"PRIVACY" E INTELLIGENZA ARTIFICIALE: SISTEMI DI IA CHE TRATTANO CATEGORIE PARTICOLARI DI DATI, TRA CONTROLLO E TUTELA DELLA PERSONA

Francesca Mollo*

SOMMARIO: 1.- Introduzione; 2.- Il trattamento di categorie particolari di dati nel Regolamento UE 1689/2024 quale strumento volto a promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile; 3.- Il bilanciamento tra controllo e tutela della persona nel circuito europeo di tutela della "privacy" in punto al trattamento di categorie particolari di dati; 4.- Conclusioni.

1.- **Introduzione.**

Le tecnologie «creano e forgiano la nostra realtà fisica e intellettuale, modificano la nostra autocomprensione, cambiano il modo in cui si relazioniamo con gli altri e con noi stessi, aggiornano la nostra interpretazione del mondo, e fanno tutto ciò in maniera pervasiva, profonda e incessante»[1], in quello spazio denominato infosfera in cui nuovi attori, padroni dell'intelligenza artificiale «muovendosi disinvoltamente tra politica ed economia, forgiano le nuove fondamenta del nostro mondo»[2]. L'odierna società dell'informazione si atteggia così sempre più spesso a società della sorveglianza[3] e del controllo, da un lato, e società del rischio[4], che tutto conosce del cittadino, anch'esso globale, immerso nella sua solitudine[5] nel contesto di una vera e propria «sorveglianza liquida»[6], orientata sempre più in senso predittivo[7].

In questa «società dell'accesso»[8] la persona è sempre più digitalizzata, profilata e trasparente; delineandosi così una società dell'integrale trasparenza che rievoca la metafora dell'uomo di vetro[9], e che legittima la pretesa di altri di richiedere e ottenere ogni informazione e che implica la classificazione (*id est*, la divisione in classi) come sospetto, cattivo cittadino, nemico dello Stato di chiunque rivendichi di mantenere spazi di intimità[10].

Le interferenze tra l'evolversi incessante della tecnologia e la "privacy" sono ineludibili: il valore attribuito delle informazioni cresce esponenzialmente per i grandi attori economici e politici a livello globale[11] che di tale tecnologia dispongono, mentre pare pericolosamente decrescere in misura

* Ricercatrice in *Tenure Track* (RTT) di Diritto privato, *Alma mater Sudiorum* - Università di Bologna.

[1] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017, 47.

[2] M.R. Ferrarese, *Poteri nuovi. Privati, penetranti, opachi*, Bologna 2022.

[3] Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari 2004, 174s.

[4] U. Beck, *La società del rischio. Verso una seconda modernità*, Roma 2004, 63ss.

[5] Z. Bauman, *La solitudine del cittadino globale*, Milano 2003, 24; M. Foucault, *Sécurité, territoire, population*, Paris 2004; Id., *Sorvegliare e punire. Nascita della prigione*, Torino 1976. Cfr., altresì, S. Rodotà, *Libertà personale. Vecchi e nuovi nemici*, in M. Bovero (cur.), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma-Bari 2004, 54.

[6] Bauman, D. Lyon, *La sorveglianza nella modernità liquida*, Roma-Bari 2015.

[7] Cfr. Garante per la protezione dei dati personali, provvedimento del 24 novembre 2016 n. 488, doc. web n. 5796783.

[8] J. Rifkin, *L'era dell'accesso*, Milano 2001, 17ss.

[9] Per un'analisi della figura dell'«uomo di vetro» in relazione ai totalitarismi e al rispetto della vita privata si veda S. Niger, *Le nuove dimensioni della privacy*, Padova 2006, 33ss.

[10] Rodotà, *Tecnopolitica* cit. 175. Nello stesso senso, Id., *La vita e le regole. Tra diritto e non diritto*, Milano 2006, 104.

[11] A. Joinson, K. Mckenna, T. Postmes, U.-D. Reips (curr.), *Oxford Handbook of Internet Psychology*, Oxford-New York 2007.

pressoché proporzionale per i titolari di dette informazioni[12], che nella c.d. «dittatura dell'algoritmo»[13], costituiscono una traccia della persona, frammenti della stessa che ne rivelano caratteristiche e peculiarità, anche attinenti alla vita privata.

In questo contesto si colloca recente Regolamento UE 2024/1689 del 13 giugno 2024 ("IA Act")[14] che stabilisce regole armonizzate sull'intelligenza artificiale.

Come si legge nel recente Rapporto Draghi di settembre 2024[15], «con il mondo che si trova sull'orlo di una rivoluzione AI, l'Europa non può permettersi di rimanere bloccata nelle "tecnologie e industrie di mezzo" del secolo precedente»[16]. Si segnala anche che il 5 settembre 2024 la Commissione europea ha firmato la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale[17], il primo accordo internazionale giuridicamente vincolante sull'IA, in linea con l'"IA Act", che prevede un approccio comune per garantire che i sistemi di IA siano compatibili con i diritti umani, la democrazia e lo Stato di diritto.

D'altra parte, come precisato pure nel recente "report" *Europol Ai And Policing The Benefits And Challenges Of Artificial Intelligence For Law Enforcement*, l'intelligenza artificiale è destinata a «offrire strumenti senza precedenti per migliorare la capacità di salvaguardare la sicurezza pubblica» anche a livello europeo, «profoundly reshap[ing] the law enforcement landscape».

2.- **Il trattamento di categorie particolari di dati nel Regolamento UE 1689/2024 quale strumento volto a promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile.**

In prima battuta, è bene ricordare che il Regolamento in tema di intelligenza artificiale pone tra i propri obiettivi, esplicitati all'art. 1, quello di «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione»[18].

In proposito, si ripropone il bilanciamento tra benessere e mercato, che rievoca quella che è stata definita «doppia anima»[19] già del Reg. UE 679/2016 in tema di protezione dei dati personali (GDPR), e in cui resta latente la dialettica tra persona e mercato[20], che ha nel tempo segnato il passaggio

[12] Cfr. R. D'orazio, *Protezione dei dati by default e by design*, in S. Sica, V. D'Antonio, G.M. Riccio (curr.), *La nuova disciplina europea della privacy*, Milano 2016, 88.
[13] Rodotà, *Il mondo della rete*, Roma-Bari 2014, 37.
[14] Regolamento UE 1689/2024 del 13 giugno 2024, PECONS 24/1/24 REV 1. Tra i primi commenti A. Gentili, *Regole per l'intelligenza artificiale*, in *Contratto e impresa* 4 (2024) 1043ss.
[15] "Report" *Il futuro della competitività Europea*, settembre 2024.
[16] *Ivi*, 17.
[17] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Vilnius 5 settembre 2024.
[18] Cfr. anche considerando 1 e considerando 176.
[19] La suggestiva espressione è in N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. Zorzi Galgano (cur.), *Persona e mercato dei dati*, Milano 2019, 35ss.
[20] Sul rapporto tra persona e mercato, con particolare riferimento all'ordinamento italiano anche in relazione al processo di integrazione europea, cfr. L. Mengoni, *Persona e iniziativa economica privata nella Costituzione*, in G. Vettori (cur.), *Persona e mercato. Lezioni*, Padova 1996, 34ss.; N. Lipari, *Persona e mercato*, in *Riv. trim. dir. proc. civ.* (2010) 766.

«dall'Europa dei mercati all'Europa dei diritti»[21], in cui i diritti sono stati via via sempre più «presi sul serio»[22] dalla giurisprudenza, divenuto poi «solido cemento edificato»[23] su cui poggia la stessa Carta dei diritti fondamentali, proprio valorizzando quella centralità della persona, divenuta la cifra del processo di integrazione europea[24].

In tema giova anche richiamare il documento *Orientamenti etici per un'IA affidabile*, ivi già definita come «inclusiva» e «antropocentrica», con un approccio poi confermato fin dal considerando 1 del Regolamento (oltre che dall'art. 1 stesso, come detto), diretto a porre le persone al centro dello sviluppo dell'IA, presentato come il grande vantaggio dell'Unione europea rispetto agli altri attori internazionali nella competizione globale. Tale documento già esplicitava i principi sui quali si fonda un'IA "reliable": rispetto dell'autonomia umana, prevenzione dei danni, equità, esplicabilità, oltre che sicurezza e trasparenza.

Sotto il profilo delle intersezioni con il tema della protezione dei dati personali, va detto che il Regolamento si colloca nell'ambito di un preciso quadro normativo europeo, che prende le mosse dalla c.d. Strategia europea sui dati 2030, varata dalla Commissione europea nel 2020[25] con l'intento di realizzare un unico sistema normativo applicabile in tutta Europa, atto a disciplinare l'economia dei dati, nonché a prevenire rischi e abusi derivanti dalla posizione dominante delle grandi piattaforme "online".

In generale, il Regolamento si ispira al c.d. "risk-based approach"[26] per classificare i principali sistemi di IA secondo una struttura piramidale a rischio crescente fondata su quattro distinti livelli di rischio determinati dall'uso di un dato sistema: rischio inaccettabile; rischio alto; rischio basso o minimo e rischio specifico per la trasparenza, introducendo restrizioni ed obblighi graduati a seconda del tasso di rischio che una determinata applicazione può presentare.

Nel quadro di tali premesse, un aspetto peculiare e che presenta aspetti di criticità è (e sarà) sicuramente rappresentato dal trattamento delle categorie personali di dati *ex* art. 9 GDPR. Ed in particolare, dei dati biometrici, cui il nuovo regolamento dedica ampio spazio.

Sul punto, va qui subito detto che l'"IA Act" fornisce sì una definizione di dati biometrici all'articolo 3 n. 34 quali «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici», che va interpretata – così esplicita già il considerando 14 – «alla luce dei dati biometrici di cui all'art. 4, punto 14, GDPR»[27], laddove il n. 37 dello stesso art. 4, quanto alle categorie particolari di dati, rinvia alla nozione contenuta nell'art. 9 GDPR. Lo stesso GDPR all'art. 4, par. 1, n. 4, definisce i dati biometrici come i «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che

[21] Sul punto, si veda G. Alpa, M. Andenas, *L'Europa dei diritti e i diritti fondamentali*, in Idd., *Fondamenti del diritto privato europeo*, Milano 2005, 53ss.
[22] Il riferimento è al volume di R. Dworkin, *I diritti presi sul serio*, Bologna 2010.
[23] R. Cosio, R. Foglia (curr.), *Il diritto europeo nel dialogo delle Corti*, Milano 2013, 116.
[24] Cfr. Rifkin, *Il sogno europeo. Come l'Europa ha creato una nuova visione del futuro che sta lentamente eclissando il sogno americano*, Milano 2004, 283; N. Bobbio, *L'età dei diritti, introduzione*, Torino 1990. Cfr. L. Ferrajoli, *L'itinerario di Norberto Bobbio: dalla teoria generale del diritto alla teoria della democrazia*, in L. Bonanate (cur.), *Teoria politica democrazia. Dal passato al futuro*, Milano 2011.
[25] Commissione europea, *Una strategia europea per i dati*, COM (2020)66, 19 febbraio 2020.
[26] Cfr. G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.* (2022) 303ss.
[27] Oltre che all'art. 3, punto 18, del regolamento UE 2018/172 e dell'art. 3, punto 13, della direttiva UE 2016/680.

ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

Essi, nell'impianto sistematico disegnato dal GDPR, rientrano in quella categoria particolare di dati cui il Regolamento pone una specifica attenzione, vietando o limitandone il trattamento, tranne che in alcune particolari situazioni, indicate dall'art. 9, par. 2, solo se tramite il loro trattamento si può giungere all'identificazione univoca o all'autenticazione di una persona fisica[28]. Il GDPR per tali dati, che consentono o confermano l'identificazione univoca dell'individuo, crea cioè una sotto-categoria all'interno della più ampia categoria dei dati particolari disciplinati dall'art. 9, per i quali la liceità del trattamento è ancorata al requisito alternativo del consenso esplicito oppure della necessità, consentendo agli Stati membri di introdurre garanzie supplementari (art. 9, par. 4)[29].

Sempre tra le definizioni dell'"IA Act", al n. 35 dello stesso art. 3 è poi contenuta quella di «identificazione biometrica», quale «il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati»[30], con esclusione dei sistemi di IA destinati a essere utilizzati per la verifica biometrica con la sola finalità di confermare l'identità di una persona fisica (autenticazione)[31], nonché di «categorizzazione biometrica» quale sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive (art. 3, n. 40). In punto a quest'ultimo, in particolare, l'art. 5, par. 1, lett. g) prevede il divieto di immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale.

Infine, fornisce una definizione di «sistema di riconoscimento delle emozioni» quale sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici (art. 3, n. 39)[32]. Sul punto, attese le manifestate preoccupazioni delle Istituzioni europee[33] in relazione alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare sotto il profilo della loro «limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità», si vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in alcuni contesti sensibili, quali situazioni relative al luogo di lavoro e all'istruzione», per i possibili effetti discriminatori o comunque invasivi dei diritti e delle libertà delle persone interessate (art. 5, par. 1, lett. f).

Attenzione particolare viene posta ai sistemi di identificazione biometrica remota, in ragione del loro potenziale significativo impatto sui diritti fondamentali in ragione del dato quantitativo – sotto il profilo dell'elevato numero di persone i cui dati biometrici possono essere trattati – e, d'altro lato,

[28] In tema di riconoscimento facciale, cfr. considerando 51 GDPR.
[29] Cfr. Garante, Provvedimento 22 febbraio 2018, recante Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679.
[30] Ad esempio, il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti.
[31] Considerando 15.
[32] Cfr. considerando 18.
[33] Cfr. considerando 44.

dell'assenza di un coinvolgimento attivo degli interessati[34]. In particolare, i sistemi di identificazione biometrica remota in spazi accessibili al pubblico, in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione (art. 3, n. 42).

I sistemi di identificazione biometrica remota *a posteriori*, invece, in ragione della loro «natura invasiva»[35], devono sempre essere utilizzati in modo proporzionato, legittimo e strettamente necessario e quindi mirato, per quanto riguarda le persone da identificare, il luogo e l'ambito temporale e sulla base di un "set" di dati chiuso di filmati acquisiti legalmente. In ogni caso, essi «non dovrebbero essere utilizzati nel quadro delle attività di contrasto per condurre una sorveglianza indiscriminata» (il tema della sorveglianza è ricorrente nella giurisprudenza multilivello, come si vedrà *infra*).

A monte, il Regolamento classifica come «ad alto rischio», diversi casi di uso critico di sistemi biometrici[36], proprio «perché i dati biometrici costituiscono una categoria particolare di dati personali»[37], nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale. Allo stesso modo, sono così classificati i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti a norma dell'art. 9, par. 1, del GDPR sulla base di dati biometrici, e i sistemi di riconoscimento delle emozioni che non sono vietati a norma del regolamento stesso.

Nel Regolamento si precisa, altresì, che esso non dovrebbe essere in alcun modo inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali, salvo quando diversamente disposto in modo specifico dallo stesso[38]. Precisa altresì il Regolamento, infatti, che l'art. 5, par. 1, lett. h) («uso di sistemi di identificazione biometrica remota in tempo reale») lascia impregiudicato l'art. 9 del GDPR per quanto riguarda il trattamento dei dati biometrici a fini diversi dall'attività di contrasto.

Ancora, nel quadro degli obblighi generali incombenti sul titolare del trattamento *ex* art. 24, e delle misure di sicurezza adottabili *ex* art. 32 del GDPR – letti in un'ottica di responsabilizzazione (o *accountability*) dello stesso – il livello di misure dovrà essere in questo caso molto elevato, trattandosi di trattamento che riguarda dati personali «particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali»[39].

---

[34] Che il criterio selettivo sia proprio l'impatto sui diritti fondamentali delle persone fisiche si ricava anche dal considerando 17, laddove si escludono i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali, adducendo esplicitamente a giustificazione di tale esclusione il fatto che «detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone senza il loro coinvolgimento attivo».

[35] Cfr. considerando 95.

[36] Cfr. art. 27.

[37] Considerando 54.

[38] Considerando 63.

[39] Cfr. considerando 51 reg. UE 2016/679.

In tale contesto, assumono centrale rilevanza e maggiore complessità, in particolare, i profili di tutela dei diritti e delle libertà degli interessati sotto il profilo del trattamento di dati su larga scala di categorie di dati personali, tra cui i dati biometrici. Ad essi si riferisce la previsione che rende obbligatoria la valutazione d'impatto[40] sulla protezione dei dati contenuta nella lett. *b)* dell'art. 35 del GDPR, con formulazione peraltro speculare rispetto a quella adottata dalla dir. UE 2016/680[(41)], e ulteriormente specificata dal provvedimento adottato dal Garante per la protezione dei dati nell'ottobre 2018[42]. In particolare, per i profili che qui rilevano, le categorie più problematiche di trattamento previste dal provvedimento del Garante, oggetto peraltro di puntuali osservazioni da parte dell'European Data Protection Board, erano proprio quelle relative al trattamento effettuato attraverso l'uso di tecnologie innovative, al trattamento dei dati biometrici, in relazione ai quali nella versione originaria dell'elenco il Garante italiano aveva mostrato di considerare suscettibili *ex se* di presentare rischi elevati per i diritti e le libertà degli interessati.

3.- **Il bilanciamento tra controllo e tutela della persona nel circuito europeo di tutela della "privacy" in punto al trattamento di categorie particolari di dati.**

Per inquadrare la questione delle intersezioni tra la nuova disciplina europea dell'IA e il trattamento di categorie particolari di dati può essere utile prendere in considerazione gli orientamenti della giurisprudenza della Corte di Strasburgo in tema[43], da leggersi secondo i criteri della "case law" inglese[44], per cui la protezione dei dati personali riveste un ruolo quasi del tutto strumentale alla tutela del diritto al rispetto della vita privata[45] di cui all'art. 8 CEDU.

In tema di trattamento di categorie particolari dati, un "leading case" in materia è la sentenza Marper c. Regno unito del 2008, avente ad oggetto la c.d. "privacy" genetica, nella creazione di banche dati genetiche e del DNA a fini di giustizia. La Corte, in questo caso, afferma che la conservazione delle impronte digitali e dei campioni biologici di DNA, a prescindere dall'effettivo utilizzo degli stessi da parte delle autorità, rappresenta un'ingerenza nella vita privata dei soggetti, attesa la sicura qualificazione delle impronte e dei campioni di DNA alla stregua di dati sensibili nella nozione

[40] Sulla valutazione di impatto si veda R. Torino, *La valutazione d'impatto*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (curr.), *I dati personali nel diritto europeo*, Torino 2019, 855ss.

[41] Cfr. art. 27 della dir. UE 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, laddove prevede che sia necessaria una valutazione d'impatto sulla vita privata «quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

[42] Cfr. Garante della protezione dei dati personali, doc. web n. 9058979 dell'11 ottobre 2018, contenente l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del reg UE n. 2016/679, pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018. Si vedano anche le osservazioni rese in proposito: EDPB, *Opinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, adottata il 25 settembre 2018 e notificato il 2 ottobre 2018, disponibile al sito *web https://edpb.europa.eu/*.

[43] In tema si veda Blasi, *La protezione dei dati personali nella giurisprudenza della Corte Europea dei diritti dell'uomo*, in *Riv. intern. dir. uomo* (1992) 543.

[44] G. Zagrebelsky, *La giurisprudenza casistica della Corte europea dei diritti dell'uomo. Fatto e diritto alla luce dei precedenti*, in Alpa (cur.), *L'essenza della democrazia. I diritti umani e il ruolo dell'avvocatura*, Roma 2010, 205ss.

[45] Cfr. O. Pollicino, M. Bassini, *Art. 8. Protezione dei dati di carattere personale*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (curr.), *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 137.

contenuta dalla Convenzione del 1981[46]. E proprio su queste premesse la Corte poi sottolinea come la giustificazione prevista dall'art. 8, comma 2, della CEDU debba essere ancorata, per porsi in termini di necessarietà della misura per una società democratica, a regole chiare, dettagliate, oltre che a garanzie minime, che nel caso concreto il Regno Unito non assicurava affatto, dal momento che non venivano previste regole minime e neppure criteri di cancellazione o distruzione dei dati genetici. La Corte, anzi, in uno dei passaggi più interessanti della sentenza[47] si dice addirittura «sorpresa» dal carattere generale e indifferenziato con cui in Inghilterra opera il meccanismo di conservazione di tali dati, laddove invece uno Stato che intendesse porsi in un'ottica pionieristica dal punto di vista dell'evoluzione tecnologica nel campo, dovrebbe prendersi anche in carico la responsabilità di compiere dei bilanciamenti[48], che nel caso concreto non sono stati compiuti affatto, con tutti i conseguenti rischi, anche in termini di stigmatizzazione sociale[49].

Il tema del controllo sui dati rappresenta, più in generale, un tema molto affrontato dalla giurisprudenza di Strasburgo sotto il profilo delle interferenze con il diritto al rispetto della vita privata di cui all'art. 8 CEDU. Si ripropone, quindi, quella preoccupazione che l'utilizzo di particolari categorie di dati «possono condurre ad una sorveglianza indiscriminata», nella formulazione del nuovo Regolamento in tema di intelligenza artificiale, con particolare riferimento ai sistemi di identificazione biometrica remota (su cui *supra*, par. 2).

Così, fin dalla storica sentenza Leander c. Finlandia del 1987, in un caso di raccolta e memorizzazione di dati in un registro segreto di polizia, in cui però ancora non si fa alcun riferimento alla protezione dei dati personali, limitandosi la Corte a vagliare se tale memorizzazione costituisca un'ingerenza giustificabile alla luce del comma 2 dell'art. 8, e concludendo per un'assenza di violazione in tal senso. A poco più di un decennio di distanza, invece, nella sentenza Rotaru c. Romania, la Corte in un caso analogo, muta orientamento, assumendo a referente esterno di valutazione inerente la protezione dati personali (come accadrà poi in altre pronunce successive) la Convenzione n. 108 del 1981, sottolineando la rispondenza di un'interpretazione estensiva della nozione di vita privata e quella elaborata dalla Convenzione del 1981, il cui scopo è garantire il rispetto della vita privata con riferimento ai trattamenti automatizzati[50].

L'ingerenza viene qui ritenuta non giustificabile dalla Corte alla luce del carattere generalizzato, indistinto e sistematico con cui le autorità trattano i dati *de quibus*, nell'assoluta assenza di criteri oggettivi di selezione e individuazione delle informazioni e dei soggetti, nonché di procedure e di meccanismi di controllo di tali operazioni, tali da implicare concretamente «il rischio di minare, persino distruggere, la democrazia per difenderla», creando di fatto un sistema di sorveglianza su base indiscriminata e generalizzata.

In tema, va registrata, peraltro, una vera e propria inversione di tendenza nell'atteggiamento della stessa corte EDU. Nel 2010, infatti, nel caso Kennedy c. Regno Unito, la Corte, pronunciandosi sulla compatibilità con l'art. 8 CEDU di alcuni sistemi di captazione delle informazioni su base generalizzata e sistemica implementati dal Regno Unito, aveva rigettato la questione in assenza di

[46] Sul punto la Corte assimila tali dati alle fotografie e alla registrazione dei campioni vocali, richiamando il caso Friedl c. Austria (19/05/1994) e il caso PG e JH c. Regno Unito n. 44787 del 1998

[47] Par. 119 della sentenza.

[48] Par. 112 della sentenza.

[49] Cfr. anche B.B. c. Francia, n. 5335/06, 17/12/2009, M.M. c. Regno Unito, n. 24029/07, 13/11/2012.

[50] Cfr. anche la sentenza della Corte EDU, 16/02/2000, n. 27798/95, Amann c. Svizzera.

allegazione da parte del ricorrente di una violazione specifica, assumendo e mantenendo quella prospettiva di "individual justice" che da sempre l'aveva contraddistinta. Ma nel 2015, nel caso Zakharov c. Russia[51], tale interpretazione subisce una vera e propria battuta d'arresto, nella misura in cui viene riconosciuto che la mancata allegazione di un pregiudizio o una conseguenza ricollegata al sistema di sorveglianza non costituisce un ostacolo per concludere sulla incompatibilità con l'art. 8 CEDU del sistema russo di captazione delle comunicazioni su base generalizzata e non ancorato a criteri oggettivi né a procedure di controllo specifiche.

Impostazione poi mantenuta nelle successive sentenze della Corte di Strasburgo in tema. Ci si riferisce qui, anzitutto, alla sentenza del 5/03/2020, resa nel caso ARM/Hambardzumyan (ric. 43478/11), nonché, più di recente, con sentenza 8/03/2021, nel caso MDA/Bostan (ric. 52507/09), in relazione ad una perquisizione condotta dalla polizia presso l'abitazione del ricorrente nell'ambito di un procedimento per contravvenzione nei confronti di una terza persona, senza mandato o permesso giudiziario, contrariamente al diritto interno. E ancora, nella più recente e celebre sentenza del 25 maggio 2021 resa nel caso UK/Big Brother Watch and Others (ric. 58170/13), in tema di intercettazione di massa e ottenimento di dati sulle comunicazioni da fornitori di servizi di comunicazione nel Regno Unito prima del 2018, nonché nel caso SWE/Centrum for Rättvisa (ric. 35252/08), con sentenza del 25/05/2021, in cui il controllo oltrepassava il margine di discrezionalità lasciato allo Stato convenuto al riguardo e, nel complesso, non metteva in guardia dal rischio di arbitrarietà e abusi[52].

La questione del trattamento di dati particolari come suscettibile di creare nuovi modelli di sorveglianza è stata, poi, a più riprese al centro dell'attenzione anche delle Istituzioni europee, in ragione del potenziale significativo impatto sui diritti fondamentali.

L'European Data Protection Board, da ultimo nel 2023 nelle linee guida in tema di uso di tecnologia di riconoscimento facciale[53], atteso che l'applicazione delle normative aventi ad oggetto il trattamento di dati biometrici è suscettibile di per sé di incidere su molti diritti fondamentali, ha fornito una lettura alla luce della Carta dei diritti fondamentali dell'Unione europea. L'applicazione delle normative aventi ad oggetto il trattamento di dati biometrici è suscettibile di per sé di incidere su molti diritti fondamentali, per cui la Carta dei diritti fondamentali dell'Unione europea è essenziale per l'interpretazione di dette normative, venendo in rilievo in particolare il diritto alla protezione dei dati di carattere personale di cui all'art. 8 della Carta di Nizza, ma anche il diritto al rispetto della vita privata di cui all'art. 7 della Carta.

In particolare, l'EDPB sottolinea a più riprese che se i dati vengono trattati sistematicamente all'insaputa degli interessati, è probabile che si generi un senso generale di sorveglianza costante, che può comportare effetti inibitori per quanto concerne alcuni i diritti fondamentali interessati, come la dignità umana *ex* art. 1 della Carta, la libertà di pensiero, di coscienza e di religione *ex* art. 10, la libertà di espressione *ex* art. 11 e la libertà di riunione e di associazione *ex* art. 12.

Il trattamento di categorie particolari di dati, quali ad esempio i dati biometrici, si può considerare «strettamente necessario» solo se l'ingerenza nella protezione dei dati personali e le sue limitazioni

[51] Corte EDU, 4/12/2015, Roman Zakharov c. Russia, n. 47143/06.

[52] Cfr. "Report" settembre 2022, *Personal data protection, Thematic factsheet, Department for the Execution of Judgments of the European Court*, consultabile al "link" https://www.coe.int/en/web/execution.

[53] *Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, adottate il 26 aprile 2023, consultabili sul sito "web" istituzionale dell'EDPB.

non eccedono la misura assolutamente necessaria, escludendo qualsiasi trattamento di carattere generale o sistematico.
E con riferimento all'utilizzo di database di riconoscimento facciale e in generale tecnologia basata su intelligenza artificiale da parte delle autorità di contrasto e dei servizi di "intelligence", il Parlamento europeo aveva già a suo tempo espresso profonda preoccupazione nella risoluzione del 6 ottobre 2021[54].
In estrema sintesi, questi i punti che emergevano nella stessa: in primo luogo, l'invito alla Commissione ad «interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa indiscriminata nei luoghi pubblici» (punto 31); in secondo luogo il rilievo dei profili di criticità del trattamento di dati genetici e DNA (punto 29); nonché una presa di posizione netta a favore del divieto di qualsiasi sistema di scoring su larga scala di cittadini, sulla considerazione che «qualsiasi forma di "citizen scoring" normativo sul larga scala da parte delle autorità pubbliche (…) conduce alla perdita di autonomia, indebolisce il principio di non discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana».
Sulla base di queste premesse e preso atto dei diversi tipi di utilizzo di riconoscimento facciale a fini di sorveglianza, il Parlamento chiedeva il divieto permanente dell'utilizzo dei sistemi di analisi o riconoscimento automatico degli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali; nonché una moratoria sulla diffusione di sistemi di riconoscimento facciale per le attività di contrasto con funzioni di identificazione.
Una lettura, quindi, che esprimeva già forte preoccupazione per la deriva che alcuni meccanismi, più o meno velatamente, di sorveglianza di massa, rischiano di prendere nell'odierna società informazionale e digitale.

4.- **Conclusioni.**

«Il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti»[55], utilizzando alcuni dati, specie quelli appartenenti alle categorie particolari, quale «surplus comportamentale privato», sottoposto a processi governati dall'intelligenza artificiale per essere trasformato in prodotti predittivi, destinati poi ad essere scambiati su un nuovo tipo di mercato per le previsioni comportamentali, definito quale «mercato dei comportamenti futuri».
Nella sopra richiamata dialettica tra persona e mercato, la libera circolazione dei dati rappresenta uno dei due interessi in gioco da bilanciare.
D'altra parte, pure nel Rapporto sulla competitività europea del settembre scorso (vedi *supra*, par. 1), si evidenziano le problematiche che sorgono dall'intersezione delle discipline in tema di IA e "privacy", sottolineando come esse possano porsi quale freno per l'innovazione, soprattutto per le

[54] Risoluzione del parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale il suo utilizzo da parte delle autorità di polizia giudiziaria in ambito penale (2020/2016 (INI).
[55] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, II ed., Roma 2023.

piccole e medie imprese occorrendo invece «un equilibrio tra regolamentazione e innovazione, per non soffocare le PMI, cuore dell'economia europea»[56].
L'attenzione tributata alla tutela dei diritti fondamentali deve però rimanere massima.
Una visione della protezione dei dati personali, quale «precondizione per il pieno godimento di altri diritti fondamentali»[57], nonché «espressione particolarmente forte – quasi metonimica – della dignità personale, meta-valore riassuntivo dell'impianto assiologico sui cui si innestano le situazioni giuridiche costituzionalmente protette»[58] impone, dunque, un approccio "data driven", non solo in funzione del miglioramento di diagnosi e cura nel quadro dell'impiego dei dati biometrici, ma proprio come approccio di processo che restituisca centralità alla persona, la cui identità viene in gioco sotto vari profili[59], adottando una prospettiva che faccia leva sul bilanciamento[60] tra i principi che di volta in volta vengano in conflitto[61], da condursi secondo ragione[62], avendo sempre come punto di riferimento la dignità della persona[63].

Abstract.- Il contributo esamina le intersezioni tra "privacy" e intelligenza artificiale, sotto il profilo del trattamento di categorie particolari di dati, attraverso l'analisi, nella cornice del nuovo Regolamento UE 1689/2024, del bilanciamento tra controllo e tutela della persona nel circuito europeo di tutela della "privacy".

The paper examines the intersections between privacy and Artificial Intelligence, from the point of view of the processing of special categories of data, through the analysis, within the framework of the new EU Regulation 1689/2024, of the balance between control and protection of the individual in the European circuit of privacy protection.

[56] Cfr. anche *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, pubblicato dall'European Parliament Research Service (EPRS).
[57] Cfr. Alpa, *Diritto privato europeo*, Milano 2016, 182; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano 1997.
[58] N. Lipari, *Diritto civile e ragione*, Milano 2019, 183ss.
[59] Cfr. Finocchiaro, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.* 4 (2022) 1085ss.; Ead., L. Balestra, M. Timoteo (curr.), *Major Legal Trends in the Digital Economy*, Bologna 2022.
[60] Si vedano le sempre attuali riflessioni sulla prudenza nel bilanciamento di Zagrebelsky, *Il diritto mite*, Torino 1992, 200.
[61] A. Morrone, voce *Bilanciamento (giustizia costituzionale)*, in *Enc. dir.*, Annali, vol. II, t. II, Milano 2008, 185-204.
[62] Cfr. P. Gianniti (cur.), *I diritti fondamentali nell'unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, Bologna 2013, 223, in cui cita in proposito F. Galgano, *Democrazia politica e legge della ragione*, in *Contr. impr.* (2007) 393ss., nonché Id., *Globalizzazione dell'economia e universalità del diritto*, in *Pol. dir*. (2009) 177ss.
[63] Cfr. anche R. Pardolesi, in nota a Trib. Milano, 28/09/2016, in *Foro it.* (2016) 3594.