n. 1*, marzo 2004.

F. MANTOVANI, *Il problema della criminalità. Compendio di scienze criminali,* Cedam, Padova, 1984.

F. META, *Artificial Intelligence Act, accordo politico al Parlamento Ue sulle nuove norme,* in *Network Digital 360,* 28 aprile 2023, consultabile su https://www.corrierecomunicazioni.it/digital-economy/artificial-intelligence-act-accordo-politico-al-parlamento-ue-sulle-nuove-norme/.

F. NIETZSCHE, *Al di là del bene e del male,* in *Opere complete,* a cura di G. Colli e M. Montinari, Adelphi, Milano, 1968, vol. VI, tomo II.

F. NIETZSCHE, *Al di là del bene e del male. Preludio a una filosofia dell'avvenire,* Giunti-Demetra, Firenze-Milano, 2006.

F. PIZZETTI, *Decreto Gdpr, le urgenze dopo l'entrata in vigore (19 settembre),* in *Agenda digitale,* editoriale del 5 settembre 2018.

F. PIZZETTI, *Gdpr e linee guida per pmi, che c'è da attendersi dal Garante privacy,* in *Agenda digitale,* editoriale del 2 ottobre 2018

F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino, 2018.

F. PIZZETTI, *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya",* in *Dir. Inform.,* 2014.

F. PIZZETTI, *Modalità e requisiti necessari per la nomina a DPO in Intelligenza artificiale;* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei Dati Personali e regolazione*, G. Giappichelli Editore, Torino, 2018.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016.

F. SARTORE, *Privacy-by-design*, *l'introduzione del principio nel corpus del GDPR,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019.

F. TINNIRELLO, *La perdita dell'alterità nella finzione social*, in *Il Chiasmo*, Treccani, 23 marzo 2018.

F. TONACCI, *Roma, il "cervellone" che ha scovato l'aggressore di Termini: meno di un minuto per cercare tra 10 milioni di volti,* 5 gennaio 2023, La Repubblica, consultabile su https://www.repubblica.it/cronaca/2023/01/05/news/polacco_roma_termini_riconoscimentofacciale-382147119/.

FEDERAL TRADE COMMISSION, *Protecting consumer privacy in an era of rapid change; A proposed framework for business and policymakers. Technical report,* dicembre 2010.

G. AGAMBEN, *Requiem per gli studenti*, in *Diario della crisi – IISF*, 22 maggio 2020.

G. ALPA, *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile,* Pacini Editore, Pisa, 2020.

G. ALPA, *La responsabilità civile. Parte generale,* Utet, Torino, 2010.

G. BORGHI, *Riconoscimento facciale e Polizia: le linee guida n. 5/2022 dell'EDPB,* in *Il Quotidiano Giuridico,* 23 giugno 2022.

G. CIACCI, *Il diritto dell'informatica: brevi note in tema di protezione dei dati personali,* in G. CIACCI, G. BUONOMO, *Profili di informatica giuridica,* Cedam, Padova, 2018.

G. DE MABLY, *De la législation,* in Œuvres complètes, 1789, tomo IX.

G. FIERRO, *AI per la sicurezza: le tecnologie di visione AI-Powered*, in *AI4Business*, 14 ottobre 2022.

G. FIERRO, *AI per la sicurezza: le tecnologie di visione AI-Powered*, in *AI4Business*, 14 ottobre 2022.

G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità,* in G. RESTA, V. Z. ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* RomaTre-Press, Roma, 2016.

G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

G. FIORIGLIO, *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, Bononia University Press, Bologna, 2008.

G. FIORIGLIO, *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos* 2-2014.

G. GIANNONE CODIGLIONE, *Internet of things e nuovo regolamento privacy*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016.

G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali,* in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016.

G. LE BON, *Psicologia delle folle,* Edizioni Clandestine, Marina di Massa, 2013.
G. LUGLI, M. RIANI (a cura di), *Espressioni ed impronte facciali nel marketing,* Giappichelli, Torino, 2018.

G. LUSARDI, *Il rispetto dei principi applicabili al trattamento dei dati personali,* in AA.VV., *Privacy e data protection,* Ipsoa, Milano, 2022.

G. MALAZZANI, *Il trattamento di categorie particolari di dati personali,* in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists* in *in the General Data Protection Regulation,* in *International Data Privacy Law,*7, 4, 2017.

G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Editoriale scientifica, Napoli, 2021.

G. PEREZ, H. COOK, *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app the helps law enforcement,* in *CBS News,* 20 febbraio 2020.

G. PILI, *Capire la "Fondazione della metafisica dei costumi" di Kant*, in *Scuola Filosofica – Rivista online*, 18 marzo 2018.

G. PREITE, *Il riconoscimento biometrico. Sicurezza versus privacy,* Editrice Uni Service, Trento, 2007.

G. PROIETTI, *Intelligenza Artificiale: una prima analisi della proposta di regolamento europeo,* in *DB Non solo diritto bancario,* 27 maggio 2021, consultabile in https://www.dirittobancario.it/art/intelligenza-artificiale-una-prima-analisi-della-proposta-di-regolamento/#:~:text=Intelligenza%20artificiale%3A%20una%20prima%20analisi%20della%20proposta%20di%20regolamento%20europeo,-27%20Maggio%202021&text=Nel%20corso%20degli%20ultimi%20anni,(di%20seguito%20anche%20IA).

G. RESTA, V. Z. ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Romatre-press*,* Roma, 2016.

G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence,* in *Panel for the future of Science and Technologies*, STOA, PE 641.5 30, giugno 2020.

G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica,* Giappichelli, Torino, 2022.

G. SIMMEL, *Sociologia,* Edizioni di Comunità, Torino, 1998.

G. W. F. HEGEL, *Enciclopedia delle scienze filosofiche in compendio,* a cura di B. Croce, Laterza, Roma-Bari, 1994.

G. W. F. HEGEL, *Fenomenologia dello spirito,* Bompiani, Milano, 2000.

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata*, in *Gazzetta Ufficiale dell'Unione europea*, C 181/24, 22 giugno 2011.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *13.12 il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze*, Relazione 2019.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Audizione del Presidente dell'Autorità Garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 6 febbraio 2019 (doc. web. 9080870).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Audizione informale di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sul disegno di legge n. 920, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 27 novembre 2018 (doc. web. 9064421).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante – Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro,* 21 luglio 2005.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il primato dell'uomo sulle macchine intelligenti – Intervento di Ginevra Cerrina Feroni – Il Messaggero,* 22 aprile 2021.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria,* 21 dicembre 2017 (doc. web. 7496252).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 12 novembre 2014*, in *Gazzetta ufficiale della Repubblica Italiana*, Serie generale – n. 280, 3.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 12 novembre 2014*, in *Gazzetta ufficiale della Repubblica Italiana*, Serie generale – n. 280.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di riconoscimento biometrico e firma grafometrica,* 12 novembre 2014.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di Regolamento (UE) sull'Intelligenza Artificiale, Camera dei Deputati – Commissioni IX e X riunite,* 9 marzo 2022 (doc. web. 9751565).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Clearview AI*, 10 febbraio 2022 (doc. web. 9751362).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di Sportitalia, società sportiva dilettantistica a responsabilità limitata,* 10 novembre 2022 (doc. web. 9832838).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo",* 19 settembre 2019.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (doc. web. 9575877).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle*

*pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 11 ottobre 2018 (doc. web. 9051774).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Più sicurezza in ospedale con le impronte digitali,* 15 aprile 2008 (doc. web n. 1523435).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento n. 16 del 14 gennaio 2021 (doc. web n. 9542071).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento n. 35 del 13 febbraio 2020 (doc. web n. 9285411).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento n. 500 del 13 dicembre 2018 (doc. web n. 9068983).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Rasi: sui dati biometrici mantenere alto il livello di attenzione,* 23 novembre 2004.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy,* 16 aprile 2021.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022 (doc. web. 9751323).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Scorza: "Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché" – Intervento di Guido Scorza – AgendaDigitale,* 23 aprile 2021 (doc. web. 9579187).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto,* 26 luglio 2018 (doc. web. 9040256).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamenti di dati biometrici dei dipendenti. Verifica Preliminare*, 18 giugno 2015 (doc. web n. 4173465).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Uso di dati biometrici nelle operazioni di trasfusione,* 19 giugno 2008 (doc. web n. 1532480).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni*, 14 novembre 2022 (doc. web. 9823282).

GRUPPO DI LAVORO ARTICOLO 29, *Documento di lavoro sulla biometria,* WP 80, 1° agosto 2003.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679,* WP259, 28 novembre 2017.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del Regolamento UE 2016/679,* WP 259, 4 maggio 2020.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* WP 251.rev.01, 3 ottobre 2017.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del Regolamento (UE) 2016/679,* 29 novembre 2017.

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del Regolamento 216/679,* WP260, rev.01, 11 aprile 2018.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2012 on purpose limitation,* 569/13/EN - WP 203, 2 aprile 2013.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 03/2015 sulla proposta di direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati,* WP233, 1° dicembre 2015.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobile,* 22 marzo 2012.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro,* WP 249, 8 giugno 2017.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità,* WP 173, 13 luglio 2010.

GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche,* WP193, 27 aprile 2012.

GRUPPO DI LAVORO ARTICOLO 29*, Parere su alcune questioni fondamentali della direttiva (UE) 680 sulla protezione dei dati nelle attività di polizia e giustizia,* WP 258, 29 novembre 2017.

H. ARENDT, *La vita della mente,* Il Mulino, Bologna, 2009.

H. ARENDT, *Lectures on Kant's political philosophy*, Chicago: University of Chicago Press, 1970.

H. ARENDT, *Vita activa. La condizione umana*, Bompiani, Milano, 2017.

H. JONAS, *Un'etica per la civiltà tecnologica,* Einaudi, Torino, 1990.

HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, SET UP BY THE EUROPEAN COMMISSION, *A definition of AI: main capabilities and disciplines. Definition developed for the purpose of the AI HLEG's deliverables,* Bruxelles, aprile 2019.

I. ANRO', *Il margine di apprezzamento nella giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei Diritti dell'uomo* in F. COSTAMAGNA, A. ODDENINO, E. RUOZZI, A. VITERBO, L. MOLA, L. POLI (a cura di), *La funzione giurisdizionale nell'ordinamento dell'ordinamento internazionale e nell'ordinamento comunitario*, Editoriale Scientifica, Napoli, 2010 (contributo in opera collettanea).

I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and tge Confidentality of Personal Identifiable Images,* Springer, Cham, 2020.

I. COLONNA (a cura di), *La psicologia delle folle. Gustave Le Bon, 1895,* consultabile in https://www.unisalento.it/documents/20152/224009/Le+Bon-LaPsicologiadelleFolle.pdf/a1b11f49-dc1b-45a7-a797-8fd81aadb416?version=1.0.

I. K. SETHY, *Biometrics, Overview and Applications,* in STRANDBURG-RAICU, *Privacy and Technologies of Identity. A cross disciplinary conversation,* Springer, 2006.

I. KANT, *Critica della ragion pratica. Testo tedesco a fronte*, Laterza, Bari-Roma, 1997.

I. KANT, *Fondazione della metafisica dei costumi*, Rusconi, 1785.

ICAO, *Biometric deployment of Machine Readable Travel Documents,* in ICAO TAG MRDT/NTWG, *Technical Report,* 21 maggio 2004.

ICT Security, *Biometria e Sicurezza Informatica*, n. 39-40-4-42, Novembre 2005 – Febbraio 2006.

Il DODO, *L'etica della responsabilità in Hans Jonas*, in *Il Dodo pensiero*, 30 novembre 2019.

IL POST, *Facebook può influenzare un'elezione?* in *Il Post,* 7 maggio 2016, consultabile su https://www.ilpost.it/2016/05/07/facebook-puo-influenzare-unelezione/.

INTERNATIONAL BIOMETRIC GROUP (IBG), "*How is «biometrics» Defined?"* in https://www.biometricsinstitute.org/what-is-biometrics/.

J. BAUDRILLARD, *Agonie des Realen,* Marve Verlag, Berlino, 1978.

J. BENNET, *Saving face: Facebook Wants Access Without Limits,* in *The Center for Public Integrity,* 31 luglio 2017, in https://publicintegrity.org/inequality-poverty-opportunity/saving-face-facebook-wants-access-without-limits/.

J. BENTHAM, *Panopticon ovvero la casa d'ispezione,* con interventi di M. Foucault e M. Perrot, Marsilio, Venezia, 2009.

J. BENTHAM, *Panopticon,* in *Works,* ed. Bowring, tomo IV, 1843.

J. BITTLE, *Lie detectors have always been suspect. AI has made the problem worse,* in *MIT Technology Review,* 13 marzo 2020.

J. CONDEMI, *Clearnview AI: cos'è e come funziona il riconoscimento facciale,* in *AI4BUSINESS*, 2 maggio 2022, in *https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/*.

J. D. WOODWARD, N. M. ORLANS, P. T. HIGGINGS, *Identity Biometrics*, McGraw-Hill, 2003.

J. GALBALLY, P. FERRARA, R. HARAKSIM, A. PSYLLOS, L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System,* EUR 29808 EN, Publication Office of the European Union, Luxemburg, luglio 2019.

J. ORLOWSKI*, The social dilemma* (2020), documentario Netflix.

J. P. SARTRE, *L'essere e il nulla. La condizione umana secondo l'esistenzialismo,* Il Saggiatore, Milano, 2008.

J. TAYLOR, *Major breach found in biometrics system used by bank, UK police and defence firms,* in *The Guardian,* 14 agosto 2019.

K. CARBONI, *Il ministero dell'Interno vuole introdurre il riconoscimento facciale nei luoghi pubblici,* in *Wired,* 2 maggio 2023, consultabile su https://www.google.com/amp/s/www.wired.it/article/piantedosi-riconoscimento-facciale-stazioni-luoghi-pubblici/amp/.

L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy Europeo,* Giuffrè, Milano, 2016.

L. CARRER, *Riconoscimento facciale: come funziona e perché i piani del governo per introdurlo sono problematici,* in *ValigiaBlu,* 16 maggio 2023, consultabile su https://www.valigiablu.it/piantedosi-riconoscimento-facciale-luoghi-pubblici/#:~:text=A%20fine%20aprile%20Piantedosi%20ha,in%20un'intervista%20al%20quotidiano.

L. CLARK, *Google's Artificial Brain Learns to Find cat Videos,* in *Wired,* 26 giugno 2012, in https://www.wired.com/2012/06/google-x-neural-network/.

L. DE FIORE, *Big data e psicopolitica: ancora e sempre fatti versus interpretazione? Una riflessione filosofica sul presente futuro dei big data,* in *Forward,* novembre 2016, consultabile su https://forward.recentiprogressi.it/it/rivista/numero-4-big-data/articoli/big-data-e-psicopolitica-ancora-e-sempre-fatti-versus-interpretazione/.

L. F. BARRETT ET AL., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements,* in *Psychological Science in the Public Interest,* 20, 1, 2019.

L. FEROLA, *La "nuova figura" del responsabile della protezione dei dati personali e le sue caratteristiche*, in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, Giuffrè Francis Lefebvre, Milano, 2019.

L. P. BALTARD, *Architectonographie des prisons,* 1829.

M CASTIGLI, A. LONGO, *Riconoscimento facciale "anti-stupro", in Italia,* in *Network Digital 360, Cybersecurity 360,* 2 maggio 2023, consultabile su https://www.cybersecurity360.it/legal/ministro-dellinterno-vuole-il-riconoscimento-facciale-in-pubblico-ecco-i-rischi-principali/-.

M. A. BODEN, *L'intelligenza Artificiale,* il Mulino, Bologna, 2019.

M. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione,* in *Dir. Fam. Pers.,* 2015, 44, 2, 740-758.

M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo,* Il Mulino, Bologna, 2019.

M. EBERS, *Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges,* in M. EBERS, S. NAVAS NAVARRO (a cura di), *Algorithms and Law,* Cambridge University Press, Cambridge, 2020.

M. FOUCAULT, *Sorvegliare e punire: nascita della prigione,* Einaudi, Torino, 2014.

M. FOUCAULT, *Sull'origine dell'ermeneutica del sé: due conferenze al Dartmouth College,* a cura di MF/Materiali foucaultiani, Cronopio, Napoli, 2012.

M. M. MOLLICONE, *Il rischio dell'intelligenza artificiale applicata. Modelli di allocazione a confronto*, in *Actualidad Jurídica Iberoamericana*, Nº 18, febbraio 2023.

M. PURDY, P. DAUGHERTY, *Why artificial intelligence is the future of growth,* Accenture, 2016.

M. RUSSO, *L'uomo dai mille volti nell'era digitale*, in *Culture digitali*, 16 giugno 2019.

M. T. CICERONE, *De Oratore*, Utet, Torino, 2017.

M. T. PACILÈ, *Quale pace per il nuovo millennio? Lèvinas e la responsabilità infinita,* in *Heliopolis – Culture civiltà politica* – Anno XV, Numero 2 – 2017.

M. TORRE, *Privacy e indagini penali,* Giuffrè Francis Lefebvre, Milano, 2020.

M. TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia Digitale,* 24 ottobre 2018, che costituisce una rielaborazione della relazione su *Il libro Bianco dell'AGID sull'intelligenza artificiale,* presentata in occasione del *III Colloquio italo-francese sul Diritto del Web,* svoltosi presso l'Università LUISS Guido Carli il 21 giugno 2018.

M. TZANOU*, The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection*, in *Vienna Journal on International Constitutional Law,* 4, 3, 2010.

MINISTERO DELL'INTERNO DIPARTIMENTO DELLA PUBBLICA SICUREZZA, *Capitolato tecnico - procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. lotto n° 1*.

N. ALAY, H. H. AL-BAITY, *Deep learning approach for multimodal biometric recognition system based on fusion of Iris, Face and Finger Vein Traits,* Sensors*,* 2020.

N. COULDRY, *The Costs of Connection. How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford University Press, 2019.

N. RANGONE, *Il contributo delle scienze cognitive alla qualità delle regole,* in *Mercato concorrenza regole,* 2012.

N. VAVOULA, *Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement*?, in F. BIGNAMI (a cura di), *EU Law in Populist Times*, Cambridge University Press, Cambridge, 2020.

*New York Times* del 04.02.2013.

OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based techologies,* 30 giugno 2004, in *http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/NT000070D6/$FILE/JT00166988*.

ORACLE, *Che cos'è l'IoT?,* in *Oracle* consultabile in https://www.oracle.com/it/internet-of-things/what-is-iot/.

P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 2: Identification,* NIST Interagency/Internal Report (NISTIR) - 8271, dicembre 2020.

P. KAUR, K. KRISHAN, S. K. SHARMA, T. KANCHAN, *Facial recognition algorithms: a literature review,* in *Medicine, Science and the Law,* Volume 60 (2), aprile 2020.

P. TRIMARCHI, *Rischio e responsabilità oggettiva,* Giuffrè, Milano, 1961.

PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica,* 2015/2103 (INL), 2018/C 252/25, 16 febbraio 2017.

PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica,* 2015/2103(INL), 2018/C 252/25, 16 febbraio 2017.

PARLAMENTO EUROPEO, *Proposta di risoluzione del parlamento europeo, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate,* 2020/2012(INL), 8 ottobre 2020.

PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale* (2020/2016(INI)), 6 ottobre 2021.

PARLAMENTO EUROPEO, *Una politica industriale europea globale in materia di robotica e intelligenza artificiale, Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale*, 2018/2088(INI), 2020/C 449/06, 12 febbraio 2019.

POLITECNICO DI MILANO 1863, SCHOOL OF MANAGEMENT [2023], *Il digitale chiama: l'Italia risponde?* in *Osservatorio agenda digitale, Agenda digitale: la strada per digitalizzare la PA,* consultabile in https://blog.osservatori.net/it_it/agenda-digitale-come-digitalizzare-pa#:~:text=In%20sostanza%2C%20l'Agenda%20Digitale,sul%20potenziale%20delle%20tecnologie%20digitali.

PORTALE CONSULENTI [2023], *Impronte digitali senza specifici requisiti*, 9 gennaio 2023, consultabile su https://www.portaleconsulenti.it/impronte-digitali-senza-specifici-requisiti/.

R. ANGELINI, *Intelligenza Artificiale e* governance. *Alcune riflessioni di sistema,* in F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR,* in *Ciberspazio e diritto,* vol. 19, n. 60 (1-2-2018).

R. COLUCCINI, *Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale*, in IRPIMEDIA, 13 gennaio 2021, consultabile su https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/.

R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016.

R. G. ROMANO, *Il bisogno di relazione nell'era digitale*, in *Pensa Multimedia Editore*, Anno XVIII – n. 3 – ottobre 2017.

R. MAC, C. HASKINS, L. MCDONALD*, Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, 27 febbraio 2020, consultabile su https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019.

R. PANETTA, *Privacy is not dead: it's hiring!,* in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà,* Giuffrè Francis Lefebvre, Milano, 2019.

R. SENNETT, *Rispetto. La dignità umana in un mondo di diseguali,* a cura di G. Turnaturi, il Mulino, Bologna, 2004.

R. V. PICARD, *Affective Computing,* in *MIT Media Laboratory Perceptual Computing Section Technical Report,* n. 321, 1995.

R. V. PICARD, *Affective computing,* MIT Press, Cambridge, 1997.

R. V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, il Penalista, 16 gennaio 2019, consultabile su https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti.

R. VIALE, *Quale mente per l'economia cognitiva,* in R. VIALE (a cura di), *Le nuove economie: dall'economia evolutiva a quella cognitiva: oltre i fallimenti della teoria neoclassica,* Milano, 2005.

R. VINCO, *Ripartire dal volto dell'Altro. Spunti di riflessione sul pensiero di Emmanuel Lévinas*, in *Esperienza e teologia 4*, 1997.

Reuters, *Italy outlaws facial recognition tech, except to fight crime*, 14 novembre 2022, consultabile su https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/.

S. AMATO, F. CRISTOFARI, S. RACITI, *Biometria: i codici a barre del corpo,* Giappichelli, Torino, 2013.

S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica,* in *Ciberspazio e diritto,* 2005.

S. D. WARREN, L. BRANDEIES, *The right to privacy,* in *Harward Law Review,* 1890, n. 5.

S. DE CESARE [2022], *In arrivo 18 telecamere con riconoscimento facciale: posizionate in punti strategici della città*, Quotidiano di Puglia, 10 novembre 2022, consultabile su https://www.quotidianodipuglia.it/lecce/lecce_telecamere_riconoscimento_facciale_dove_a_cosa_servono_cosa_cambia-7043768.html?refresh_ce.

S. GIROTTO, *Il trattamento dei dati biometrici,* in *Il governo del corpo*, Giuffrè, Milano, 2011.

S. MARASCIO, *Intelligenza Artificiale, biometria e indagini di Polizia*, Ciberspazio e diritto, vol. 23, n. 70 (1 - 2022).

S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world,* Wiley Computer Publishing, 2002, 20.

S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014.

S. RODOTÀ, *Tecnopolitica*, *La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 2004.

S. RODOTA', *Il problema della responsabilità civile,* Giuffrè, Milano, 1964.

S. SALMERI, L. LUCANI, *AI Act: approvati gli emendamenti del Parlamento europeo alla Proposta di Regolamento,* in *Studio Previti Associazione Professionale,* 17 maggio 2023, consultabile su https://www.previti.it/ai-act-approvati-gli-emendamenti-del-parlamento-europeo-alla-proposta-di-regolamento.

S. SCAGLIARINI, *Il nuovo codice in materia di protezione dei dati personali: la normativa italiana dopo il d.lgs. n. 101/2018,* G. Giappichelli Editore, Torino, 2019.

S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016.

S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explaination of Automated Decision-Making Does Not Exists in the General Data Protection Regulation,* in *International Data Privacy Law,* 7, 2, 2016.

S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma, 2019.

STUDIO LEGALE MONDINI RUSCONI, *Big data: privacy, gestione, tutele: acquisizione e protezione dati, linee guida GDPR, concorrenza e mercato, proprietà intellettuale, valorizzazione,* Altalex Editore, Milano, 2018.

T. MARQUENIE, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework,* in *Computer Law e Security Review,* Volume 33, Issue 33, 2017.

TAG TALENT GARDEN, *Cos'è il Data Scraping e quali sono le sue applicazioni per l'Analisi Dati,* in *Tag Talent Garden,* 4 maggio 2022, consultabile su https://talentgarden.org/it/data/web-scraping-cosa-applicazioni/.

THE IRISH COUNCIL FOR BIOETHICS, *Biometrics: Enhancing Security or Invading Privacy?,* Dublin, 2009.

U. BECK, *La società del rischio. Verso una seconda modernità,* Carocci Editore, Roma, 2000.

U. GALIMBERTI, *L'ospite inquietante. Il nichilismo e i giovani*, Feltrinelli, Milano, 2007.

U. RUFFOLO, *Prefazione,* in A. F. AURICCHIO, G. RICCIO, U. RUFFOLO, *Intelligenza artificiale tra etica e diritti. Prime riflessioni a seguito del Libro Bianco dell'Unione europea,* Cacucci, Bari, 2020.

V. FERRARIS, *Il migrante datificato nei confini del futuro: senza potere di fronte a un oscuro potere*?, in S. GOZZO, C. PENNISI, V. ASERO, R. SAMPUGNARO (a cura

di), *Big Data e processi decisionali. Strumenti per l'analisi delle decisioni giuridiche, politiche economiche e sociali*, Egea, Milano, 2020.

V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea,* in *Federalismi.it,* 2017.

V. FLUSSER, *La cultura dei media,* a cura di A. Borsari, Bruno Mondadori, Milano, 2004.

V. GIANMASTIANI, *La relazione con l'Altro: L'Abramo di Levinas e il Socrate di Arendt*, in *Dialegesthai – Rivista telematica di filosofia*, 31 luglio 2022.

V. MAY-ER-SCHONBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think,* Hougthon Mufflin, Londra, 2013.

W. v. HUMBOLDT, *La diversità delle lingue,* a cura di D. Di Cesare, Laterza, Roma-Bari, 2000.

WIKILABOUR [2022], *Garante per la protezione dei dati personali, ordinanza ingiunzione contro Sportitalia ssd,* 10 novembre 2022, consultabile su https://www.wikilabour.it/segnalazioni/privacy/garante-per-la-protezione-dei-dati-personali-ordinanza-ingiunzione-contro-sportitalia-ssd/.

WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based techologies,* 30 giugno 2004.

Y. WANG, M. KOSINSKY, *Deep neural networks are more accurated than humans at detecting sexual orientation from facial images,* in *Journal of personality and Social Psycology,* 114 (2), 2018.

Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella moderna liquidità,* Laterza, Roma-Bari, 2015, versione e-book.

Z. BAUMAN, E. MAURO, *Babel*, Laterza, Roma-Bari, 2015.

Z. BAUMAN, *La società dell'incertezza,* Il Mulino, Bologna, 1999.

Z. BAUMAN, *Modernità Liquida,* Laterza, Roma, 2020.