Quaderni della Rivista Tecnologie e Diritto
diretta da Pasquale Femia e Carolina Perlingieri

ARCHITETTURE GIURIDICHE PER LA TRANSIZIONE DIGITALE

DIALOGHI INTERDISCIPLINARI PER GOVERNARE LA TECNOLOGIA

Atti del Convegno conclusivo
Governing Technology to Manage the Transition - GoTMaT
Padova, 26-29 novembre 2025

a cura di

Elisa de Belvis

Edizioni Scientifiche Italiane

ARCHITETTURE GIURIDICHE PER LA TRANSIZIONE DIGITALE

DIALOGHI INTERDISCIPLINARI PER GOVERNARE LA TECNOLOGIA

ARCHITETTURE GIURIDICHE PER LA TRANSIZIONE DIGITALE

DIALOGHI INTERDISCIPLINARI PER GOVERNARE LA TECNOLOGIA

Atti del Convegno conclusivo
Governing Technology to Manage the Transition - GoTMaT
Padova, 26-29 novembre 2025

a cura di

Elisa de Belvis

Edizioni Scientifiche Italiane

La pubblicazione di questo volume è stata possibile grazie al contributo dell'Unione Europea per il progetto "Governing Technology to Manage the Transition" (GoTMaT) CUP B53C22003990006 finanziato da bando a cascata del Programma di Ricerca "Security and rights in the Cyberspace (SERICS)" identificato con codice PE_00000014 - Next Generation EU – Piano Nazionale Resistenza e Resilienza (PNRR) - Missione 4 Componente 2 Investimento 1.3

DE BELVIS, Elisa (*a cura di*)
Architetture giuridiche per la transizione digitale.
Dialoghi interdisciplinari per governare la tecnologia
Atti del Convegno conclusivo *Governing Technology to Manage the Transition - GoTMaT*
Padova, 26-29 novembre 2025
Collana: Quaderni di Tecnologie e Diritto, 13
Napoli: Edizioni Scientifiche Italiane, 2026
pp. XVIII+574; 24 cm
ISBN 978-88-495-6192-0

80121 Napoli, via Chiatamone 7

Internet: www.edizioniesi.it
E-mail: info@edizioniesi.it

Gli autori dichiarano che l'eventuale utilizzo di sistemi di intelligenza artificiale per la redazione dei lavori è avvenuto soltanto a fini strumentali e di supporto dell'attività intellettuale.

Carolina Perlingieri

RIFLESSIONI SULLA QUESTIONE GIURIDICA DELL'USO DEI DATI BIOMETRICI

Sommario: 1. Rilievi introduttivi. L'àmbito di applicazione della biometria, la natura giuridica e la regolamentazione dei dati che la compongono. – 2. La dibattuta nozione di dato biometrico tra provvedimenti dei Garanti europei e interventi legislativi. – 3. Le principali criticità riconducibili ai dati biometrici: le finalità e le implicazioni dell'impiego dei sistemi di IA. – 4. La stringente connessione tra IA, siti *web* e piattaforme *online.* Il problema dell'identificazione biometrica. – 5. La categorizzazione biometrica connessa ai sistemi di IA come attività «ad alto rischio» alla luce del «contesto» e della «proporzionalità». - 5.1. La qualificazione della categorizzazione biometrica in relazione alle persone fisiche in forma aggregata. Profili evolutivi derivanti dalla proposta di rilettura della nozione di dato personale. – 6. La categorizzazione biometrica connessa ai sistemi di IA nelle attività di rilevamento delle emozioni: una questione culturale.

1. La biometria, nell'attuale contesto tecnologico, vede accrescere il suo ruolo non piú relegabile all'àmbito investigativo e giudiziario, nonché al contesto della pubblica sicurezza, ma esteso a sfere applicative sempre piú ampie e rilevanti della vita di relazione, dal godimento di particolari servizi, passando per la tracciabilità e il monitoraggio dell'accesso ad aree riservate, l'efficienza nel commercio, la sicurezza nel settore finanziario, fino alla tutela della salute, quale contributo alla diagnosi di malattie, considerato che anche l'analisi del DNA è stata ammessa tra le tecnologie biometriche.

Occuparsi di dati biometrici richiede, dunque, in primo luogo, individuarne la natura.

I «dati biometrici», tra i tipi di dati personali, si connotano per essere non semplici dati inerenti a caratteristiche in sé dell'interessato, bensí «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica *che ne consentono o confermano l'i-*

 ISBN 978-88-495-6192-0

dentificazione univoca, quali le immagini facciali o i dati dattiloscopici»[1].

Trattasi di una nozione, questa di «dato biometrico», prevista dal GDPR e ripresa dal RIA[2] (art. 4, n. 14 e Considerando 51; art. 3, n. 34 RIA), che deve essere integrata da un ulteriore criterio qualificante riconducibile alla finalità del rispettivo uso in relazione alla quale occorre distinguere tra autenticazione biometrica ed identificazione biometrica, due modalità operative con valenza diversa che presuppongono, tuttavia, un comune processo biometrico con la creazione di un modello matematico, detto *template*.

Questo contributo non riguarderà i problemi legati all'autenticazione quale verifica biometrica, diretta a confermare l'identità di una persona fisica allo scopo di accedere a un servizio, sbloccare un dispositivo, quale procedimento di raffronto di tipo "uno-a-uno" tra il *template* della caratteristica biometrica di un determinato soggetto, generato al momento della transazione, e uno specifico *template* presente in un dato archivio. Le riflessioni avranno, invece, ad oggetto le questioni connesse all'identificazione biometrica e all'identificazione finalizzata alla categorizzazione biometrica, quali trattamenti ulteriori rispetto a quel processo di estrazione di caratteristiche personali che consente di acquisire dati biometrici.

Infatti, l'identificazione è diretta ad attribuire un'identità personale mediante un raffronto di tipo "uno-a-molti" tra il *template* della caratteristica biometrica di un determinato soggetto e tutti i *template* presenti in un dato archivio e relativi a un insieme di soggetti.

[1] A mero titolo esemplificativo si allude ad impronte digitali quali le linee cutanee dei polpastrelli, di mani e piedi, o anche all'iride o alla retina, alla voce, a *pattern* comportamentali.

[2] Rispettivamente il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), consultabili rispettivamente in *https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=it*; *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689*.

ISBN 978-88-495-6192-0

2. Nonostante sia questa la definizione di «dato biometrico», confermata anche dal RIA, uno dei primi problemi ha riguardato tale nozione[3].

La questione è stata oggetto di una serie di pronunce da parte dei Garanti europei, compreso quello italiano, con riguardo al fenomeno dello *scraping* rispetto al quale è stata evidenziata la differenza tra attività di raccolta via *web* di immagini di volti di persone – non qualificabili di per sé come dati biometrici – e la successiva attività di trasformazione delle stesse, mediante algoritmi di *machine learning*, in immagini vettoriali da comparare con gli altri modelli indicizzati presenti nel *database* raschiato dal *web*[4], soltanto quest'ultima qualificata in termini di trattamento illecito per mancanza di un'adeguata base giuridica[5].

Distinzione confermata successivamente dal legislatore europeo, consapevole della differenza tra attività di raccolta nel *web* e attività di utilizzo delle banche dati cosí ottenute per operare il riconoscimento facciale, sí da introdurre con il RIA (art. 5, lett. *e*) RIA) non il divieto di *web scraping* bensí il divieto di riconoscimento facciale mediante sistemi di IA che utilizzano le banche dati ottenute con *scraping* non mirato[6] di immagini facciali, da internet o da filmati di telecamere a circuito chiuso; nonché, nella medesima prospettiva, dallo stesso Garante *privacy* italiano che, nel maggio 2024, ha emanato delle specifiche linee guida[7] per i gestori – pubblici o privati – di

[3] Sulle problematiche definitorie di dato biometrico, v. A.C. Nazzaro, *La tutela dei dati biometrici tra GDPR e AI ACT*, in *EJPLT*, 2024, p. 37 ss.

[4] S. Del Gatto, *La* governance *delle nuove tecnologie tra tentativi di regolazione e istanze di* self regulation. *Il caso del riconoscimento facciale*, in *Riv. it. dir. pubbl. comp.*, 2023, p. 37 ss., spec. p. 41 ss.

[5] F. Lala, *Data collection via web sraping: privacy and facial recognition after Clearview*, in *Riv. sc. giur. sc. cogn. int. art.*, 2023, p. 34 ss.

[6] Il divieto non riguarda lo *scraping* mirato, ossia quello volto a raccogliere immagini e video contenenti unicamente volti umani di individui specifici o di un gruppo predefinito al fine, ad esempio, di identificare responsabili di reati o le potenziali vittime.

[7] Cfr. il documento con il quale il Garante intende fornire prime indicazioni sul fenomeno della raccolta massiva di dati personali dal *web* per finalità di addestramento dei modelli di intelligenza artificiale generativa e segnalare possibili azioni di contrasto che i gestori di siti *internet* e di piattaforme *online*, sia pubblici che privati, operanti in Italia, quali titolari del trattamento dei dati personali oggetto di pubblicazione, potrebbero implementare al fine di prevenire, ove ritenuta incompatibile con le basi giuridiche e le finalità della pubblicazione, la raccolta di dati da parte

 ISBN 978-88-495-6192-0

siti *web* e di piattaforme *online*. Su costoro, che rivestono il ruolo di titolari del trattamento, gravano gli obblighi previsti dal GDPR tra i quali, in attuazione del principio di responsabilizzazione, quello di impedire a terzi che sviluppano sistemi di IAG l'impiego non autorizzato di dati personali pubblicati, sollecitando l'adozione di azioni di contrasto quali: *a*) la creazione di aree riservate alle quali accedere solo previa registrazione; *b*) il monitoraggio del traffico rete delle richieste *http*; *c*) gli interventi sui *bot* come l'inserimento di verifiche CAPTCHA, l'inserimento di clausole contrattuali *ad hoc* di divieto di utilizzo di tecniche di *web scraping* al fine di prevenire o mitigare le raccolte per finalità di addestramento di IAG.

3. In questa direzione, dunque, i problemi connessi ai dati biometrici attengono all'esigenza di continuare a riflettere sulle finalità di impiego dei sistemi di IA[8] e sulle implicazioni derivanti da tale utilizzo soprattutto tenendo conto della stringente connessione tra IA, siti *web* e piattaforme *online*.

In tale prospettiva, la diffusione dei meccanismi di IA all'interno del *web* e delle piattaforme può riguardare sia *a*) i sistemi diretti al riconoscimento di contenuti, come appena evidenziato con la raccolta di immagini spesso arricchite anche da altre informazioni correlate, si pensi alla geolocalizzazione della foto; sia *b*) quelli diretti alla categorizzazione biometrica che fanno ricorso alle c.dd. biocaratteristiche; sia infine *c*) quelli diretti al riconoscimento delle emozioni, in grado di processare dati sequenziali quali segni ossia linee, angoli, curve e rapporti di significato tra gli stessi per correlarli ai diversi sentimenti nel caso di immagini di volti associati a persone identificate ma anche identificabili.

Esigenza particolarmente pregnante se si considera la forza trasformativa dell'IA, avuto riguardo alla duplice circostanza che essa da un lato, non è piú soltanto un mero supporto tecnico della rete

di terzi per finalità di addestramento dei modelli di intelligenza artificiale: «*Web scraping* ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto», consultabile in *www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10020334*, nonché il provvedimento del 20 maggio 2024, consultabile sul sito *www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10020316*.

[8] Sul tema, V. Fusco, *Luci e ombre del GDPR nell'era dell'intelligenza artificiale*, in *Oss. dir. civ. comm.*, 2025, p. 77 ss., spec. p. 92 ss.

ISBN 978-88-495-6192-0

e delle piattaforme nella loro multifunzionalità e poliedricità, ma è diventata l'elemento centrale, in costante evoluzione, dei loro diversi modelli di *business*; dall'altro, comporta un aggravio dei rischi in quanto è in grado di incidere non soltanto sulle libertà e sui diritti fondamentali bensí sulla stessa peculiarità della condizione umana per quello che la tecnica può fare dell'uomo.

4. La riflessione sulla diffusione dell'impiego dei sistemi di IA, con riguardo ai dati biometrici, solleva innanzitutto un problema relativo all'identificazione biometrica.

È particolarmente recente l'ordinanza della Suprema Corte[9] che conferma la sanzione del Garante *privacy* nei confronti di un Istituto universitario.

Il Tribunale di Milano aveva accolto il ricorso dell'Università avverso un provvedimento del Garante *privacy*[10] che aveva individuato la violazione di una serie di norme in materia di trattamento dei dati personali – artt. 5, § 1, lett. *a*), *c*) ed *e*), 6, 9, 13, 25, 35, 44 e 46, del Regolamento, nonché 2-*sexies* del codice – per aver utilizzato un sistema di rilevamento del volto degli studenti durante esami a distanza al fine di controllarne la regolarità. Secondo il Garante il consenso espresso dagli studenti non poteva reputarsi una valida base giuridica del trattamento perché non avrebbe rappresentato una "manifestazione di volontà libera" [art. 4, § 1, n. 11) GDPR], in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento (cfr. considerando n. 43 del Regolamento). Il Tribunale aveva confutato il ragionamento del Garante negando *in nuce* la classificazione del dato come biometrico, poiché nel caso di specie si sarebbe trattato di una semplice comparazione di immagini fotografiche, senza un trattamento specifico e soprattutto senza la finalità di identificazione.

La Cassazione, al contrario, qualificava biometrico il trattamento in quanto ne riconosceva l'elaborazione tecnica che consentiva l'identificazione univoca dello studente dato che il *software* utilizzato dall'Università elaborava automaticamente le riprese, individuava e

[9] Cass., ord. 13 maggio 2024, n. 12967, in *Tecn. dir*., 2025, p. 424 ss., con nota di S. Esposito, *Trattamento dei dati biometrici mediante sistemi di intelligenza artificiale: rischi e tutele.*

[10] Garante per la protezione dei dati personali, 16 settembre 2021, n. 317 in *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9703988.*

 ISBN 978-88-495-6192-0

segnalava le anomalie, generava un video di sintesi contrassegnato con un complesso di operazioni e la successiva verifica, operata dal docente, costituiva un controllo *ex post* meramente ricognitivo non sufficiente ad incidere sulla qualificazione giuridica del trattamento già effettuato. Dunque, la Suprema Corte – considerando anche le Linee guida del Garante europeo 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29 gennaio 2020 – al punto 76, alla luce degli artt. 4, § 14, e 9 GDPR, qualifica la fattispecie "trattamento di dati biometrici" in virtú della presenza dei tre criteri relativi *a*) alla natura dei dati riguardanti biocaratteristiche; *b*) ai mezzi e alle modalità del trattamento in quanto ottenuti da un trattamento tecnico specifico e *c*) alle finalità del trattamento perché utilizzati per realizzare un'identificazione univoca.

Questa decisione, a mio avviso, suscita il quesito circa il possibile superamento, in questo contesto di istruzione e formazione, del divieto di trattamento dei dati biometrici in mancanza di consenso valido.

L'Allegato III del RIA, infatti, prevede che l'uso dei sistemi di IA è ammesso a certe condizioni nei settori ad alto rischio quali quello della biometria per i sistemi di identificazione biometrica remota; oltre che per i sistemi destinati a essere utilizzati per la categorizzazione biometrica e per il riconoscimento delle emozioni; nonché nel settore ad alto rischio dell'istruzione e formazione; per i sistemi destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli, oltre che per quelli utilizzati per valutare i risultati dell'apprendimento.

Dunque, se questi sistemi sono ammessi specialmente nel settore dell'istruzione e della formazione anche per monitorare e rilevare comportamenti vietati degli studenti durante le prove, occorre verificarne le condizioni d'uso, pur sempre in conformità al GDPR, individuando una base giuridica diversa dal consenso che, a mio avviso, andrebbe rinvenuta nel "legittimo interesse"[11] al trattamento

[11] L'invocabilità della base giuridica del legittimo interesse per il trattamento di categorie particolari di dati personali ai sensi dell'art. 9 GDPR è in linea anche con quanto previsto dall'art. 8, comma 1 "Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario" della l. n. 132 del 2025 "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", in *www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/sg*. Tale base giuridica, infat-

ISBN 978-88-495-6192-0

di dati biometrici. Trattamento che è qualificabile come necessario nell'ottica di assicurare la finalità di formazione e che deve essere anche proporzionato alla predetta finalità e prevedere sia misure appropriate e specifiche a tutela dei diritti fondamentali dell'interessato sia una limitazione temporale rispetto alla conservazione dei dati in coerenza con i princípi di minimizzazione e responsabilizzazione.

In questi termini, la risposta al quesito relativo al superamento del divieto di trattamento di dati biometrici in mancanza di consenso valido è positiva tenuto conto del RIA e delle basi giuridiche alternative al consenso al trattamento dei dati personali.

5. La biometria, come accennavo, collegata ai sistemi di IA ne qualifica la natura in termini di alto rischio, non soltanto, con riguardo all'identificazione biometrica remota ma anche con riguardo ai sistemi destinati a essere utilizzati per la categorizzazione biometrica e per il riconoscimento delle emozioni.

ti, può essere invocata per lo sviluppo e il funzionamento dei sistemi e dei modelli di IA a condizione che siano previste adeguate garanzie.

Posizione sollecitata dapprima dal Parere del Comitato europeo per la protezione dei dati (EDPB) del 18 dicembre 2024 sull'uso dei dati personali per lo sviluppo di modelli di IA (in *www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_it)* e, in seguito, confluita anche nella proposta di Regolamento (UE) 2025/837 che, con il nuovo art. 88c GDPR, riconosce – qualora il trattamento sia strettamente necessario e sia assicurato il bilanciamento dei diritti – il legittimo interesse quale base giuridica per lo sviluppo, l'allenamento e il funzionamento dei sistemi di IA subordinatamente a garanzie rafforzate (trasparenza, minimizzazione, diritto incondizionato di opposizione); nonché nella proposta di Regolamento (UE) 2025/836 che, con il nuovo art. 4a estende la possibilità di trattare categorie particolari di dati (art. 9 GDPR) a tutti i fornitori e utilizzatori di sistemi e modelli di IA non limitandosi ai soli sistemi ad alto rischio qualora il trattamento sia necessario e proporzionato.

Tuttavia, sul punto, da ultimo il parere congiunto 1/2026 dei Garanti *privacy* UE EDPB e EDPS, adottato il 20 gennaio 2026, *On the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, in *www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12026-proposal_en*, nel quale pur riconoscendosi l'appropriatezza dell'estensione si richiede, al fine di evitare potenziali abusi, che tali trattamenti siano circoscritti a situazioni gravi limitate al rilevamento, alla prevenzione e alla mitigazione di *bias* che possano influire sulla salute e sulla sicurezza delle persone e possano avere un impatto negativo sui diritti fondamentali o condurre a discriminazioni vietate dal diritto dell'Unione europea.

 ISBN 978-88-495-6192-0

Con riguardo ai primi relativi alla categorizzazione biometrica, l'Allegato III del RIA li definisce (art. 3, n. 40 RIA) sistemi che utilizzano dati biometrici al fine di assegnare le persone fisiche a categorie specifiche, di classificarle in una o piú categorie in base ad attributi sensibili quali età, sesso, ma anche abitudini di consumo o in base al solo comportamento umorale a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive.

Dunque, sono ammessi e, anche in tal caso, ciò che è vietato è la finalità di un utilizzo del punteggio sociale, c.d. *credit scoring* delle persone fisiche o delle persone in quanto appartenenti a gruppi, per realizzare un trattamento pregiudizievole o sfavorevole in contesti sociali non collegati a quelli nei quali i dati sono stati in origine generati-raccolti o un trattamento ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità [art. 5, lett. *c*) RIA].

Due condizioni che ponendo dei confini conformativi all'attività di profilazione nei limiti di «contesto» e di «proporzionalità» generano un problema interpretativo. In questa direzione la soluzione deve fondarsi su una cornice assiologica in coerenza con la centralità della persona nell'ordinamento[12]. Sí che, la valutazione deve riguardare la verifica di due nessi: quello relativo al "contesto sociale" che, alla luce di tale approccio, non può che essere interpretato quale nesso funzionale coerente tra i dati raccolti, generati e inferiti[13] e il fine rispetto al quale il profilo risulta servente; quello riguardante la "proporzionalità"[14], la

[12] P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972, *passim*; Id., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, 2005, spec. pp. 3 ss., p. 63 ss.; Id., Privacy *digitale e protezione dei dati personali tra persona e mercato: relazione svolta a Firenze*, in *Foro nap.*, 2018, p. 481 ss.

[13] Cfr. B. Parenzo, *La profilazione algoritmica nel prisma dell'autonomia privata*, Napoli, 2024, pp. 235-236.

[14] Sulla necessità del trattamento e della elaborazione dei dati biometrici secondo i princípi di proporzionalità ed equità, v. F. Fontanarosa, *Dati biometrici e tutela della* privacy *tra divergenze giuridiche ed esigenze di unificazione*, in *Ann. dir. comp*., 2019, p. 807 ss.; con specifico riferimento alla declinazione della proporzionalità quale parametro per gli interventi dell'autorità di polizia, v. S. El Sabi, *La tutela della* privacy *nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Dir. inf.*, 2023, p. 789 ss., spec. p. 813 ss.

In termini generali, sulla rilevanza del principio di proporzionalità quale strumento di bilanciamento tra diritti e libertà costituzionali, anche in rapporto alla ragionevolezza, v. P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo*

ISBN 978-88-495-6192-0

«giusta proporzione o quantificazione» quale parametro non separabile dalla ragionevolezza[15].

5.1. La scelta del legislatore europeo di consentire l'attività di profilazione nei limiti di «contesto» e di «proporzionalità» mediante categorizzazione biometrica rappresenta il recepimento normativo di una pratica diffusa da tempo, impiegata dalle piattaforme (classificazione finalizzata alla profilazione) le quali, per superare il divieto di profilazione senza consenso, introdussero la predisposizione di "schede gruppi" dove la schedatura avveniva su base volontaria.

Infatti, di fronte al divieto di profilazione individuale e al divieto di uso di dati biometrici senza il consenso esplicito (artt. 22 e 9 GDPR), l'*escamotage* consentiva ugualmente la profilazione sulla base dell'appartenenza volontaria a determinati gruppi.

Al riguardo, dunque, occorre chiedersi se sia possibile escludere la natura di dato biometrico quando tali dati sono utilizzati per categorizzare gruppi.

Secondo un parere del WP29 del Gruppo di lavoro art. 29, oggi *European Data Protection Board* (EDPB), la natura di dati personali rispetto ai dati biometrici in questo caso verrebbe meno in quanto utilizzati per categorizzare "persone non individuate" perché si presentano in forma aggregata.

Parere che, a mio avviso, può sollevare qualche perplessità dato che le persone fisiche in forma aggregata "non individuate" sono individuabili soprattutto se il parametro biometrico si connota per la

il sistema italo-europeo delle fonti, II, *Fonti e interpretazione*, 4ª ed., Napoli, 2020, p. 185 ss.; G. Scaccia, *Ragionevolezza e proporzionalità nel diritto costituzionale*, in A. Fachechi (a cura di), *Dialoghi su ragionevolezza e proporzionalità*, Napoli, 2019, p. 177 ss.; E. Giorgini, *Ragionevolezza, proporzionalità e bilanciamento*, in G. Perlingieri e A. Fachechi (a cura di), *Ragionevolezza e proporzionalità nel diritto contemporaneo*, Napoli, 2017, p. 513 ss.

[15] Ampiamente, sulla portata del principio di ragionevolezza e sulle sue specifiche declinazioni applicative, v. G. Perlingieri, *Ragionevolezza e bilanciamento nell'interpretazione recente della Corte costituzionale*, in P. Perlingieri e S. Giova (a cura di), *I rapporti civilistici nell'interpretazione della Corte costituzionale nel decennio 2006-2016*, Atti del 12° Convegno Nazionale, Napoli, 2018, p. 283 ss.; Id., *Sul criterio di ragionevolezza*, in G. Perlingieri e A. Fachechi (a cura di), *Ragionevolezza e proporzionalità nel diritto contemporaneo*, cit., p. 1 ss.; Id., *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, *passim*.

 ISBN 978-88-495-6192-0

sua unicità (si pensi soltanto alle caratteristiche del volto); individuabilità che costituisce requisito sufficiente per definire quei dati non anonimi e come tali, al pari dei dati pseudononimizzati, sottoposti alla disciplina del GDPR.

Questione che deve anche tener conto della revisione della nozione di dato personale che emerge dalla proposta di Regolamento (UE) 2025/837 sulla semplificazione della normativa sul digitale – c.d. *Digital omnibus* –, presentata dalla Commissione europea il 19 novembre 2025[16] che introduce un cambio di prospettiva nella qualificazione di dato personale non piú soltanto in termini positivi con la valorizzazione della riferibilità delle informazioni a una persona fisica identificata o identificabile[17], bensí in termini negativi stabilendo che un dato «non è *qualificabile* personale per un determinato soggetto se quest'ultimo non dispone dei mezzi (che di regola potrebbero essere ragionevolmente utilizzabili) per identificare la persona cui si riferisce».

Una nozione che è in funzione non soltanto della pura capacità tecnologica dell'utilizzatore, come ha invece evidenziato Oreste Pollicino[18] (titolare dei dati, titolare del trattamento, ecc.) [art. 3, § 1, lett. *a*)] ma, a mio avviso, del ragionevole utilizzo di questa capacità che può consentirne l'uso anche per trattare dati "identificabili" se si discorre di un utilizzo ragionevole, lí dove la ragionevolezza va intesa come giustificabilità, *rectius* diversa modalità di valutare l'entità dell'interesse sotteso all'identificazione, pur sempre da comparare e bilanciare con altri interessi[19].

[16] Il *Digital Omnibus Package*, che prevede le due proposte gemelle di Regolamento nn. 836 e 837/2025, si colloca nella cornice della strategia digitale 2024-2029 dando attuazione alle raccomandazioni del Rapporto Draghi sulla competitività dell'Unione al fine di snellire un ecosistema normativo eccessivamente frammentato e oneroso.

[17] Per ulteriori riferimenti, anche sul versante bibliografico, sia consentito rinviare a C. Perlingieri, *Creazione e circolazione del bene prodotto dal trattamento algoritmico dei dati*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Atti del 14° Convegno Nazionale, Napoli, 2020, p. 177 ss., spec. note 6 e 7.

[18] Cosí O. Pollicino, *Col* Digital Omnibus *l'Europa può smarrire sé stessa*, pubblicato il 21 novembre 2025 in *www.iaic.it/news/pollicino-col-digital-omnibus-leuropa-puo-smarrire-se-stessa/*.

[19] P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, IV, *Attività e responsabilità*, 4ª ed., Napoli, 2020, p. 99 ss., p. 121 ss., spec. p. 122; Id., *I princípi giuridici tra pregiudizi, diffidenza e conservatorismo*, in *Ann. SISDiC*, 2017, p. 1 ss. Nella medesima prospettiva, sul bilanciamento

ISBN 978-88-495-6192-0

6. La biometria collegata ai sistemi di IA ne qualifica la natura in termini di alto rischio oltre con riguardo all'identificazione biometrica e alla categorizzazione biometrica anche nei casi nei quali i sistemi sono utilizzati per il riconoscimento delle emozioni.

I dati biometrici possono consentire il rilevamento delle emozioni, una pratica anche questa ammessa, come risulta sempre dall'Allegato III del RIA, salvo se diretta a inferire le emozioni di una persona fisica nell'àmbito del luogo di lavoro e degli istituti di istruzione (art. 5, lett. *f*) RIA).

Il tema del rilevamento delle emozioni può essere analizzato soprattutto con riguardo alle pratiche di *neuromarketing* condizionanti l'inconscio che, nel contesto digitale, si avvalgono di sistemi di riconoscimento delle emozioni utilizzando dati biometrici e sfruttando quindi le vulnerabilità[20] quale posizione di debolezza del soggetto legata al contesto tecnologico che prescinde sia da uno *status*, sia da una posizione all'interno di una relazione soggettiva[21].

La stessa *Digital Market Manipulation*[22] si fonda sullo sfruttamen-

tra interessi necessariamente meritevoli di tutela, tra gli altri, V. Velluzzi, *Interpretazione sistematica e meritevolezza: alcune questioni*, in *Storia Metodo Cultura nella scienza giuridica*, *La meritevolezza*, 2022, p. 3 ss.; F. Maisto, *Per una teoria dell'osmosi tra la clausola generale della meritevolezza contrattuale e il principio costituzionale di ragionevolezza delle pretese giustiziabili*, in *Ann. SISDiC*, 2018, p. 123 ss.; I. Martone, *Il giudizio di meritevolezza. Questioni aperte e profili applicativi*, Napoli, 2017, pp. 9 ss., 20 ss.

[20] Sul concetto di vulnerabilità v. N. Lipari, *Vulnerabilità esistenziale e strumenti di tutela*, in *Ann. Sisdic*, 2018, p. 1, secondo il quale è impossibile «ridurre la vulnerabilità esistenziale e sociale a fattispecie», in quanto la vulnerabilità «chiede di essere colta nella specificità delle sue condizioni, non nell'astrattezza di una qualificazione tipologica»; da ultimo G. Carapezza Figlia, *Vulnerabilità digitale e post-modernità giuridica*, in *Dir. merc. ass. fin*., 2025, p. 3, il quale descrive la vulnerabilità quale «fenomeno stratificato».

Per la vulnerabilità con riferimento alle pratiche commerciali scorrette, v. le riflessioni di K. De Blasio, *Il* marketing *algoritmico tra tutela della* privacy *e pratiche commerciali scorrette*, in *Dir. inf.*, 2025, p. 379 ss., spec. p. 385 ss.

[21] In questi termini cfr. V. Ricciuto, *La persona e la vulnerabilità tecnologica: il diritto della tecnologia sostenibile*, in *Riv. dir. impr*., 2023, p. 489 s.

[22] In argomento J.D. Hanson, D.A. Kysar, *Taking Behavioralism Seriously: some evidence of market manipulation*, in *112 Harvard Law Rev.*, 1999, p. 1424; F. Babiloni, V.M. Meroni, R. Soranzo, *Neuroeconomia, Neuromarketing e Processi Decisionali*, Milano, 2007, p. 37 s.; R. Calo, *Digital Market Manipulation*, in *82 George Washington Law Rev.*, 2014, p. 995 s.

 ISBN 978-88-495-6192-0

to non soltanto delle distorsioni cognitive riconducibili all'inganno o alle pressioni, rispetto alle quali si può discorrere di pratiche ingannevoli o aggressive, ma soprattutto della vulnerabilità emotiva[23] del consumatore rispetto alla quale si pongono i maggiori problemi. Al riguardo le neuroscienze da un lato e gli studi dell'economia comportamentale[24] dall'altro hanno dimostrato che gli esseri umani tendono a svolgere processi decisionali di carattere automatico dal momento che la maggior parte del cervello umano è adibito a processi automatici e il comportamento dell'uomo «è sotto la dominante e non riconoscibile influenza dell'emotività, localizzabile in particolari regioni del cervello»[25], sorretto da elementi impulsivi quindi irrazionale.

Vulnerabilità che consente lo sfruttamento delle emozioni stimolando scelte, utilizzando i *bias* delle persone, cosa ben diversa dall'inganno o dall'indebolimento della resistenza che conduce a vere e proprie distorsioni cognitive per le quali è pur sempre possibile ricorrere ai rimedi civilistici.

Vulnerabilità emotiva, dunque, rispetto alla quale diventa arduo individuare un rimedio[26] potendo soltanto immaginare, eventual-

[23] Da ultimo S. Orlando (a cura di), *Profili giuridici del neuromarketing. Annuario 2023-2024 OGID Osservatorio Giuridico sull'Innovazione Digitale*, Roma, 2025; Id., *Neuromarketing, vizi del consenso e libertà di scelta*, *ivi*, p. 13, il quale evidenzia che «le emozioni e gli impulsi "istintivi" sembrano assumere un ruolo cruciale nel condizionare le scelte degli esseri umani (…), conducendoli a compiere errori (i c.d. *bias*) che deviano il processo decisionale rispetto a quello perfettamente razionale».

[24] In argomento v. A. Zoppini, *Le domande che ci propone l'economia comportamentale ovvero il crepuscolo del «buon padre di famiglia»*, in G. Rojas Elgueta e N. Vardi (a cura di), *Oltre il soggetto razionale. Fallimenti cognitivi e razionalità limitata nel diritto privato*, Roma, 2014, in *chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://romatrepress.uniroma3.it/wp-content/uploads/2019/05/1ledo-anzo.pdf*, p. 13.

[25] F. Babiloni, V.M. Meroni, R. Soranzo, *o.c.*, pp. 5-6.

[26] Di diverso avviso S. Orlando, *o.u.c.*, p. 17 ss., interrogandosi sull'invocabilità della disciplina dei vizi del consenso in caso di utilizzazione delle tecniche di *neuromarketing* nell'ottica di sfruttare i *bias* e condizionare le scelte dell'altra parte contraente al fine di garantire una maggiore tutela dell'individuo dinanzi a uno «stato generale di vulnerabilità digitale» (p. 21). Al riguardo l'A., muovendo dalla constatazione che sia la disciplina codicistica sia quella consumeristica rispondono alla medesima logica di protezione della libertà di scelta e del libero e consapevole consenso delle parti, afferma che l'utilizzo di tecniche di *neuromarketing* nella fase di formazione del contratto può costituire un'ipotesi di annullabilità del contratto quando sussistano i concreti presupposti per configurare l'errore e il dolo riconoscendo una conclusione parzialmente diversa soltanto con riguardo alla violenza fisica e morale.

ISBN 978-88-495-6192-0

mente, una mancanza di volontà e invocare la nullità dell'atto e non anche, come sostenuto[27], la nullità di protezione o il risarcimento del danno *ex* art. 1337 c.c. qualora sia provata la violazione dell'obbligo di comportarsi secondo buona fede a séguito della produzione di distorsioni cognitive. Due rimedi che, se invocabili a fronte di pratiche commerciali scorrette di *neuromarketing*, non si giustificano, a mio avviso, nel caso di mera vulnerabilità emotiva connotata da comportamenti irrazionali ben diversi da quelli di regola ascrivibili al soggetto tradizionale del diritto privato, quale attore razionale[28].

Dunque, diventa centrale e resta aperto il tema della manipolazione delle emozioni e l'uso sleale del *neuromarketing* nella contrattazione dove i nuovi pericoli riguardano l'esigenza di preservare, oltre al pensiero meditante, il pensiero nella sua *privacy*/nella sua riservatezza se è vero che «il volto è la finestra dell'anima»[29]. Pericoli che

Contra L. Tafaro, *Neuromarketing e tutela del consenso*, Napoli, 2018, secondo la quale non è condivisibile l'applicabilità della disciplina codicistica dei vizi del consenso in caso di utilizzazione di tecniche di *neuromarketing* escludendo: l'errore, difettando i requisiti dell'essenzialità e della riconoscibilità (p. 78 ss. e spec. p. 84); la violenza morale per la mancanza dei tratti tipici della molestia quale comportamento che arreca un disturbo o un disagio al consumatore al punto di spingerlo a contrarre al fine di far cessare il comportamento in questione (p. 87); il dolo determinante per l'assenza di un raggiro di rilevanza (p. 91).

Per un approccio critico in merito all'applicabilità dei tradizionali rimedi codicistici nell'àmbito della contrattazione di massa e in particolare nei contratti tra professionista e consumatore cfr. G. Vettori e G. Taddei Elmi, *Rimedi civilistici e disciplina della concorrenza*, in C. Rabitti Bedogni e P. Barucci (a cura di), *20 Anni di Antitrust. L'evoluzione dell'Autorità Garante della concorrenza e del Mercato*, Torino, 2010, p. 1039 s.; C. Tenella Sillani, *Pratiche commerciali sleali e tutela del consumatore*, in *Obbl. contr*., 2009, p. 780.

[27] In particolare cfr. L. Tafaro, *o.c.*, pp. 93 ss., 137 ss. e 181 ss., la quale prospetta per il contratto stipulato a séguito di atti promozionali di *neuromarketing* sia il ricorso alla categoria della nullità di protezione di cui all'art. 36 c. cons., quale norma speciale che può essere applicata analogicamente ai casi, aventi *eadem ratio* per i quali, come in tale ipotesi, sussiste una lacuna in ordine ai rimedi da attuare; sia il risarcimento del danno *ex* art. 1337 c.c. che sarebbe da individuare *ex se* (p. 97) in presenza di condotta di chi utilizza tecniche di *neuromarketing*.

[28] A. Zoppini, *Le domande che ci propone l'economia comportamentale ovvero il crepuscolo del «buon padre di famiglia»*, cit., p. 14 ss.

[29] S. Porter *et al*., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces*, in *Canadian Journ. of Behavioural Science*, 40, III, 2008, p. 171 ss.

 ISBN 978-88-495-6192-0

sono insiti nel sistema tecnologico e come tali in grado di incidere profondamente sulla collettività soprattutto in assenza di comportamenti razionali.

In questi termini, quindi, il problema è, in primo luogo, culturale e richiede lo sviluppo di uno spirito critico e di un'autonomia di pensiero acquisendo la consapevolezza di riuscire a distinguere le emozioni autentiche da quelle indotte che sono in grado di incidere su tutte le scelte a partire dalle piú piccole che, tra l'altro, sono quelle quotidiane e che avvengono, per lo piú, in modo casuale. È da queste che occorre iniziare al fine di recuperare quella consapevolezza che appare necessaria per formulare un equilibrato giudizio della desiderabilità quale espressione del controllo della personalità umana.

ISBN 978-88-495-6192-0

ELENCO DEGLI AUTORI*

Prof. Avv. Giuseppe Amadio, Università di Padova[1]

Prof. Avv. Elisa de Belvis, Università di Padova

Dott. Maria Costanza Gallinella Muzi, Prefettura di Padova

Dott. Adamo Antonello Ianniello, Prefettura di Padova

Prof. Antonino Nocera, Università di Pavia

Dott. Marco Arazzi, Università di Pavia

Dott. Alessandro Galeazzi, Università di Padova

Prof. Avv. Claudio Scognamiglio, Università Tor Vergata

Prof. Maria Savona, University of Sussex

Prof. Fabio Bravo, Università di Bologna

Prof. Elena Buoso, Università di Padova

Prof. Giulia Avanzini, Università di Pavia

Prof. Stefano Rossa, Università del Piemonte Orientale

Prof. Angela Ferrari Zumbini, Università Federico II di Napoli

Prof. Isabella Martone, Università della Campania Luigi Vanvitelli

Prof. Marina Pietrangelo, CNR

Prof. Carolina Perlingieri, Università Federico II di Napoli

Prof. Beatrice Zuffi, Università di Padova

Dott. Eugenia Italia, Tribunale per i Minorenni di Venezia

* L'ordine segue quello dei contributi all'interno del volume.

 ISBN 978-88-495-6192-0

Avv. Marco Ripa, Ordine degli Avvocati di Padova

Avv. Carolina Brunazzetto, Ordine degli Avvocati di Padova

Dott. Michele Manente, Notaio in Marcon

Prof. Alessia Fachechi, Università Vanvitelli

Prof. Anna Carla Nazzaro, Università degli Studi Internazionali di Roma

Prof. Avv. Marisaria Maugeri, Università di Catania

Prof. Avv. Francesco Macario, Università Roma Tre

Dott. Elena Belmonte, Università di Salerno

Prof. Silvia Signorato, Università di Padova

Prof. Alessandro Ciatti Caimi, Università di Torino

Prof. Riccardo Ursi, Università di Palermo

Prof. Claudio Sarra, Università di Padova

Avv. Marco Vianello, foro di Venezia

Prof. Giuseppe Corasaniti, *Universitas Mercatorum*

Avv. Alessia Campagnaro, Università di Padova

Dott. Anna Laura Coggi, Università di Padova

Dott. Francesco Magagna, Università di Padova

568

ISBN 978-88-495-6192-0

INDICE

 ISBN 978-88-495-6192-0

ISBN 978-88-495-6192-0

 ISBN 978-88-495-6192-0

Sezione VIII

Cybersicurezza e profili rimediali

Sezione IX

Etica degli algoritmi, datificazione della persona e sicurezza informatica nelle professioni legali

Sezione X

Le comunicazioni dei borsisti giuridici GoTMaT

572

ISBN 978-88-495-6192-0

LA BUONA STAMPA

Questo volume è stato impresso
nel mese di aprile dell'anno 2026 per
le Edizioni Scientifiche Italiane S.p.A.
Stampato in Italia

Edizioni Scientifiche Italiane

www.edizioniesi.it info@edizioniesi.it

https://www.edizioniesi.it
https://www.esidigita.it
edizioni_scientifiche_italiane
Edizioni Scientifiche Italiane
Edizioni Scientifiche Italiane

La profonda transizione digitale che caratterizza la nostra epoca impone al giurista una riflessione sistemica e richiede uno sforzo (ri)costruttivo delle stesse categorie dogmatiche del diritto che, pur necessitando di una ridefinizione, continuano a rappresentare strumenti imprescindibili di tutela della persona. Lo studioso del diritto, però, non può governare, da solo, le nuove tecnologie: è necessario un dialogo tra sapere giuridico e informatico, in una virtuosa contaminazione di competenze.

Il presente volume raccoglie oltre trenta contributi tratti dagli interventi del Convegno conclusivo del Progetto PNRR *Governing Technology to Manage the Transition - GoTMaT*, organizzato dall'Università di Padova. L'opera – frutto di un dialogo autenticamente interdisciplinare tra giuristi di differente specializzazione e informatici, esponenti del mondo accademico, professionale e istituzionale – propone un itinerario che intreccia la prospettiva civilistica sulla qualificazione del dato digitale con quella economica sul suo valore e sulla sua *governance*; affianca alla riflessione amministrativistica sull'agire algoritmico, sulla legalità e sulla riserva di umanità l'analisi informatica dei profili di cybersicurezza; coniuga lo studio dei dati personali come attributi della personalità con l'esame delle tecniche di trattamento biometrico e delle loro implicazioni sistemiche. Lungi dall'essere meramente teorico, il lavoro prende le mosse dai "casi d'uso" sviluppati presso le Pubbliche Amministrazioni coinvolte nel Progetto di ricerca – laboratorio applicativo in cui il confronto competenze giuridiche e informatiche si misura con problemi concreti di governo della tecnologia – e si estende alle professioni legali.

Elisa de Belvis è Professore Ordinario di Diritto privato nella Scuola di Giurisprudenza dell'Università degli Studi di Padova, ove insegna, tra l'altro, Diritto civile e Diritto Privato Generale e dell'Informatica. Attualmente insegna, altresì, al Master in Giurista Internazionale di Impresa. Ha tenuto corsi e lezioni al Corso di Dottorato in Diritto internazionale e Diritto privato e del lavoro (del cui Collegio Docenti è membro), alla Scuola di Specializzazione per le Professioni Legali delle Università di Ferrara, Padova, Trieste e Venezia Ca' Foscari, alla Leopold-Franzens-Universität Innsbruck, alla School of Law e al LLM (International Family Law) dello University College Cork.

È stata Responsabile Scientifico del progetto di ricerca "GoTMaT" e delle *Winter Schools* in *Private Law and Technology* organizzate in seno all'Ateneo patavino.

Ha partecipato come relatore a più di quaranta Convegni nazionali e internazionali.

È autrice di quattro monografie dedicate al diritto delle successioni, all'esecuzione privatizzata e ai rapporti tra dati personali, relazioni familiari e tecnologie digitali, nonché di oltre una quarantina di scritti minori, anche in lingua inglese.

7426075260

ISBN 978-88-495-6192-0