

L'evoluzione del diritto alla *privacy* nell'era dell'intelligenza artificiale: una comparazione tra ordinamento giuridico italiano e peruviano

The evolution of the right to privacy in the age of artificial intelligence: a comparison between the Italian and Peruvian legal systems

MARIA CRISTINA GAETA 

Ricercatore in Diritto privato

Senior Researcher ReCEPL

Università degli Studi Suor Orsola Benincasa

Abstract

Il contributo analizza l'evoluzione normativa del diritto alla *privacy* nell'ordinamento giuridico italiano, dalle origini all'era dell'intelligenza artificiale. Il tema della *privacy* rappresenta ormai una delle tematiche più dibattute con conseguenti e incisive modifiche della normativa applicabile, in risposta all'evoluzione del contesto socioculturale di riferimento. Pertanto, il punto di partenza dello studio non possono che essere le origini della tutela della *privacy* nei due sistemi a confronto, per poi analizzare la relativa disciplina normativa attualmente vigente, evidenziandone le similitudini e le differenze nella prospettiva della tutela della persona.

This article analyses the regulatory evolution of the right to privacy in the Italian legal system, from its origins to the era of artificial intelligence. Privacy is now one of the most highly debated issues, with consequent and incisive changes to the applicable legislation in response to the evolution of the socio-cultural context. Therefore, the starting point of the study can only be the origins of privacy protection in the two systems being compared, followed by an analysis of the relevant regulations currently in force, highlighting the similarities and differences from the perspective of personal protection.



Keywords: *Privacy*; Artificial Intelligence; ordinamento giuridico Italiano; ordinamento giuridico peruviano.

Summario: [1. La rilevanza del diritto alla *privacy* in Italia e in Perù.](#) – [2. Gli aspetti socioculturali alla base della regolamentazione della *privacy* nei due ordinamenti giuridici a confronto.](#) – [3. Il contesto normativo italiano sulla protezione dei dati personali.](#) – [4. La tutela dei dati personali nel sistema peruviano.](#) – [5. La necessità di bilanciare la *privacy* con l'innovazione tecnologica.](#) – [5.1. Il diritto fondamentale alla *privacy* e la tutela della persona.](#) – [5.2. Il concetto di vulnerabilità tecnologica nell'era dell'intelligenza artificiale.](#) – [6. Similitudini nella disciplina della *privacy* in due ordinamenti giuridici geograficamente distanti.](#)

1. La rilevanza del diritto alla *privacy* in Italia e in Perù.

Il presente lavoro mira ad evidenziare le origini e l'evoluzione normativa del diritto alla *privacy* negli ordinamenti giuridici di due Stati apparentemente distanti: l'Italia ed il Perù¹.

Il tema della *privacy* ha da sempre ricoperto un ruolo centrale e costituisce ormai una delle tematiche più dibattute dell'era digitale, con conseguenti e incisive modifiche e ripensamenti della normativa di riferimento, in risposta all'evoluzione del contesto sociale e culturale. Di recente, lo sviluppo delle nuove tecnologie - prime tra tutte quelle di intelligenza artificiale (IA) - ha ulteriormente inciso sui profili regolatori della *privacy* ponendo i legislatori di fronte a nuove sfide per garantire una protezione adeguata degli individui anche in relazione a tali nuove tecnologie².

Pertanto, il punto di partenza dell'analisi non può che essere il contesto sociale e culturale nel quale si è sviluppata la tutela della *privacy*, dalle origini al XXI secolo, per poi analizzare la regolamentazione normativa nei due ordinamenti giuridici di riferimento.

¹ La scelta della comparazione tra l'ordinamento giuridico italiano e quello peruviano vuole essere un omaggio al Maestro Cesare Massimo Bianca, i cui studi hanno rappresentato, e costituiscono tutt'oggi, un punto di riferimento non solo per la dottrina italiana, ma anche per quella di molti altri stati, come il Perù. Il legame tra la cultura civilista italiana e peruviana è sempre stato molto forte e caratterizzato dal reciproco rispetto e dalla comune attenzione ai valori fondamentali che stanno alla base dell'esperienza giuridica. La traduzione in spagnolo di alcune delle principali opere del Professore Bianca dimostra come l'attenzione per i suoi studi sia stata tale da incentivare la fruibilità degli stessi anche oltreoceano e testimonia il rapporto culturale tra i due paesi. In tal senso cfr. C.M. BIANCA (con la collaborazione di M.BIANCA), *Instituciones de Derecho Privado*, traduzione di A. SÁNCHEZ RAMÍREZ e con introduzione di J. ESPINOZA ESPINOZA, Perù, 2025; C.M. BIANCA, P. SIRENA, S. PATTI, *Derecho privado moderno*, traduzione di C.A. AGURTO GONZÁLES e S.L. QUEQUEJANA MAMANI, Santiago-Chile, 2015. Tra l'altro l'Università Nazionale Maggiore di San Marcos di Lima – alla quale afferiscono Agurto Gonzáles e Quequejana Mamani - ha conferito la laurea *honoris causa* al Prof. Bianca.

² Per approfondire la relazione di strutturale vulnerabilità tra di essere umano e ambiente digitale, si veda L. GATT, *Essere umano e ambiente digitale come relazione di strutturale vulnerabilità*, in AA.Vv., *Costruire una nuova strategia per un diritto europeo protettivo in ambiente digitale (Building a New Strategy for European Protection Law in a technological environment)*, a cura di L. GATT, M.C. GAETA, Napoli, 2023, 11 – 18; poi approfondito in L. GATT, I.A. CAGGIANO, M.C. GAETA, P. GRIMALDI, A.A. MOLLO, L. AULINO, *Vulnerabilità tecnologica: una prospettiva di diritto privato*, in AA.Vv., *Vulnerabili. Questioni giuridiche, dilemmi bioetici*, a cura di A. PATRONI GRIFFI, Napoli, 2025, 611 – 654. Si veda anche A.A. MOLLO, *La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici*, in EJPLT, 2021, I, 199 - 210.

Infatti, sia l'Italia che il Perù, hanno introdotto normative *ad hoc* per la tutela della *privacy*, ma con approcci diversi. La regolamentazione italiana dipende dalla sua appartenenza all'Unione Europea, mentre in Perù la disciplina si fonda su norme nazionali. Entrambe le discipline, però, sono propriamente incentrate sulla tutela dei dati personali, fattispecie in parte differente rispetto al concetto di *privacy*, ma che può essere in essa ricompresa. In Italia la nozione di *privacy* (riservatezza) ha due accezioni. Secondo la prima accezione per *privacy* si intende il diritto alla non divulgazione dei dati di carattere personale, ormai confluito nel diritto alla protezione dei dati personali, conformemente a quanto previsto dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea. La seconda accezione, invece, si fonda sulla tutela dell'intimità della sfera privata e della vita familiare, c.d. diritto alla *privacy*, ai sensi dell'art. 7 della Carta dei diritti fondamentali dell'Unione Europea³ e dell'art. 8 della Convenzione Europea dei diritti dell'Uomo (CEDU)^{4,5}. Pertanto, la *privacy* in senso stretto è un diritto individuale che tutela il rispetto della sfera personale, mentre con diritto alla protezione dei dati personali concretamente si estende la tutela dell'individuo oltre la sfera della vita privata e familiare a tutte le relazioni sociali, garantendo così il diritto dell'individuo ad autodeterminarsi e al controllo sulla circolazione dei propri dati personali⁶.

Il presente contributo – per esigenze di brevità della trattazione – prende in considerazione la nozione più ampia e moderna di *privacy*, ricomprendendovi al suo interno quella di tutela dei dati personali.

2. Gli aspetti socioculturali alla base della regolamentazione della *privacy* nei due ordinamenti giuridici a confronto.

Gli aspetti sociali e culturali sono significativi nella percezione di una fattispecie giuridica e della relativa evoluzione normativa della stessa; in quest'ottica, anche la disciplina normativa della *privacy* in Italia e in Perù è il risultato delle scelte etiche e politiche riguardo alla *privacy* e alla tutela dei dati personali. Le similitudini e le differenze delle due società di riferimento, e della loro cultura, rispecchiano la diversa gestione e normazione della fattispecie in esame.

Molteplici sono gli aspetti di comunanza tra l'ordinamento giuridico italiano e quello peruviano sul piano della tutela degli individui, sebbene la normativa di riferimento non sempre si basi sugli stessi aspetti socioculturali. Il Codice

³ Carta dei diritti fondamentali dell'Unione Europea (anche nota come Carta di Nizza), proclamata il 7.12.2000 a Nizza e, in una versione adattata, il 12.12.2007 (2000/C 364/01).

⁴ Consiglio d'Europa, Convenzione Europea dei diritti dell'Uomo (CEDU), firmata il 4.11.1950.

⁵ P.M. VECCHI, *Il diritto alla protezione dei dati personali*, in Aa.Vv., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, n.196 («Codice della Privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, Tomo I, Padova, 2007, 3 ss.

⁶ Il Prof. C.M. Bianca è stato tra i pochi esponenti della dottrina italiana a cogliere sin da subito la differenza concettuale tra le due nozioni di riservatezza, evidenziando come l'evoluzione del concetto di *privacy* abbia «portato a identificare la riservatezza nella protezione dei dati personali» distinguendo, però, quest'ultima nozione dalla tradizionale riservatezza quale intimità della vita privata e familiare. Cfr. C.M. BIANCA, *Nota introduttiva*, in Aa.Vv., *La protezione dei dati personali*, a cura di C.M. BIANCA, F.D. BUSNELLI, op. cit., XX, poi ripreso da V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in Aa.Vv., *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 23; V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, 25.

civile peruviano è stato influenzato dalla cultura giuridica italiana sotto diversi profili⁷, che vanno dalla struttura del Codice civile, ai principi generali e ai fondamentali istituti giuridici. Nel corso degli anni, alcune modifiche al codice civile peruviano sono state determinate dalle evoluzioni della dottrina giuridica italiana, riflettendo un continuo scambio culturale tra i due sistemi⁸. Inoltre, si avverte anche un forte ascendente della dottrina giuridica italiana negli studi civilistici peruviani⁹.

Venendo all'oggetto del presente contributo, tra gli aspetti del diritto peruviano nel quale è possibile riscontrare l'influenza dalla cultura giuridica italiana, si annovera proprio quello della *privacy*. Allo stesso tempo, però, non di poco conto sono le differenze tra i due ordinamenti giuridici. In Italia, ad esempio, Paese democratico dove la cultura è fortemente influenzata dalla tradizione europea e occidentale, vi è una maggiore sensibilità nei confronti della protezione della *privacy* e dei dati personali. Ciò si è riflettuto nella maggiore consapevolezza dell'importanza della riservatezza sin dalle sue origini. In Perù, una nazione con diverse sfaccettature sul piano sociale, la percezione della *privacy* è stata influenzata da fattori come la storia coloniale, le lotte alle disuguaglianze socioeconomiche e la maggiore diversità culturale all'interno della popolazione, traducendosi in una varietà di prospettive sulla *privacy*, a seconda delle esperienze e delle concezioni individuali. In entrambi i sistemi però – come si vedrà – la centralità dei diritti dell'individuo ha contribuito allo sviluppo di una cultura in cui la *privacy* è considerata un diritto fondamentale¹⁰.

⁷ Si ritiene che il Codice civile peruviano sia l'opera di codificazione che ha recepito nel modo più ampio le norme del testo omologo italiano. Cfr. L. LEÓN, *I quaranta anni del Codice Civile peruviano. Tra l'influenza italiana e la ricerca della propria identità*, in *Rivista dell'Accademia dei civilisti italiani*, 2024, IV, 350.

⁸ Per approfondire i lineamenti fondamentali dell'ordinamento giuridico peruviano: J. LEON BARANDIARAN, *Curso elemental de derecho civil peruano*, 2ª ed., Lima, 1973; A. CORVETTO VARGAS, *Manual elemental de derecho civil peruano*, Tomo I, Lima, 1945.

⁹ L. LEÓN, *I quaranta anni del Codice Civile peruviano*, op. cit., 349 – 360, evidenzia come la cultura civilistica peruviana abbia come caratteristica la consultazione continua dei testi della dottrina italiana, la quale ha illustrato «le origini, il senso e le funzioni degli istituti regolamentati nel Codice civile italiano del 1942, da Messineo a Santoro-Passarelli, da Barbero a Trabucchi», conosciuti grazie al lavoro di traduzione in spagnolo delle loro opere. Con specifico riferimento a Cesare Massimo Bianca, l'Autore ripercorre le riflessioni di Bianca, formulate quando in Italia si discuteva della riforma legislativa sull'aborto, in quanto, il Codice civile peruviano ripropone l'artificiale differenza tra persona (per il diritto) e soggetto di diritto, dalla quale risulta – secondo una parte della dottrina peruviana – che la legge riconosca al concepito la soggettività giuridica. L'art. 1, co. 2 del Codice civile peruviano sancisce che: «La vita umana inizia con il concepimento. Il concepito è soggetto di diritto per tutto quanto gli sia favorevole. L'attribuzione dei diritti patrimoniali è subordinata a che nasca vivo». Inoltre, León sottolinea che sul rapporto obbligatorio di fondamentale importanza risultano essere le opere di Emilio Betti, Michele Giorgianni, Luigi Mengoni, Cesare M. Bianca (citando, in particolare, C.M. BIANCA, *El interés*, in *Ius et Veritas*, traduzione di F. CRUZ, 1994, IX, 111 - 115), Adolfo Di Majo, Francesco Benatti, Carlo Castronovo, Umberto Breccia, Giovanni D'Amico, Fabrizio Piraino.

¹⁰ T.E. FROSINI, *Liberté, Egalité, Internet*, Napoli, 142, afferma che per il diritto alla *privacy* non sono ammesse situazioni di incertezza: «o è un diritto fondamentale oppure no». Ciò nonostante, essendo un diritto fondamentale – e la collettività vuole che lo sia – occorre tutelarlo come tale. G.F. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in *Osservatorio del diritto civile e commerciale*, 2015, II, 421 - 446, il quale definisce il diritto alla protezione dei dati personali come disomogeneo diritto fondamentale in virtù della nozione tanto ampia di dato personale, nella quale rientrano le categorie più disparate di dati compresa (ma non solo) quella inerente la dignità umana, che sarebbe configurabile come diritto inviolabile e non «meramente» fondamentale, ai sensi dell'art. 1, Carta dei diritti fondamentali dell'Unione europea. Del resto, in Italia, sia la *privacy* che la protezione dei dati personali sono diritti fondamentali dell'individuo ai sensi della Carta di Nizza (artt. 7 - 8).

Le politiche di protezione dei dati personali in Italia e in Perù, pertanto, potrebbero essere il risultato di tali differenze culturali e sociali. In Italia, dove vi è una maggiore attenzione alla *privacy*, la normativa di riferimento appare essere più stringente e orientata alla tutela dei diritti degli individui, anche se non sempre efficace e al passo con lo sviluppo tecnologico. In Perù, invece, potrebbero essere necessari ulteriori sforzi per una maggiore sensibilizzazione sulla *privacy* al fine di garantire un'effettiva tutela dei dati personali.

In definitiva, le differenze socioculturali tra Italia e Perù giocano un ruolo importante nella regolamentazione, interpretazione e applicazione della disciplina sulla protezione dei dati personali e, più in generale, sulla presa di coscienza della *privacy*. Comprendere e tenere conto di tali differenze è fondamentale per l'analisi della regolamentazione giuridica nei due ordinamenti, le quali rispecchiano, appunto, le specificità di ciascun contesto nazionale.

Partendo da qui è possibile valutare come promuovere una tutela della *privacy* degli individui che sia realmente efficace in considerazione dello sviluppo sempre più rapido delle tecnologie di intelligenza artificiale che inevitabilmente aumentano la tipologia e la quantità dei trattamenti dei dati non sempre nel rispetto delle opportune basi giuridiche.

3. Il contesto normativo italiano sulla protezione dei dati personali.

Il contesto normativo italiano in materia di *privacy* è chiaramente influenzato dall'appartenenza dell'Italia all'Unione Europea. Infatti, il processo di integrazione del mercato unico europeo ha raggiunto il suo apice nel 1992 con la stipula del Trattato di Maastricht¹¹, che ha istituito l'Unione Europea e ha esteso le competenze comunitarie includendo due nuove aree strategiche: la Politica esterna e di sicurezza comune (PESC)¹² e la Cooperazione nel campo della Giustizia e degli Affari Interni (GAI)¹³. Contestualmente, è stato istituito il sistema di libera circolazione delle persone e delle merci, rappresentato dall'area Schengen¹⁴. Tuttavia, questa evoluzione ha sollevato problematiche

¹¹ Trattato sull'Unione Europea (TUE), 7.02.1992 (in vigore dal 1.11.1993), che definisce i c.d. tre pilastri dell'Unione europea, stabilendo anche le regole politiche e i parametri economico-sociali necessari per l'ingresso degli Stati membri nella suddetta Unione (noti come parametri di Maastricht).

¹² Nel 2009, il Trattato di Lisbona (Trattato di Lisbona che modifica il trattato sull'Unione Europea e il trattato che istituisce la Comunità europea, 13.12.2007, ed entrato ufficialmente in vigore l'1.12.2009) ha radicalmente riformato l'architettura istituzionale dell'Unione Europea, eliminando la precedente configurazione a pilastri e sopprimendo la distinzione netta tra i diversi ambiti dell'integrazione europea. Nonostante alcune modifiche successive, la PESC continua essenzialmente a operare secondo il metodo intergovernativo, limitando significativamente il ruolo della Commissione Europea e del Parlamento Europeo, ai quali vengono attribuiti poteri relativamente contenuti in tale ambito.

¹³ Oggi è il Consiglio Giustizia e affari interni (GAI), che elabora politiche comuni e di cooperazione su diversi aspetti transfrontalieri al fine di realizzare uno spazio di libertà, sicurezza e giustizia a livello europeo. Per maggiori dettagli si rinvia alla pagina web ufficiale: <https://www.consilium.europa.eu/it/council-eu/configurations/jha/>.

¹⁴ La principale tappa qualificante nella costituzione di un mercato interno volto a garantire la libera circolazione delle persone è rappresentata dalla stipula degli Accordi di Schengen, costituiti dall'accordo di Schengen propriamente detto (sottoscritto il 14.06.1985) e dalla Convenzione di applicazione dell'accordo di Schengen (sottoscritta il 19.06.1990 ed entrata in vigore il 26.03.1995). Tale quadro normativo ha costituito un elemento fondamentale per l'abolizione delle frontiere interne tra gli Stati firmatari, favorendo l'effettiva integrazione e la libera circolazione dei cittadini all'interno dell'area di Schengen.

di natura normativa, in particolare la mancanza di un quadro normativo uniforme a livello europeo sulla protezione dei dati personali. La libera circolazione dei dati, in un contesto di mercato unico, richiede regolamentazioni armonizzate tra gli Stati membri per prevenire fenomeni di distorsione della concorrenza, quali il dumping normativo, e per evitare che le differenze regolamentari ostacolino il flusso transfrontaliero di dati. A tal fine, la Commissione Europea ha adottato la Direttiva 95/46/CE¹⁵, successivamente sostituita dal Regolamento Generale sulla Protezione dei Dati (Reg. 2016/679/UE - GDPR)¹⁶. Pertanto, a livello europeo la prima regolamentazione della *privacy* risale agli anni '90 ed è rappresentata dalla c.d. Direttiva Madre (Direttiva 95/46/CE), la quale ha implicato l'introduzione negli stati membri di una disciplina sul trattamento dei dati personali.

La decisione di adottare una direttiva invece del Regolamento – come poi invece è stato fatto con il GDPR – risponde a motivazioni di carattere strategico e normativo proprie del contesto storico e giuridico dell'epoca. In quegli anni, il settore della protezione dei dati personali si trovava ancora in uno stadio embrionale, con conoscenze e regolamentazioni limitate. La complessità della materia, unitamente alla mancanza di un quadro normativo armonizzato e vincolante a livello europeo, rendeva impraticabile l'adozione di una normativa uniforme e direttamente applicabile in tutti gli Stati membri. Per tale motivo, risultava preferibile l'emanazione di una direttiva, che specificava gli obiettivi di tutela e stabiliva i principi fondamentali, lasciando ai legislatori nazionali il compito di recepire e attuare tali disposizioni nel diritto interno, garantendo in tal modo adeguata flessibilità e rispetto delle differenze giuridiche nazionali.

Sono stati così stabiliti dalla Direttiva del '95 le condizioni generali di liceità del trattamento (capo II), e viene, altresì, espressamente riconosciuta la possibilità per la persona lesa di esperire anche un rimedio giurisdizionale, oltre a quello amministrativo, in caso di violazione dei diritti garantiti dalle disposizioni nazionali applicabili al trattamento dei dati personali (capo III). In Italia la Direttiva Madre è stata recepita con l'adozione della L. n. 675/1996 (c.d. legge sulla *privacy*)¹⁷ – poi abrogata dal codice *privacy* – la quale ha introdotto la prima disciplina organica in Italia sul trattamento dei dati personali. Essa, inoltre, ha istituito la figura dell'Autorità garante per la protezione dei dati

¹⁵ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.

¹⁶ 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*. Per uno studio sistematico del GDPR si vedano: Aa.Vv., *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *op. cit.*; Aa.Vv., *Il codice della privacy: commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, a cura di R. SCIAUDONE e E. CARAVÀ, Pisa, 2019; Aa.Vv., *Privacy digitale. riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di E. TOSI, Milano, 2019; S. GORLA e C. PONTI, *Privacy UE: il vecchio e il nuovo. Confronto tra D.Lgs 196/2003, Codice privacy e Regolamento europeo 2016/679 GDPR*, Milano, 2018; Aa.Vv., *GDPR e normativa privacy: commentario*, a cura di G.M. RICCIO, G. SCORZA e E. BELISARIO, Milano, 2018. Per un approfondimento sul ruolo e sulle funzioni del DPO, figura introdotta dal GDPR, si rinvia a G. BUTTI, M.R. PERUGINI, *GDPR: la privacy nella pratica quotidiana: tutte le domande a cui un DPO deve sapere rispondere*, Milano, 2020; mi sia consentito rinviare anche a M.C. GAETA, *Hard law and soft law on data protection: What a DPO should know to better perform his or her tasks*, in EJPLT, 2019, II, 61 - 78.

¹⁷ Legge 31.12.1996, n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*. Per un'attenta disamina della normativa originaria, prima delle intervenute modifiche cfr. Aa.Vv., *Trattamento dei dati e tutela della persona*, a cura di V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH, Milano, 1999.

personali (nota anche come Garante *privacy*)¹⁸, che è l'organo pubblico indipendente di vigilanza incaricato di garantire il rispetto della normativa *privacy* applicabile in Italia (in particolare Capo VII, L. n. 675/1996). Il Garante *privacy*, ha compiti ben precisi che nel tempo sono aumentati e in parte mutati, ma ha sempre svolto un ruolo fondamentale nella vigilanza sul corretto utilizzo dei dati personali, sulla gestione delle segnalazioni di violazione della *privacy* e nell'imposizione di sanzioni in caso di violazione della normativa sulla tutela dei dati personali, costituendo un organo da adire alternativamente o preventivamente a quello giudiziario nazionale¹⁹.

In aggiunta, è nella legge del '96 che viene disciplinato il consenso al trattamento dei dati personali da parte dell'interessato (art. 11, L. n. 675/1996)²⁰, che allora doveva essere documentato per iscritto e oggi rappresenta una delle principali basi giuridiche del trattamento, se non la principale, seppure ormai con evidenti limiti di efficacia per le difficoltà di garantire che il consenso sia realmente libero, specifico, informato ed inequivocabile²¹, ma non con riguardo a vincoli di forma, attualmente solo limitati alla prova del conferimento.

Infine, l'esplicito collegamento tra l'allora normativa di parte speciale (legge sulla *privacy*) e quella di parte generale (Codice civile) viene introdotto dall'art. 18 della L. n. 675/1996, poi inizialmente mantenuto nell'art. 15 del D.lgs. n. 196/2003 (Codice *privacy*), fino all'entrata in vigore del GDPR, di cui si dirà. In particolare, i menzionati articoli prevedono il diritto al risarcimento del danno derivante dall'illecito trattamento dei dati personali ai sensi dell'art. 2050 del Codice civile italiano qualificandolo quale ipotesi di responsabilità derivante dall'esercizio di attività pericolose (responsabilità aggravata)²².

¹⁸ Maggiori informazioni sull'Autorità garante per la protezione dei dati personali sono disponibili sul suo sito web ufficiale: <https://www.garanteprivacy.it/home>.

¹⁹ Nell'era dell'intelligenza artificiale il ruolo della autorità di protezione dei dati personali si è esteso dovendo ora ricomprendere anche l'esperienza e la competenza nel gestire l'impatto dell'IA sui diritti fondamentali, in particolare sul diritto alla protezione dei dati personali; v. EDPB, Dichiarazione 3/2024 on DPAs role in AI Act framework, 16 luglio 2024.

²⁰ Nello specifico, l'art. 11, co. 3, L. n. 675/1996 sanciva espressamente che: «Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 1».

²¹ Nel 2016, il Centro di Ricerca in Diritto Privato Europeo (ReCEPL), congiuntamente al Living Lab Utopia, entrambi istituiti presso l'Università Suor Orsola Benincasa, ha condotto un esperimento commissionato da Microsoft Italia per misurare la consapevolezza e la comprensione degli utenti in materia di protezione dei dati personali in un contesto digitale e verificare le peculiarità del consenso al trattamento dei dati personali dagli stessi espresso. I risultati dell'esperimento sono stati pubblicati in AA.VV., *Privacy and Consent. A Legal and UX&HMI Approach*, a cura di L. GATT, R. MONTANARI, I.A. CAGGIANO Napoli, 2021. Per un'ulteriore analisi del consenso *privacy* intendo il dato personale quale corrispettivo contrattuale, si vedano: L. GATT, *The contradictions of the privacy law*, in EJPLT, 2020, Special Issue, VIII; V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, 166 - 178; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in Osservatorio del diritto civile e commerciale, 2018, I, 67 - 106.

²² Per un approfondimento sulla responsabilità per esercizio di attività pericolose prima della riforma del GDPR, si veda. C.M. BIANCA, *Diritto civile, V, Responsabilità civile*, 2ª ed., Milano, 2021, 677 - 687. Per un'analisi sull'evoluzione della fattispecie della responsabilità per illecito trattamento dei dati personali alla luce dell'entrata in vigore del GDPR cfr.: L. GATT, *Rapporto possibile tra atipicità dell'illecito ed esimenti della concezione bianchiana della responsabilità quale tutela civile contro l'illecito: il caso del trattamento abusivo di dati personali*, in AA.VV., *La responsabilità. Principi e funzioni. Continuando a dialogare con Cesare Massimo Bianca*, Milano, a cura di M. BIANCA, 2023, 345 - 351; E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale: oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Milano, 2019.

Nel 2003, il legislatore italiano ha emanato l'attuale Codice in materia di protezione dei dati personali (noto anche come Codice *privacy* - D.lgs. n. 196/2003²³) il quale stabilisce più nel dettaglio le regole per la raccolta e la gestione dei dati personali, e impone ai titolari del trattamento il rispetto di dettagliati principi e tutele degli interessati – come il diritto di accesso ai dati personali²⁴ (artt. 7-10 codice *privacy*, abrogati nel 2018 per l'attuazione del GDPR) – nonché determinati obblighi per il trattamento dei dati personali, come quelli informativi²⁵ (art. 13, codice *privacy*, anch'esso abrogato nel 2018). Il Codice *privacy* per realizzare gli obiettivi di riservatezza nell'uso delle informazioni personali ha fatto ricorso al principio di necessità del trattamento dei dati²⁶ (art. 3, codice *privacy*, poi abrogato nel 2018), che impone ai sistemi informativi di ridurre al minimo l'impiego dei dati personali, favorendo l'ipotesi di un utilizzo di dati anonimi.

Contemporaneamente all'adozione del codice *privacy* italiano, però, l'impatto di nuove tecnologie²⁷ anche nel settore delle telecomunicazioni, e sulla scia americana, ha condotto il legislatore europeo ad integrare le disposizioni della Direttiva Madre, introducendo la c.d. *e-Privacy Directive* (Direttiva 58/2002/CE)²⁸ che, appunto, mira a disciplinare la riservatezza delle comunicazioni elettroniche. Continua così la serie di numerosissime modifiche della disciplina italiana sulla *privacy*, poi culminata in quelle dettate dall'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR), recepito in Italia con D.lgs. n.101/2018²⁹, con conseguente abrogazione di intere parti del codice *privacy*, essendo immediatamente applicabile in Italia il regolamento europeo, il GDPR appunto.

Il GDPR nasce dalla consapevolezza che la Direttiva 95/46/CE, sebbene abbia mantenuto ancora oggi validi i suoi obiettivi e principi, non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione. Il passaggio, dunque, dallo strumento della direttiva a

²³ D.Lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*. Tra i commentari al codice *privacy* si evidenzia per completezza, sistematicità e attualità delle riflessioni dopo quasi venti anni dalla pubblicazione: Aa.Vv., *La protezione dei dati personali*, a cura di C.M. BIANCA, F.D. BUSNELLI, *op.cit.*

²⁴ E. BARGELLI, *Diritto di accesso ai dati personali e altri diritti (commento all'art. 7)*, in Aa.Vv., *La protezione dei dati personali*, a cura di C.M. BIANCA, F.D. BUSNELLI, *op. cit.*, 130 - 141.

²⁵ M.G. CUBEDDU, A. NARDONE, S. WINKLER, F. GREBO, A. CES E M. QUARGNOLO, *Informativa (commento all'art. 13)*, in Aa.Vv., *La protezione dei dati personali*, a cura di C.M. BIANCA, F.D. BUSNELLI, *op.cit.*, 294 - 332.

²⁶ G. BUTTARELLI, *Principio di necessità del trattamento dei dati (commento all'art. 3)*, in Aa.Vv., *La protezione dei dati personali*, a cura di C.M. BIANCA, F.D. BUSNELLI, *op. cit.*, 32 - 40.

²⁷ La pervasività delle nuove tecnologie e il loro impatto sulla protezione dei dati personali è particolarmente evidente: P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Il foro napoletano*, 2018, II, 481 ss.; G. ALPA, *Quale modello normativo europeo per l'Intelligenza Artificiale?*, in *Contr. e impr.*, 2021, IV, 1003 - 1026, sottolinea che uno dei tre pilastri del modello di disciplina dell'uso delle tecniche di intelligenza artificiale a livello europeo, è quello della tutela della persona, cui si aggiungono la responsabilità per i danni derivanti dall'uso di queste tecnologie e la tutela del diritto d'autore che sta alla base delle nuove tecnologie. Sulla tutela degli individui e dei propri diritti nell'era dell'IA si veda anche: R. TREZZA, *La tutela della persona umana nell'era dell'Intelligenza Artificiale*, in *Federalismi*, 2022, XVI, 277 - 305.

²⁸ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

²⁹ D.Lgs. 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).

quello del regolamento europeo ha avuto lo scopo di armonizzare la tutela del bene giuridico (i dati personali) sia sotto il profilo preventivo (si pensi, in particolare, ai principi della c.d. *privacy by design* e *privacy by default*) che rimediale (va fatto riferimento sia al sistema sanzionatorio ampliato con i rimedi amministrativi e civili esperibili, con rinvio anche a quelli penali previsti a livello nazionale, che all'inasprimento dell'ammontare delle sanzioni comminate). Da un punto di vista strutturale, invece, il GDPR è fondato sull'approccio "*risk-based*", attualmente molto diffuso nel modello di regolamentazione europeo³⁰.

Come evidenziato, il contesto normativo della *privacy* in Italia è in costante evoluzione per rispondere alle sfide poste dal rapido sviluppo delle tecnologie digitali e dal conseguente aumento delle minacce alla sicurezza informatica, con evidenti risvolti anche sulla *privacy*. Con l'entrata in vigore del GDPR, l'Italia si è allineata alla regolamentazione europea in materia di protezione dei dati personali, garantendo una maggiore coerenza e coesione nel quadro normativo della *privacy*. Aderendo ad un approccio internazionale, poi, l'Italia sta dando sempre più rilievo ai c.d. standards internazionali, norme tecniche che forniscono linee guida e requisiti per garantire la qualità, la sicurezza, l'efficienza e la sostenibilità in vari settori, come lo Standard ISO/IEC 2700 in ambito *privacy* sulla sicurezza delle informazioni³¹. Tuttavia, la strada per garantire un'effettiva tutela degli individui in relazione allo sviluppo tecnologico sembra essere ancora lunga e, probabilmente, senza fine.

4. La tutela dei dati personali nel sistema peruviano.

In Perù la *privacy* è stata inizialmente normata nel Codice civile del 1984. In particolare, nell'ambito del libro I, titolo II, dedicato ai diritti della persona, l'art.

³⁰ Il modello del c.d. *Risk based approach* è stato utilizzato in diversi atti normativi europei tra i quali da ultimo rileva l'Artificial Intelligence Act (Regolamento del Parlamento europeo e del Consiglio 2024/1689/UE, del 13.06.2024, *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti n. 300/2008/CE, 167/2013/UE, 168/2013/UE, 2018/858/UE, 2018/1139/UE e 2019/2144/UE e le direttive 2014/90/UE, 2016/797/UE e 2020/1828/UE* (Regolamento sull'intelligenza artificiale)), che muove nella direzione della tutela degli individui in relazione alle nuove tecnologie applicando nuovamente l'approccio basato sul rischio, sia per la classificazione dell'IA, che per la misurazione e gestione dei rischi stessi. Si tratta di un significativo intervento normativo che costituisce un quadro giuridico di riferimento dell'IA, ma che non è da solo sufficiente a tutelare gli individui da tutti i potenziali rischi delle intelligenze artificiali. Per un approfondimento sulla gestione del rischio (risk management) si rinvia al recente studio di A. BERTOLINI, *Artificial Intelligence and Civil Liability*, studio commissionato dal JURI Committee del Parlamento europeo, PE 776.426, Luglio 2025. L'autore si occupa da tempo delle tematiche connesse alla responsabilità civile per danno da prodotto intelligente. Per uno studio preliminare della riforma della Strategia europea sull'IA e dei successivi interventi di *soft law* e poi anche di *hard law*, v. A. BERTOLINI, *Insurance and risk management for robotic devices: Identifying the problems*, in *Global Jurist*, 2016, XVI, 291 ss.; AA.VV. *Intelligenza artificiale affidabile Risk management e compliance per il governo degli algoritmi*, a cura di P. MANES, Milano, 2025. L'approccio basato sul rischio dell'AI Act riguarda sia l'intero ciclo di vita di un sistema di IA ad alto rischio (ai sensi dell'art 9 AI Act) che la valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio (c.d. FRIA acronimo della traduzione inglese *Fundamental Rights Impact Assessment*, ai sensi dell'art. 27 AI Act). Per un approfondimento sulla FRIA: A. MANTELERO, M.S. ESPOSITO, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer law & security review*, 2021, 41, 1-35; e mi sia consentito rinviare a L. GATT, I.A. CAGGIANO, M.C. GAETA, E. TROISI, R. SAVELLA, F. PRATESI, R. TRASARTI, *FRIA implementation model according to the AI Act*, in *EJPLT*, 2024, II, 192 - 204, DOI: <https://doi.org/10.57230/EJPLT242LGIACMCGETRSRTEP>.

³¹ Standard ISO/IEC 2700 1:2022, certificazione di un sistema di gestione della sicurezza delle informazioni (SGSI).

14 del Codice civile peruviano disciplina la *privacy* come intimità della vita privata e familiare³². Espressamente il menzionato articolo pone il limite del consenso dell'interessato al trattamento per la divulgazione delle informazioni riguardanti la propria sfera personale e, in caso di morte dello stesso, del consenso del coniuge, dei discendenti, degli ascendenti o dei fratelli, esclusivamente in tale ordine. Tale disposto normativo evidenzia la centralità della tutela dei diritti della personalità anche in Perù e, nello specifico, la tutela del diritto alla *privacy* degli individui³³.

Successivamente, considerata la crescente complessità della materia e le esigenze di prevedere una tutela organica del diritto alla *privacy*, analogamente a quanto previsto in Italia, anche in Perù è stata approvata una disciplina normativa di parte speciale sulla tutela dei dati personali: *Ley de Protección de Datos Personales* (Legge n. 29733/2011³⁴) e *Reglamento de la Ley de Protección de Datos Personales* (Decreto Supremo n. 003-2013-JUS del 2013³⁵). Similmente all'ordinamento italiano, anche la regolamentazione peruviana si fonda sulla protezione dei dati personali e la riservatezza delle informazioni sulle persone, stabilendo regole e principi da seguire per il trattamento sicuro e lecito dei dati personali. Nello specifico, la legge sulla protezione dei dati personali disciplina la tutela tale diritto fondamentale, così come previsto dall'art. 2, co. 6, della Costituzione politica del Perù, nel rispetto degli altri diritti fondamentali dalla stessa riconosciuti. La Legge, inoltre, definisce i diritti degli interessati (in Perù denominati *titulares de datos personales*, art. 2, n. 16, L. n. 29733/2011) ed i principi e le condizioni da applicare nel trattamento dei dati personali.

In particolare, la Legge sulla protezione dei dati personali in Perù garantisce il diritto fondamentale alla *privacy* e impone, tra l'altro, l'obbligo dei titolari del trattamento (denominati *Encargados de tratamiento de datos personales*, art. 7, n. 16, Legge n. 29733/2011) di adottare le misure di sicurezza adeguate per proteggere i dati personali dai rischi di accesso e divulgazione non autorizzati, perdita, o distruzione³⁶. Gli interessati hanno il diritto di essere informati sul trattamento dei loro dati (*derecho de información*), di impedire il trasferimento a soggetti terzi (*derecho a impedir el suministro*), di essere tutelati innanzi all'Autorità nazionale per la protezione della *privacy* (*derecho a la tutela*) e di

³² Per un commento dell'art. 14 codice peruviano e, più in generale, al libro primo, si rinvia a C. FERNÁNDEZ SESSAREGO, *Derecho de las personas. Análisis de cada artículo del Libro Primero del Código Civil peruano del 1984*, ed. XIV, Lima, 2022; J. ESPINOZA ESPINOZA J., M. SALAZAR GALLEGOS (a cura di), *Nuevo Comentario al Código Civil Peruano*, Tomo I, *Título Preliminar y Derecho de las Personas*, Lima (Breña), 2021; C. FERNÁNDEZ SESSAREGO, *Consideraciones sistemáticas preliminares para la revisión del Libro. Primero del Código Civil peruano*, Lima, 1964.

³³ Per approfondire la tutela civilistica della persona in Perù si rinvia a: C.A. AGURTO CONZÁLES., *Derecho de las personas*, Lima (Breña), 2023; E. VARSÍ ROSPIGLIOSI, *Tratado de derecho de las personas*, Lima (Breña) 2021; M. MUÑO ROJO, M. TORRES CARRASCO, *Código Civil comentado*, Tomo I, *Título Preliminar, Derechos de las Personas, Actos Jurídicos*, 4ª ed., Lima, 2020; C. FERNÁNDEZ SESSAREGO, *Derecho y personas*, 5ª ed., Buenos Aires, 2015; V. GUEVARA PEZO, *Instituciones del Derecho civil peruano (Visión Histórica)*, Tomo I, *Instituciones del derecho de personas*, Lima, 1996; C. FERNÁNDEZ SESSAREGO, *La noción jurídica de personas*, Lima, 1962; F. LEONCIO OLAZABAL, *Derecho Civil. Nociones generales de derecho, personas, acto jurídicos*, Cuzco, 1961; J. LEON BARANDIARAN, *Comentarios al Código civil peruano (Del título preliminar y del derecho de las personas)*, Tomo IV, Lima, 1952. Con specifico riferimento alla natura giuridica della persona si veda M. RUBIO CORRERA, *El ser humano como persona natural*, Lima, 1992.

³⁴ Ley 3.07.2011 n.29733, *Ley de Protección de Datos Personales*.

³⁵ Decreto Supremo 22.03.2013, n. 003-2013-JU, *Reglamento de la Ley de Protección de Datos Personales*.

³⁶ Defensoría del Pueblo, *Manual de protección de datos personales*, Lima, 2019, 13.

essere indennizzati in caso di danno derivante da illecito trattamento dei dati personali (*derecho a la indemnización*)³⁷.

Il Regolamento della Legge sulla protezione dei dati personali, invece, garantisce il diritto alla protezione dei dati personali, regolandone il trattamento adeguato sia da parte degli enti pubblici che privati. Disciplina, inoltre, il consenso al trattamento, le misure di sicurezza, i diritti degli interessati. Esso prevede l'inserimento dei dati personali nel Registro Nazionale della Protezione dei Dati Personali, l'unità di archiviazione destinata a contenere principalmente le informazioni relative alle banche dati personali di proprietà pubblica o privata allo scopo di rendere pubblica l'iscrizione in tali banche dati, in modo da consentire l'esercizio dei diritti di accesso alle informazioni, rettifica, cancellazione, opposizione e altri diritti previsti dalla Legge e dal Regolamento. Infine, il Regolamento detta un regime sanzionatorio applicabile in caso di mancato rispetto delle norme sulla protezione dei dati personali.

Anche in Perù è stata istituita l'autorità di controllo per la protezione dei dati personali, denominata *Autoridad nacional de protección de datos personales* (ANPDP)³⁸, che ha il compito di vigilare sull'applicazione della normativa *privacy* nel Paese, nonché di rispondere alle segnalazioni di violazione e sanzionare coloro che agiscono in violazione della stessa.

Pertanto, anche nel sistema peruviano la regolamentazione della *privacy* mira a garantire la riservatezza e la sicurezza delle informazioni personali. Per promuovere la fiducia nell'utilizzo dei servizi digitali e nelle nuove tecnologie, appare opportuna un'implementazione efficace della normativa nazionale, parallelamente all'ordinamento giuridico italiano e alla maggior parte degli ordinamenti attualmente impegnati nella regolamentazione dell'intelligenza artificiale.

5. La necessità di bilanciare la *privacy* con l'innovazione tecnologica.

5.1. Il diritto fondamentale alla *privacy* e la tutela della persona.

Così ricostruito il quadro sociale, culturale e normativo della *privacy* nell'ordinamento giuridico italiano e in quello peruviano, appare opportuno evidenziare come la protezione dei dati personali sia considerata un diritto fondamentale dell'individuo e come i due sistemi di riferimento la disciplinino nell'ambito dei rispettivi quadri normativi esistenti nella prospettiva della tutela della persona.

Il legame tra *privacy* e tutela dell'individuo nei contesti italiano e peruviano sottolinea l'importanza della protezione dei dati personali quale elemento essenziale per garantire la tutela di uno tra i più complessi diritti fondamentali dell'individuo. La *privacy* è strettamente legata ai diritti alla dignità, all'autodeterminazione, alla libertà e alla sicurezza personale e, in questa

³⁷ Defensoría del Pueblo, *op. cit.*, Lima, 2019, 20.

³⁸ Per maggiori informazioni sulla Autoridad nacional de protección de datos personales (ANPDP), si invia alla pagina web ufficiale: <https://www.gob.pe/anpdp>.

prospettiva, la protezione dei dati personali assume un ruolo cruciale nel garantire che tali diritti siano preservati e rispettati in favore dell'individuo.

La persona è centrale nelle Carte costituzionali dell'Italia e del Perù. Tuttavia, a differenza del sistema peruviano, che nella propria Carta costituzionale disciplina la *privacy* quale diritto fondamentale (dall'art. 2, co. 6, Cost. Perù)³⁹, a livello costituzionale italiano non è espressamente disciplinato il diritto alla *privacy* in quanto, all'epoca della promulgazione (1947) e dell'entrata in vigore (1948) della Costituzione italiana, non vi era ancora particolare attenzione alla fattispecie giuridica in esame, giunta solo negli anni '60. In generale, però, molteplici sono i riferimenti costituzionali alla riservatezza nella prospettiva della tutela della persona, primo tra tutti l'art. 2 Cost., norma cardine del c.d. principio personalista, che pone l'individuo al centro dell'ordinamento giuridico riconoscendo e garantendo i suoi diritti inviolabili tutelati dalla Repubblica, tanto nella dimensione sociale («formazioni sociali») quanto in quella individuale («come singolo»). Va, altresì, menzionato l'art. 3 Cost. relativo all'uguaglianza formale e all'uguaglianza sostanziale con riferimento al pieno sviluppo della persona umana, nonché l'art. 13 Cost. sull'inviolabilità della libertà personale tutelata da ogni indebita ingerenza nella sfera fisica e psichica; l'art. 14 Cost., poi, che sancisce l'inviolabilità del domicilio, tutelando, così la sede privilegiata della vita privata e familiare, nonché l'art. 15 Cost. sulla libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, protetti quali diritti inviolabili dell'uomo.

Nel contesto italiano, quindi, la *privacy* è riconosciuta essa stessa quale diritto fondamentale dell'individuo, tanto a livello nazionale, quanto sovranazionale, ai sensi dell'art. 12 della Dichiarazione universale dei diritti umani⁴⁰, della Convenzione 108 del Consiglio d'Europa⁴¹ e delle già menzionate Carta di Nizza (artt. 7-8) e CEDU (art. 8)⁴²; essa oggi è disciplinata, in particolare, dal Codice della *privacy* e dal GDPR, i quali riconoscono il diritto alla riservatezza e alla protezione dei dati personali quale diritto dell'individuo. Il rispetto della *privacy* è essenziale per garantire la dignità e l'autonomia degli individui e per prevenire l'abuso e l'uso improprio delle informazioni personali.

Parallelamente in Perù, la Costituzione, sancisce il divieto per i servizi informatici, pubblici o privati, di fornire informazioni che incidano sulla *privacy* personale e familiare degli individui. Inoltre, a livello internazionale la *privacy* è riconosciuta quale diritto fondamentale dalla Dichiarazione universale dei

³⁹ Constitución política del Perú del 1993, all'art. 2 sui diritti fondamentali della persona sancisce che: «*Toda persona tiene derecho: (...) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*»

⁴⁰ Organizzazione delle Nazioni Unite (ONU), Dichiarazione universale dei diritti umani (*Universal Declaration of Human Rights* - UDHR), firmata il 10.12.1948. L'Italia entrò a far parte dell'Assemblea generale delle Nazioni Unite il 14.12.1955.

⁴¹ Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, 28 gennaio 1981, la quale rappresenta il primo trattato internazionale vincolante sulla protezione dei dati personali tra Stati membri del Consiglio d'Europa

⁴² La tutela della *privacy* come diritto fondamentale è centrale nella giurisprudenza europea nel XX e XXI secolo: Corte giustizia Unione Europea, Grande Sez., 30 gennaio 2024, n. 118/22; Corte giustizia Unione Europea, Grande Sez., 21 dicembre 2023, n. 261/22. Con lo sviluppo delle nuove tecnologie, tale diritto fondamentale viene spesso richiamato dalla Corte EDU in relazione ai trattamenti dei dati personali tramite le tecnologie dell'informazione e della comunicazione (TIC), soprattutto in relazione alle c.d. comunicazioni elettroniche. In tal senso: Corte giustizia Unione Europea, Grande Sez., 30 aprile 2024, n. 178/22; Corte giustizia Unione Europea, 30 aprile 2024, n. 470/21.

diritti umani, sottoscritta sia dal Perù che dall'Italia, e dalla Convenzione americana sui diritti dell'uomo⁴³, firmata solo dallo Stato peruviano. In particolare, le Carte internazionali tutelano la privacy attraverso il diritto alla riservatezza della vita personale, familiare, e della propria abitazione (Art. 12 DUDU e art. 11, Convenzione americana), nonché prevedendo il rispetto del proprio onore e il riconoscimento della propria dignità (art. 11, Convenzione americana).

La Legge sulla protezione dei dati personali peruviana riconosce la *privacy* quale diritto fondamentale correlato ai diritti umani, ponendo l'accento sull'importanza di garantire la sicurezza e la riservatezza delle informazioni personali come forma di tutela della libertà e dell'autodeterminazione degli individui.

Pertanto, in entrambi gli ordinamenti giuridici è evidente la stretta correlazione tra il diritto fondamentale alla *privacy* e la tutela dell'individuo e dei propri diritti, attraverso principi chiave come il consenso informato, il principio di necessità nel trattamento dei dati personali, la trasparenza nel trattamento, i limiti al trasferimento a terzi delle informazioni e l'obbligo di adottare misure di sicurezza adeguate per proteggere i dati. In entrambi i Paesi, poi, la protezione dei dati personali non è solo una questione giuridica, ma rappresenta anche un aspetto sociale di estrema rilevanza per garantire il rispetto della dignità umana e la protezione della sfera privata degli individui. L'equilibrio tra la necessità di utilizzare lecitamente i dati personali (anche tramite le tecnologie di IA) e la tutela della *privacy* degli individui costituisce una sfida costante e ormai quotidiana dell'era digitale.

5.2. Il concetto di vulnerabilità tecnologica nell'era dell'intelligenza artificiale.

La necessità di tutelare la privacy dell'individuo è ancora più evidente con lo sviluppo di nuove tecnologie e, in particolare, di quelle IA che evolvono rapidamente⁴⁴, trasformando diversi settori di particolare interesse e rilevanza: dall'ambito del commercio elettronico a quello della sanità, dal settore ludico a quello dell'istruzione. Tuttavia, tale avanzamento tecnologico solleva interrogativi cruciali riguardo la tutela degli individui, i quali, sempre più spesso, risultano essere in una posizione di vulnerabilità rispetto allo sviluppo di tali tecnologie comportando la necessità di individuare in concreto il giusto bilanciamento tra tutela dei diritti dell'uomo e lo sviluppo dell'IA. Si tratta del concetto di potenziale vulnerabilità tecnologica, in cui possono trovarsi gli individui che agiscono in un ambiente tecnologico, a prescindere da altre oggettive situazioni di vulnerabilità (diversamente abili, minori di età, anziani, soggetti in posizione di asimmetria del potere contrattuale o di asimmetria

⁴³ Organizzazione degli Stati Americani, Convenzione americana sui diritti dell'uomo (nota anche come Patto di San José di Costa Rica), firmata il 22.11.1969 ed entrata in vigore il 18.07.1978.

⁴⁴ Lo scorso anno sono state pubblicate le linee guida del Comitato europeo per la protezione dei dati sui trattamenti tramite modelli di IA (EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17 dicembre 2024). Inoltre, U. RUFFOLO, A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo"*, in Giur. It., 2019, VII, 1658 – 1670, a proposito dell'evoluzione delle nuove tecnologie di IA, si soffermano sulla tematica di frontiera della «progressiva tecnologizzazione dell'uomo» in cui la necessità di un'adeguata tutela dell'individuo, che include anche i suoi dati personali, è particolarmente marcata, in ragione proprio della diretta incisività delle tecnologie sull'essere umano.

informativa), per il fatto di essere maggiormente esposti al rischio di danno in ragione di una posizione di debolezza rispetto al rischio di alcune tecnologie (ad esempio, proprio le categorie di IA classificate ad alto rischio nell'AI Act) o alla potenza delle stesse (si pensi al loro utilizzo da parte di alcune delle realtà socioeconomiche, come quelle delle *big tech*)⁴⁵.

Tra le potenziali vulnerabilità rientrano quelle dell'ambito *privacy* inteso estensivamente (non solo illecito trattamento dei dati personali, ma anche lesione della libertà personale, della corrispondenza cartacea ed elettronica, del domicilio fisico e informatico, dell'immagine) in cui l'impatto dell'IA è particolarmente evidente ed è dovuto all'intrinseco trattamento dei dati personali da parte dell'IA, necessario per il funzionamento⁴⁶. Il trattamento dei propri dati personali da parte di un operatore economico, infatti, è stato prima facilitato tramite lo sviluppo dei servizi della società dell'informazione, come i *social network* e i motori di ricerca e, successivamente, dallo sviluppo dei sistemi di intelligenza artificiale costituisce attualmente la controprestazione dell'utente per poter accedere a beni o servizi⁴⁷.

Le applicazioni di IA richiedono spesso il trattamento di grandi quantità di dati (personali e non) per impiego efficace delle stesse e questo solleva preoccupazioni sui diritti degli utenti e sull'uso legale ed etico delle loro informazioni⁴⁸. La questione è di particolar rilevanza in alcuni ambiti di applicazione dell'IA, come i sistemi predittivi (si pensi alla giustizia predittiva⁴⁹

⁴⁵ Gli studi sulla vulnerabilità tecnologica sono da attribuire a L. GATT, *The vulnerability of the human being in a technological environment: the need for protective regulation*, in AA.VV., *Social networks and multimedia habitats, Jean Monnet Chair PROTECH, "European Protection Law of Individuals in Relation to New Technologies"* 1st International Workshop a.y. 2019-2020, Abstract Book a cura di L. GATT, Napoli, 2021. In particolare, l'approfondimento di tali tematiche da parte dell'Autrice, si è sviluppato nell'ambito delle attività della Cattedra Jean Monnet "European Protection Law in Relation to New Technologies" (PROTECH), istituita presso l'Università degli Studi Suor Orsola Benincasa. Il nome proposto per la Cattedra intende evidenziare l'approccio protettivo del diritto europeo nel disciplinare il rapporto tra individui e tecnologie, con specifico riferimento alla vulnerabilità dei primi rispetto alle seconde. I risultati finali del progetto sono stati pubblicati in AA.VV. *Costruire una nuova strategia per un diritto europeo protettivo in ambiente digitale (Building a New Strategy for European Protection Law in a technologies Environment)* a cura di L. GATT, M.C. GAETA, Napoli, 2023.

⁴⁶ V. RICCIUTO, *Intelligenza artificiale e protezione dei dati*, in EJPLT Special Issue 2025, 1- 14, analizza il tema della protezione dei dati personali alla luce del recente e pervasivo fenomeno dell'IA, soffermandosi sul valore economico dei dati per evidenziare come sia nel caso dei beni e servizi basati sull'IA, quanto in generale in quello delle piattaforme digitali, l'attività di raccolta e trattamento dei dati degli utenti costituisce un'attività centrale, nella quale bilanciare, caso per caso, il diritto alla protezione dei dati con la libera circolazione degli stessi.

⁴⁷ Sul valore economico dei dati a partire dallo sviluppo delle piattaforme digitali fino a quello dell'IA: V. RICCIUTO, *Intelligenza artificiale e protezione dei dati*, op. cit., 2-3. Inoltre, G. CERRINA FERONI, *Intelligenza Artificiale e protezione dei dati personali: percorsi di analisi*, in AA.VV., *AI Anthology. Profili giuridici, economici e sociali dell'Intelligenza Artificiale*, a cura di G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA, Bologna, 2022, 26, evidenzia il concetto di dipendenza tecnologica quale «prezzo da pagare» per poter usufruire dei servizi della società dell'informazione. Più segnatamente sul trattamento dei dati personali tramite IA: G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, VII, 1676; R. CINGOLANI, D. ANDRESCIANI, *Robot, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in AA.VV., *Diritto e Intelligenza Artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, a cura di G. ALPA, Pisa, 2020, 23 ss.

⁴⁸ A. MANTELERO, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Berlino-Heidelberg, 2022, 93 - 132 https://doi.org/10.1007/978-94-6265-531-7_1.

⁴⁹ Sui rischi delle tecnologie di IA nel settore giustizia cfr. a L. GATT, I.A. CAGGIANO, M.C. GAETA, E. TROISI, R. SAVELLA, F. PRATESI, R. TRASARTI, *FRIDA implementation model according to the AI Act*, op. cit., 198 - 199; più in generale sulla giustizia predittiva A. PUNZI, Parte I - *Il giudizio umano-algoritmico e i suoi nemici*, in AA.VV. *Diritto dell'intelligenza artificiale*, Vol. 1, op. cit., 175 - 192; U. RUFFOLO, Parte II - *I due volti della giustizia predittiva: decisoria e consultiva*, in AA.VV. *Diritto dell'intelligenza artificiale*, Vol. 1, op. cit., 193 -216.

o ai modelli negoziali automatizzati⁵⁰), quelli di autoapprendimento (es. i sistemi di automazione dei processi tramite IA, come i veicoli autonomi)⁵¹, tecnologie di IA che implicano un trattamento di grandi quantità di dati personali (è il caso delle *smart cities*)⁵². Le tecnologie biometriche⁵³, poi, fanno sorgere interrogativi sulla sorveglianza e sull'uso improprio delle informazioni personali, e le neurotecnologie⁵⁴ comportano il trattamento di dati particolarmente sensibili, come i dati neurali e i dati mentali, dei quali è già molto complessa anche solo la classificazione giuridica. Inoltre, l'utilizzo di internet (dall'*Internet of Things* al metaverso)⁵⁵ aumenta i casi di trattamento di dati personali anche al di fuori dell'UE e nello specifico nell'ambito dei confini planetari della rete Internet, con evidenti conseguenze sul fronte delle tutele della *privacy*, le quali non sono affatto equivalenti nei diversi ordinamenti giuridici, soprattutto in alcuni come degli Stati Uniti d'America.

⁵⁰ Altre questioni relative al trattamento dei dati personali dipendono dalla gestione e condivisione, anche digitale, dei dati personali attraverso strumenti contrattuali, che possono essere anche dotati di un più o meno alto livello di automazione. Sul funzionamento dei modelli negoziali di condivisione dei dati e il relativo trattamento dei dati personali: I.A. CAGGIANO, *Modelli negoziali di condivisione di dati: prospettive applicative e la sostenibilità ambientale*, in AA.VV., *Dalla Data Protection alla Data Governance: il regolamento (UE) 2022/868 Commentario al Data Governance Act*, a cura di A. MORACE PINELLI, Pisa, 2024, 83 - 106.

⁵¹ L'incisività delle nuove tecnologie nella realtà giuridica si evince in particolar modo in alcuni settori come quello dei c.d. veicoli autonomi, ovvero autoveicoli dotati di un'automazione di diverso livello (classificati secondo lo standard internazionale SAE J3016), interconnessi in rete tramite Internet e in grado di dialogare scambiando dati, spesso personali. Per approfondire le questioni della *data protection* connesse all'operatività dei veicoli autonomi v. A.C. NAZZARO, *Privacy e smart mobility*, in AA.VV., *Smart mobility, smart cars e intelligenza artificiale: responsabilità e prospettive*, a cura di D. CERINI e A.P. TEDESCO, 45 - 62; A.C. NAZZARO, *Macchine intelligenti (smart cars): assicurazione e tutela della privacy*, in *Diritto del mercato assicurativo e finanziario*, 2018, I, 1 - 8; mi sia consentito rinviare anche a M.C. GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf. e informatica* 2018, I, 147 - 179.

⁵² Con riguardo al trattamento dei dati personali su larga scala, come nel caso delle *smart cities*, dove i trattamenti dei dati personali spaziano dal settore dei trasporti (si veda A.C. NAZZARO, *Privacy smart cities e smart cars*, in AA.VV., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di E. TOSI, 2019, Milano, 325 - 345) a quello sanitario nel contesto regolatorio non solo del GDPR ma anche dell'EHDS e dell'AI Act (cfr. I.A. CAGGIANO, *Interessi e norme nell'ecosistema europeo dei dati sanitari: la techno-regolazione abilitativa e le sfide per l'efficacia*, in A. MORACE PINELLI (a cura di), *Sanità Digitale Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, vol. I, *Uso dei dati e assetti organizzativi*, Pisa, 19- 23; C. SOLINAS, *Diritto alla salute del paziente e uso primario dei dati sanitari elettronici personali*, in *EJPLT*, Special Issue 2025, 1 - 17; C. DE MENECH, *Intelligenza artificiale in sanità: lo statuto degli obblighi informativi*, in AA.VV. *Diritto dell'intelligenza artificiale*, Vol. 1, 217 - 230).

⁵³ A.C. NAZZARO, *La tutela dei dati biometrici tra GDPR e AI ACT*, in *EJPLT*, 2024, II, 37 - 53, DOI: <https://doi.org/10.57230/EJPLT242ACN>.

⁵⁴ Sulle questioni giuridiche – inclusa la *privacy* – connesse allo sviluppo di tecnologie di BCI si vedano: L. GATT, I.A. CAGGIANO, M.C. GAETA, P. GRIMALDI, A.A. MOLLO, L. AULINO, *Vulnerabilità tecnologica: una prospettiva di diritto privato*, op.cit., 616 - 635; L. GATT, I.A. CAGGIANO, M.C. GAETA, A.A. MOLLO, *BCI Devices and Their Legal Compliance: A Prototype Tool for Its Evaluation and Measurement*, in *EJPLT*, 2022, I, 301-314. DOI : <https://doi.org/10.57230/EJPLT221LGIACMCGAAM>; L. GATT, I.A. CAGGIANO, L. AULINO, E. TROISI, I. IZZO, D.S. D'ALOIA, *BCI Devices and Their Capacity to Express Human Will Having Legal Value: A Model of Risk-Based Classification*, in *EJPLT*, 2022, I, 289-300, DOI: <https://doi.org/10.57230/EJPLT221LGIACLAETLIDSD>.

⁵⁵ Il metaverso è uno spazio digitale condiviso, tridimensionale e persistente, dove le persone, attraverso avatar personalizzati, possono interagire tra loro, vivendo un'esperienza più immersiva rispetto alle connessioni dell'era digitale caratterizzate da Internet. Si tratta di un ambiente digitale che permette interazioni sociali, economiche e, potenzialmente, giuridiche con conseguenti questioni da affrontare sul piano legale, come quelle connesse al trattamento dei dati personali nel metaverso. A tal proposito si rinvia a G. CASSANO, M. IASELLI, G. SPANGHER, *Cybersecurity e sicurezza nazionale nel metaverso*, AA.VV., *Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT*, a cura di G. CASSANO e G. SCORZA, Pisa, 2023, 1 - 54; F. BAVETTA, *Metaverso e protezione dei dati personali*, in AA.VV., *Metaverso*, op. cit., 173 - 196; A.C. NAZZARO, *La natura giuridica del metaverso tra Stato, essential facility e giardino privato*, in AA.VV., *Metaverso*, op. cit., 55 - 64.

Per la tutela della persona e in considerazione dello sviluppo tecnologico gli ordinamenti giuridici italiano e peruviano sono intervenuti con una regolamentazione dell'IA. L'Italia, sempre nell'ottica dell'appartenenza all'Unione europea e sulla scia dell'entrata in vigore dell'AI Act⁵⁶ ha adottato la L. n. 132/2025 di approvazione del D.d.L in materia di IA n. 1146/2024⁵⁷, che disciplina gli spazi normativi rimessi dal Regolamento UE all'autonomia degli Stati membri ed è diventato, così, il primo Paese in Europa ad aver legiferato dopo l'AI Act, in linea con questo, ma con uno sguardo rivolto alle sfide poste dall'IA nel panorama nazionale, sebbene senza prevedere ulteriori obblighi per i soggetti coinvolti (art. 3, co. 5, L. n.132/2025)⁵⁸.

L'Italia è direttamente coinvolta nella politica europea sull'intelligenza artificiale⁵⁹, che si basa sull'innovazione e l'utilizzo dell'IA, garantendo, al tempo stesso, la tutela dei diritti fondamentali degli individui. Infatti, l'UE privilegia un'IA che sia rispettosa dei diritti umani, inclusiva e sostenibile, promuovendo anche la cooperazione internazionale e l'adozione di norme comuni. Parte di tale approccio è la strategia europea sull'IA del 2018⁶⁰, la quale si concentra su quattro obiettivi principali: sviluppare un ecosistema favorevole all'IA, preparare i cittadini e le imprese, garantire un uso etico e affidabile dell'IA, rafforzare la governance e la normativa europea in materia. Tali obiettivi si sono poi concretizzati nell'approccio europeo all'eccellenza e alla fiducia del 2020⁶¹, che prevede azioni concrete e regolamentazioni adeguate. Da ultimo, per rafforzare le precedenti iniziative, è stato adottato il piano d'azione sull'IA nel 2025⁶², che mira a rendere l'Europa un *leader* mondiale in

⁵⁶ Tra i primi commenti all'AI Act: AA.Vv., *Intelligenza artificiale commentario. Regolamento (UE) 2024/1689 - AI ACT, Linee guida Commissione europea pratiche vietate, Disegno di legge sull'intelligenza artificiale*, a cura di A. MANTELERO, G. RESTA, G.M. RICCIO, Milano, 2025. Per un'analisi più approfondita sulle questioni di regolazione in una prospettiva interdisciplinare: L. GATT, M.T. LO CONTE, M.E. MAZZARELLA, *L'ambito di applicazione, soggettivo e oggettivo, dell'AI Act*, in AA.Vv. *Diritto dell'intelligenza artificiale*, Vol. 1, *Responsabilità. Contratto. Regolazione. Veicoli autonomi*, a cura di RUFFOLO e A. AMIDEI, Roma, 2025, 49- 89. Sugli obiettivi perseguiti dal legislatore UE con l'AI Act: G. FINOCCHIARO, *I molteplici obiettivi perseguiti dal regolamento, 2024*, 101 - 111; si veda anche R. RUOPPO, *Il regolamento UE in materia di Intelligenza Artificiale, (c.d. AI Act): un quadro normativo uniforme per la tutela dei diritti fondamentali*, in *Rass. dir. civ.*, 2024, III, 995 ss.

⁵⁷ Il D.d.L. n. 1146/2024, *Disposizioni e delega al Governo in materia di Intelligenza artificiale*, è stato approvato il 20.03.2025 al Senato e alla Camera con modifiche il 25.06.2025, poi definitivamente approvato al Senato il 17.09.2025 e pubblicato in Gazzetta Ufficiale il 23.09.2025 come L. 23.09.2025, n. 132, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*.

⁵⁸ Recita testualmente l'art. 3, co. 5, L. n.132/2025: «La presente legge non produce nuovi obblighi rispetto a quelli previsti dal regolamento (UE) 2024/1689 per i sistemi di intelligenza artificiale e per i modelli di intelligenza artificiale per finalità generali.

⁵⁹ Per un approfondimento si rinvia alla pagina ufficiale della Commissione europea sull'Approccio europeo all'intelligenza artificiale: <https://digital-strategy.ec.europa.eu/it/policies/european-approach-artificial-intelligence>.

⁶⁰ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L'intelligenza artificiale per l'Europa*, 25.4.2018 COM(2018) 237 final.

⁶¹ Commissione europea, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 19 febbraio 2020.

⁶² Comunicazione della Commissione al Parlamento europeo, al Consiglio, alla Commissione europea, al Comitato economico e sociale europeo e al Comitato delle regioni, *AI Continent Action Plan*, 9.4.2025 COM(2025) 165 final. Un primo commento sulla comunicazione in cui viene evidenziata la politica della sovranità digitale dell'UE è offerto da D. IMBRUGLIA, *La futura politica europea di sovranità digitale annunciata dalla Commissione europea nella comunicazione The AI Continent Action Plan del 9 aprile 2025 e nel documento An International Digital Strategy for the European Union del 5 giugno 2025*, in *Persona e mercato*, 2025, 2, 614 – 617.

ambito IA, almeno in prospettiva regolatoria e non direttamente di sviluppo tecnologico.

Nel contesto dell'IA, l'AI Act opera come normativa di riferimento per la disciplina dei sistemi di IA che, trattando dati personali, richiedono la congiunta applicazione al GDPR, sebbene con non poche difficoltà di allineamento. Si pensi ai trattamenti automatizzati dei dati personali tramite IA che devono essere necessariamente conformi all'art. 22 GDPR, tra le cui tre basi giuridiche che derogano al divieto generale di trattamento automatizzato, vi è quella del consenso. La difficoltà principale a tal proposito risiede nella eccessiva difficoltà di fare in modo che il consenso dell'interessato sia realmente informato quando il trattamento è effettuato tramite *software* di IA di cui spesso si ignora il funzionamento, almeno in parte, e non se ne comprende realmente l'impatto sui dati personali⁶³. L'individuazione dei c.d. ruoli *privacy*, poi, e, in particolare, del Titolare e del Responsabile del trattamento, desta non poche incertezze quando si tratta di dispositivi intelligenti, ponendosi, da un lato, coloro che sostengono la tesi della responsabilità del produttore e dei soggetti allo stesso collegati⁶⁴ e, dall'altra, coloro i quali avanzano la proposta della soggettività giuridica (personalità elettronica) del sistema di IA⁶⁵.

Il Perù, al contempo, è intervenuto con una regolamentazione dell'IA nel 2023 (ley n. 31814/2023)⁶⁶, che ha lo scopo di promuovere l'uso dell'IA nell'ambito del processo nazionale di trasformazione digitale, tutelando gli individui e garantendo il rispetto dei loro diritti, al fine di favorire lo sviluppo economico e sociale del Paese, in un ambiente sicuro che garantisca un uso "etico, sostenibile, trasparente, replicabile e responsabile" (art. 1, ley n. 31814/2023).

Il futuro dell'intelligenza artificiale non può che essere guidato da un equilibrio tra innovazione e tutela dei diritti umani, con particolare attenzione ai diritti fondamentali dell'uomo come, appunto, la *privacy*, individuando caso per caso il possibile bilanciamento tra interessi contrapposti. Un'adeguata regolamentazione, accurate sperimentazioni e la collaborazione degli *stakeholders* (istituzioni e altri enti pubblici e privati coinvolti), sono fondamentali per garantire che i progressi tecnologici non compromettano irrimediabilmente i diritti fondamentali. Solo così sarà possibile sfruttare appieno il potenziale dell'IA, promuovendo allo stesso tempo un ambiente di fiducia e sicurezza.

⁶³ AA.Vv., *Privacy and Consent. A Legal and UX&HMI Approach*, op. cit.

⁶⁴ Sin dai primi contributi in materia (A. BERTOLINI, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in *Law Innovation and Technology*, 2013, Vol. 5, fasc. II, 214-247) e giungendo ai più recenti (A. BERTOLINI, *Intelligenza artificiale e responsabilità civile. Problema, sistema, funzioni*, Bologna, 2024, 215 -) Bertolini è chiaro e lineare nel sostenere la tesi della responsabilità del produttore del sistema di IA incorporato o non incorporato in un robot, pur individuandone gli attuali limiti da superare. L'Autore riconosce, altresì, la funzionalità di alcune tesi sulla soggettività giuridica – nella forma della personalità elettronica – dell'IA (127 - 149).

⁶⁵ La visione prospettica di Lucilla Gatt sulla soggettività dell'IA, è decisamente pionieristica e non si può che ravvisarne le opportunità, sebbene riscontrabili nel medio-lungo periodo: L. GATT, *Legal anthropocentrism between nature and technology: the new vulnerability of human beings*, in *European Journal of Privacy Law & Technologies*, 2022, I, 15-26, DOI: <https://doi.org/10.57230/EJPLT221LG>.

⁶⁶ Ley 5.07.2023, n. 31814, *que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*.

6. Similitudini nella disciplina della *privacy* in due ordinamenti giuridici geograficamente distanti.

L'analisi comparata sull'evoluzione normativa del diritto alla *privacy* in Italia e Perù, nel contesto dell'era dell'Intelligenza Artificiale (IA), evidenzia una sorprendente vicinanza giuridica tra i due ordinamenti, nonostante la loro distanza geografica e le differenze socioculturali.

Le differenze, sebbene marginali, permangono e derivano in parte dal diverso sistema regolatorio e in parte da fattori socioculturali, come la storicamente maggiore sensibilità alla *privacy* riscontrata in Italia. Di fatto, pur condividendo l'obiettivo generale di tutelare la *privacy*, la regolamentazione italiana e quella peruviana appaiono differire in parte nei dettagli specifici delle disposizioni normative, nei ruoli e nel sistema sanzionatorio previsto in caso di violazioni. Per di più, le differenze sociali e culturali tra i due Paesi hanno inciso, in generale, sul loro sistema regolatorio e, in particolare, anche sulla *privacy*, comportando differenze sul piano dell'efficacia della normativa di riferimento e della consapevolezza del diritto alla riservatezza tra le due popolazioni. Nello specifico, l'Italia, essendo uno stato membro dell'Unione Europea, deve attenersi al GDPR e, in generale, al quadro regolatorio eurounitario che riguarda anche la *privacy*, implicando una maggiore coerenza normativa a livello sovranazionale rispetto al Perù, il quale, invece, parrebbe avere un quadro giuridico di riferimento più specificamente calato nella realtà nazionale (legge sulla protezione dei dati personali e relativo regolamento, oltre ad una norma del codice civile (art. 14), che sancisce il principio generale della *privacy*).

Ciononostante, risultano essere di gran lunga prevalenti le similitudini tra i due sistemi, le quali ne evidenziano, appunto, la vicinanza.

Entrambi i sistemi giuridici hanno riconosciuto la centralità della *privacy* come diritto fondamentale dell'individuo, ponendo le basi per un quadro normativo incentrato sulla protezione dei dati personali e sulla tutela della persona, rispondendo anche all'esigenza di regolare tale fenomeno nella realtà dell'era dell'IA.

In Italia, la disciplina dei dati personali è intrinsecamente legata al modello multilivello europeo, fondandosi sul Codice della *Privacy* e sul GDPR, il quale conferisce maggiore coerenza al quadro sovranazionale. Il Perù, d'altro canto, si affida a una normativa nazionale (*Ley de Protección de Datos Personales*), arricchita da un esplicito riferimento alla *privacy* sia a livello costituzionale che nel Codice civile peruviano. Entrambi gli ordinamenti giuridici, poi, sono calati nel contesto internazionale di riferimento. Inoltre, le similitudini si estendono ai meccanismi di controllo, con l'istituzione in entrambi gli Stati di un'autorità indipendente di vigilanza (l'Autorità garante per la protezione dei dati personali, in Italia, e l'*Autoridad nacional de protección de datos personales*, in Perù.) e si concretizzano nella condivisione di principi cardine come la trasparenza, l'adozione di misure di sicurezza adeguate e, soprattutto, il requisito del consenso informato.

La vera frontiera per entrambi gli ordinamenti è rappresentata dalla loro attenzione all'IA, anche con riguardo alla sua intrinseca necessità di dati (personali) per operare, che espone l'individuo ad una nuova forma di vulnerabilità, quella tecnologica. A tal riguardo, è significativo che entrambi i sistemi giuridici abbiano risposto con una legislazione specifica: l'Italia con la L.

132/2025, allineata all'AI Act europeo, e il Perù con la Ley n. 31814/2023 per un uso etico e responsabile dell'IA. Ecco perché in entrambi i sistemi giuridici il futuro della *privacy* è indissolubilmente legato alla capacità di bilanciare l'innovazione tecnologica con la tutela dei diritti umani. Superare le complessità applicative legate all'IA - come assicurare un consenso realmente informato in sistemi di cui si ignora in parte il funzionamento e definire con certezza i ruoli di responsabilità nel trattamento dei dati - richiede uno sforzo continuo in termini di regolamentazione, sperimentazione e collaborazione tra tutti gli stakeholders.

In conclusione, entrambi i Paesi hanno una normativa incentrata sulla prospettiva antropocentrica della tutela della persona⁶⁷, mentre le inevitabili differenze tra i due sistemi restano marginali e sullo sfondo. L'obiettivo ultimo, che accomuna i due sistemi, è chiaro: tutelare l'essere umano, garantendo che il progresso non comprometta irrimediabilmente i diritti fondamentali dell'individuo.

⁶⁷ P. PERLINGIERI, *Presentazione*, in AA.Vv., *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, a cura di P. PERLINGIERI E S. GIOVA, Napoli, 2020, VII ss., il quale sottolinea come sia ineludibile la diffusione di una cultura antropocentrica e solidale che consenta il monitoraggio dei risultati prodotti, verificandone la compatibilità con la scelta personalistica del costituzionalismo europeo, proprio per la tutela della persona e con il fine ultimo di arginare il pericolo di schiacciamento dell'essere umano da parte del progresso tecnologico ad oggi in grado di incidere direttamente negli schemi regolatori (tecnoregolazione).