

Le linee guida in materia di Intelligenza Artificiale: alla ricerca di un'“etica by design” nel nuovo scenario digitale

di Daniela MESSINA*

SOMMARIO: **1.** La tutela dei diritti fondamentali nel nuovo scenario digitale. **2.** Attività di profilazione e processo decisionale automatizzato nel Regolamento (UE) 2016/679. **3.** Le *Ethics Guidelines for Trustworthy AI*. **4.** Le linee guida in materia di Intelligenza Artificiale alla luce del Regolamento (EU) 2016/679. **5.** Conclusioni.

ABSTRACT: *In the search for an adequate balance between the protection of fundamental rights and the evolution of new technologies, particular attention must today be given to the use of Artificial Intelligence, whose diffusion, in the absence of appropriate rules, is potentially capable of limiting the exercise of the freedoms traditionally recognized as a fundamental pillar of every democratic society. To this end, in the context of the broader regulation of profiling activities and automated decision-making processes, the European Commission adopted in April 2019 the Ethics Guidelines for Trustworthy AI on the basis of the belief that the development of such technologies must necessarily be realized in a reliable and ethically sustainable way. Starting from the analysis of the aforementioned Guidelines structured around a principle of "ethics by design", the work aims to assess the role of these rules within the articulate legislative framework outlined by the European legislator in the field of protection of personal data with the Regulation (EU) 679/2016 and what could be the further possible regulatory implications.*

1. La tutela dei diritti fondamentali nel nuovo scenario digitale.

L'evoluzione tecnologica, come è noto, ruota attualmente intorno a tre innovazioni fondamentali - analisi dei *big data*, *Internet of things* (IOT) ed utilizzo dell'intelligenza artificiale (IA) - il cui combinato agire sta profondamente modificando la fisionomia delle moderne società digitali. Si tratta di una trasformazione di straordinarie dimensioni che abbraccia tutti gli

* Professore a contratto di diritto dell'informazione e dell'informatica presso l'Università degli Studi di Napoli "Parthenope".

aspetti della vita di un comune individuo: dalle modalità di acquisto e di consumo dei beni, all'interazione con la pubblica amministrazione, passando per le attività lavorative e l'utilizzo dei servizi pubblici.

In particolare, con il termine IOT si suole indicare la capacità di alcuni oggetti di uso comune di connettersi ad Internet e di scambiarsi vicendevolmente dati ed informazioni per offrire agli individui esperienze di consumo e di utilizzo sempre più avanzate e personalizzate. Si fa riferimento, ad esempio, agli impianti di domotica che consentono di controllare via web in remoto gli elettrodomestici che sono presenti in casa, ovvero ai dispositivi indossabili, come gli *smartwatch* che consentono di aggregare, monitorare e di inviare a terzi informazioni sullo stato di salute dell'utente¹. L'utilizzo di tali tecnologie è in crescente aumento anche all'interno delle città dove l'impiego di oggetti connessi consente la diffusione di servizi sempre più efficienti ai cittadini, garantendo al contempo l'impiego ottimale delle risorse a disposizione e la riduzione del relativo impatto ambientale soprattutto nelle grandi metropoli².

L'intelligenza artificiale, invece, attiene ad una ulteriore fase evolutiva nel più ampio panorama di implementazione delle nuove tecnologie e di sfruttamento delle potenzialità offerte dalla Rete. Come indicato dalla Commissione Europea, con tale termine, infatti, si fa riferimento «a sistemi progettati dall'uomo che, dato un obiettivo complesso, agiscono nel mondo fisico o digitale percependo

¹ Per un'analisi della portata rivoluzionaria dell'*Internet of things* si rinvia, fra gli altri, allo studio realizzato dalla Commissione Europea tramite la DG Communications Networks, Content & Technology nell'ambito dell'«Agenda Digitale», una delle sette iniziative principali individuate nella più ampia Strategia EU2020, che punta alla crescita inclusiva, sostenibile ed intelligente entro l'anno 2020. COMMISSIONE EUROPEA, *DG Communications Networks, Content & Technology, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, Final Report, 2013. L'analisi ha evidenziato che l'impiego di tale tecnologia garantirà una crescita economica di oltre 20 miliardi di euro all'interno dell'Unione Europea entro l'anno 2020 e rappresenta uno dei pilastri della creazione del mercato unico digitale europeo (c.d. *Digital single market*).

² Sulla nascita delle nuove realtà urbane basate sull'utilizzo delle tecnologie dell'informazione e della comunicazione cfr. G. OLIVIERI – V. FALCE, *Smart cities e diritto dell'innovazione*, in «Collana di Quaderni di giurisprudenza commerciale», Giuffrè, 2016. Rileva sottolineare che il progetto a livello sovranazionale della realizzazione di *smart cities* all'interno del panorama europeo ha trovato la sua più compiuta realizzazione con la creazione del partenariato «Città e comunità intelligenti» (CCI) - *Smart Cities and Communities* (EIP-SCC) che mira a stimolare la crescita tecnologica nei settori in cui «la produzione, la distribuzione e l'uso dell'energia, la mobilità e i trasporti e le tecnologie di informazione e comunicazione (TIC) sono strettamente legati e possono offrire nuove opportunità interdisciplinari di migliorare i servizi, riducendo il consumo di energia e risorse e le emissioni di gas a effetto serra e di altre sostanze inquinanti». Sul punto v. COM (2012) 4701, Comunicazione della Commissione Europea, Città e Comunità Intelligenti Partenariato Europeo di innovazione, 2012.

l'ambiente di riferimento, interpretando i dati raccolti in maniera strutturata e non strutturata, ragionando sulla conoscenza derivata da tali dati e decidendo le azioni migliori da intraprendere per raggiungere l'obiettivo prefissato»³.

In altri termini, le tecnologie basate sull'intelligenza artificiale mirano a riprodurre la logica sottesa al comportamento umano, basata su principi di razionalità, efficienza ed analisi critica delle informazioni acquisite nel corso del tempo, al fine di produrre servizi che siano ottimali per gli utenti. È questo quello che succede quando un sito web propone ai propri clienti una serie di prodotti che potrebbero piacere sulla base delle precedenti decisioni di acquisto ovvero quando una piattaforma audiovisiva "suggerisce" un film o una serie televisiva alla luce delle preferenze espresse dallo spettatore – spesso inconsapevolmente - con le precedenti visioni.

Il "collante" tra le due suddette innovazioni è, infine, rappresentato dai *big data*. Come è noto, con tale termine si fa riferimento «a grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti» la cui gestione avviene attraverso l'utilizzo di potenti processori, software ed algoritmi⁴. In un panorama sempre più digitalizzato, infatti, l'elemento chiave non è più rappresentato, come avveniva in un recente passato, dal singolo dato raccolto, bensì dalla correlazione tra molteplici *dataset* e dalla capacità di estrarre da essi valore aggiunto attraverso la previsione di comportamenti ovvero decisioni future⁵. A tal fine, l'utilizzo ottimale dell'intelligenza artificiale

³ HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics Guidelines for Trustworthy AI*, p.36. Sull'analisi di tali linee guida ci si soffermerà, in maniera più specifica, successivamente.

⁴ Questa è la definizione data dalla COMMISSIONE EUROPEA nella Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e Al Comitato delle Regioni dal titolo *Verso una florida economia basata sui dati* COM/2014/0442.

⁵ Sul significato dei *big data* e sul relativo impatto sulla tutela dei dati personali cfr. da ultimo CONSIGLIO D'EUROPA, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasburgo, 2017. Sul relativo ruolo all'interno delle moderne società digitali cfr. COM (2014) 442, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Verso una florida economia basata sui dati*, 2014; S. RUBINSTEIN IRA, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 2013, Vol. 3, No. 2; B. VAN DER SLOOT- S.VAN SCHENDEL, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study in Jipitec, Journal of Intellectual Property, Information Technology and E-Commerce Law*, n.7 (2)/2016. A testimonianza della trasversalità delle problematiche connesse all'utilizzo dei *big data*, in data 30 maggio 2017 è stata avviata un'indagine conoscitiva congiunta che coinvolge l'Autorità Garante della Concorrenza e del Mercato (AGCM), il Garante per la protezione dei dati personali e l'Autorità per le Garanzie nelle Comunicazioni (AGCOM). Lo studio, ancora in corso, è finalizzato all'individuazione di eventuali criticità concorrenziali connesse ai *big data* e alla definizione di un quadro di regole atto a promuovere e tutelare la concorrenza dei mercati della economia digitale, consentendo al contempo una più efficace

diviene cruciale in tale peculiare panorama, in quanto la gestione di enormi e diverse quantità di informazioni impone capacità di analisi che superano quelle naturalmente presenti in un essere umano. I dati, pertanto, "oltrepassano" gli individui e «vengono inseriti in modelli algoritmici alla ricerca di correlazioni ancora ignote che si possano convertire in profitti»⁶.

Città sempre più "smart", servizi personalizzati e soluzioni efficaci ed ottimali ai grandi problemi delle moderne società, come il repentino cambiamento climatico, il progresso nelle cure mediche e la tutela dagli attacchi informatici, sono una evidente espressione del combinato agire dei suddetti tre elementi. Tuttavia, dietro tale straordinario ed accattivante panorama si celano delle significative criticità che impongono una profonda riflessione, soprattutto con riferimento alla tutela dei diritti fondamentali, dei valori e dei principi che rappresentano i pilastri del vivere democratico.

La diffusione di piattaforme connesse e di intese attività di profilazione, nonché l'implementazione dell'IA e di processi decisionali automatizzati, rischia, infatti, di limitare drasticamente l'esercizio di diritti ritenuti da sempre essenziali per il libero dispiegarsi delle società democratiche, quali la libertà di espressione, il pluralismo dell'informazione, l'uguaglianza nelle possibilità di partecipazione alla vita sociale, il libero determinarsi della identità personale.

La sorprendente capacità di tali strumenti di prevedere ed anticipare comportamenti con un'accuratezza senza precedenti rischia, infatti, non solo di accentuare situazioni di discriminazione sociale già esistenti, ma di incardinare gli individui all'interno di una specifica categoria, limitandone le possibili alternative di scelta e le opportunità di crescita ed eventualmente di cambiamento. Offrire prodotti e servizi "su misura" perché basati sulle precedenti decisioni di acquisto, anticipare i comportamenti ovvero limitare l'accesso alle sole informazioni di carattere culturale, economico, sociale, politico che sulla base di una precedente attività di profilazione risultano essere maggiormente in linea con la personalità e le ideologie di un individuo equivalgono a porlo all'interno di una "filter bubble"⁷, una vera e propria bolla,

realizzazione dei compiti istituzionali di ciascuna Autorità. Il provvedimento è consultabile al link http://www.agcm.it/component/joomdoc/allegatinews/IC53_avvio%20ind.%20con.pdf/download.html

⁶ Così V. MAYER-SCHÖNBERGER - K. N. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, p. 129.

⁷ Sul significato di "filter bubble" e sulle possibili conseguenze nelle attuali società digitali, cfr., *inter alia*, M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in *MediaLaws – Rivista dir. media*, 2, 2019, in corso di pubblicazione; V. MAYER-SCHÖNBERGER - K. N. CUKIER, *Big*

sicuramente rassicurante per il soggetto, ma estremamente limitante per l'evoluzione della persona, sia come individuo, sia come cittadino. In antitesi con la necessaria diffusione plurale delle informazioni e delle idee considerata essenza stessa di un sistema democratico, nonché della piena e libera evoluzione dell'identità dei singoli costituzionalmente tutelata, il diffondersi di tecnologie basate sull'IA, se non correttamente regolamentato, rischia, pertanto, di sacrificare il fondamentale valore del pluralismo in nome dell'efficienza produttiva, minando la crescita sostenibile delle moderne società digitali⁸.

Ne consegue che, in un panorama dominato da tecnologie connesse e dall'invisibile trama che collega enormi quantità di dati personali, diviene prioritaria la ricerca di un adeguato bilanciamento tra la tutela dei diritti fondamentali sanciti nelle carte costituzionali e proclamati dai trattati europei a livello sovranazionale ed il valore economico delle informazioni, al fine di garantire che il progresso delle moderne società sia pur sempre realizzato in un'ottica democratica.

2. Attività di profilazione e processo decisionale automatizzato nel Regolamento (UE) 2016/679.

Le criticità emergenti dall'uso sempre più intenso di tecnologie connesse e della diffusione di forme sempre più sofisticate di intelligenza artificiale ha spinto il legislatore europeo a delineare una disciplina peculiare in materia nell'ambito del nuovo Regolamento destinato alla protezione dei dati

Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà, op.cit.

⁸ Sul punto si permetta di indicare D. MESSINA, *Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent*, in *MediaLaws – Rivista dir. media*, 2, 2019, in corso di pubblicazione; M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018; M. R. ALLEGRI - G. D'IPPOLITO (a cura di), *Accesso a internet e neutralità della rete, tra principi costituzionali e regole europee*, Roma, 2017; S. WACHTER, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in *Computer law & security Review*, n. 34/2018, pp. 436–449; I. S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, op.cit.; G. D'ACQUISTO – M.NALDI, *Big data e privacy by design*, Torino, 2017; V. MAYER-SCHÖNBERGER - K. N. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, op.cit.; O. POLLICINO – T. E. FROSINI – E. APA, *Diritti e libertà in Internet*, Milano, 2017; R. BIFULCO - O. POLLICINO - G. D'ACQUISTO - M. NALDI - M. BASSANI - F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dati personali e regolazione*, Milano, 2018.

personali⁹. Il testo, entrato in vigore nel maggio 2018 in tutti gli Stati membri, definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»¹⁰. Affinchè tale attività possa essere sottoposta al sistema di norme delineato a livello europeo è necessario, quindi, che essa consista in un procedimento automatizzato, anche in completa assenza del coinvolgimento umano.

È in questo punto che si identifica il nodo cruciale della questione ed emerge in maniera significativa il ruolo dell'intelligenza artificiale: la profilazione in sé non rappresenta qualcosa di necessariamente lesivo dei diritti degli individui. Può, tuttavia, potenzialmente diventarlo nel momento in cui la raccolta ed il trattamento dei dati personali avviene in maniera automatizzata e l'intervento degli individui sugli algoritmi operanti in tali attività risulta estremamente limitato se non addirittura nullo. Questo è il motivo per cui il legislatore europeo, all'interno del nuovo quadro normativo, ha spostato la propria attenzione dalla semplice attività di profilazione alle ben più rischiose decisioni basate unicamente sul trattamento automatizzato, dettando per quest'ultime una differente e specifica disciplina.

Nel primo caso, infatti, come indicato dal Considerando 72), l'attività deve realizzarsi nel pieno rispetto delle norme e dei principi stabiliti in via generale

⁹ 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). Sul punto cfr., inter alia, D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 2018; G. FINOCCHIARO, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali – dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*. Vol. 2, Torino, 2016; L. BOLOGNINI –E. PELINO – C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; G. BUTTARELLI, *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law*, 2/2016; F. DI RESTA, *La nuova 'Privacy europea': I principali adempimenti del regolamento UE 2016 e profili risarcitori*, Torino, 2018, T.ZARSKY, *Incompatible: The GDPR in the Age of Big Data* in *Seton Hall Law Review*, 47(4), 2017, 995 ss.

¹⁰ Regolamento (EU) n. 679/2016, art. 4, par. 4.

per il trattamento dei dati personali, come i principi di liceità, correttezza, trasparenza e minimizzazione delle informazioni che sono definiti nel Capo II del Regolamento europeo. Il titolare deve inoltre garantire pienamente il sistema di diritti riconosciuto e tutelato dal quadro normativo a favore del soggetto interessato, con particolare riferimento ai casi in cui l'operazione si sostanzia in una valutazione sistematica e globale di aspetti personali e su di essa si fondino decisioni che hanno effetti giuridici o incidono in modo analogo in maniera significativa sui soggetti interessati¹¹.

Nel secondo caso, invece, l'assenza assoluta dell'intervento umano legittima un inasprimento delle norme in materia. Ai sensi dell'articolo 22, in presenza di decisioni basate esclusivamente su un trattamento automatizzato, si pensi ad esempio all'impiego di un algoritmo che opera automaticamente in assenza dell'intervento discrezionale ed eventualmente correttivo di un individuo, il soggetto interessato ha il diritto di opporsi nel caso in cui tale attività produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Il GDPR, quindi, riconosce il potere di opporsi a un trattamento effettuato in assenza di coinvolgimento umano.

¹¹ Come è noto, ai sensi dell'art. 35 del Regolamento (UE) 679/2016 in caso di trattamenti che in virtù delle tecnologie utilizzate possono esporre i soggetti interessati ad un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto, ancor prima di intraprendere l'attività, di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Poiché tale analisi, nota anche come DPIA - *Data protection impact assessment* - affinché sia significativa deve necessariamente tenere conto della natura, dell'oggetto, del contesto e delle finalità perseguite dal titolare, il legislatore europeo non ha delineato in maniera puntuale il modo in cui tale procedura deve essere necessariamente eseguita. Tuttavia, sul punto è intervenuto successivamente il WP29, il Gruppo di lavoro art. 29, oggi sostituito dall'*European Data Protection Board*, che, attraverso le *Guidelines on Personal data breach notification under Regulation 2016/679*, ha individuato una serie di informazioni fondamentali che il titolare è tenuto obbligatoriamente ad inserire all'interno della valutazione d'impatto. In particolare, tra quest'ultime rientrano: la descrizione dettagliata del trattamento, compresi i dati personali coinvolti; la metodologia ed il periodo di conservazione di tali informazioni; le risorse su cui si basano i dati personali (hardware, software, reti, persone, canali di trasmissione cartacei e non cartacei); la descrizione delle misure previste per conformarsi al Regolamento con particolare riferimento ai principi di necessità e proporzionalità (articoli 5 e 6 del GDPR) e ai diritti degli interessati (articoli 12 - 21, capitolo V e art. 36 del GDPR); la descrizione dei rischi per i diritti e le libertà degli interessati e le misure previste per il contenimento di tali rischi. Inoltre, la documentazione deve includere anche una prova documentale della conformità ai codici di condotta, se esistenti, ai sensi dell'articolo 40 del GDPR, nonché certificazioni, marchi di fabbrica e *binding corporate rules* relativi alla protezione dei dati. L'obiettivo è dimostrare che il titolare, alla luce della rischiosità dell'attività prevista, abbia adottato le misure tecniche ed organizzative necessarie ad assicurare la piena conformità alle norme del Regolamento europeo.

Tale previsione in presenza di un uso sempre più pervasivo delle nuove tecnologie assume una straordinaria importanza ai fini della tutela dei diritti fondamentali dei soggetti interessati.

E' recente, infatti, risalendo ad aprile 2019, la sentenza con la quale il Consiglio di Stato, in materia di assegnazione di sedi scolastiche mediante sistemi automatizzati, ha dichiarato che nelle procedure valutative «il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico»¹². Prova questa che l'utilizzo di tecnologie, soprattutto in settori estremamente importanti e delicati come quello della pubblica amministrazione, le cui attività inevitabilmente si riflettono sulla sfera personale e sociale dei cittadini, richiede un'attenzione particolare, nella piena consapevolezza che il coinvolgimento umano deve sempre essere considerato elemento fondamentale, se non imprescindibile di tale panorama. Anche quando l'intelligenza artificiale oggettivamente consente di raggiungere risultati più efficaci in minore tempo e con minore sforzo, il suo impiego non può comunque sganciarsi dal fattore umano, da quell'universo di valori, principi, logiche che orientano razionalmente l'agire degli individui e che permette di assumere decisioni senza ledere gli elementi cardine di una società democraticamente avanzata.

3. Le *Ethics Guidelines for Trustworthy AI*.

Alla luce di quanto evidenziato e delle nuove sfide che emergono all'interno di uno scenario estremamente complesso e in perenne trasformazione, un'attenzione particolare è attualmente rivolta ai dispositivi fondati sull'utilizzo

¹² Cons. St., sez. VI, sent. 2270/2019 del 8.4.2019. La sentenza ha avuto origine dal ricorso sollevato dal personale di una scuola che lamentava come l'utilizzo da parte del MIUR di un algoritmo avrebbe inficiato e, sotto alcuni aspetti, alterato la procedura valutativa a cui erano stati sottoposti per l'inserimento nel contesto scolastico a tempo indeterminato. In particolare, secondo gli appellanti, tale algoritmo avrebbe disposto i trasferimenti «senza tener conto delle preferenze indicate nelle rispettive domande di trasferimento, senza alcuna motivazione e in difetto della benché minima trasparenza» seguendo una procedura totalmente irrazionale che ha portato ad assegnare docenti con svariati anni di servizio ad ambiti territoriali mai richiesti e situati a centinaia di chilometri di distanza dalla propria città di residenza. Il Consiglio di Stato, pur sottolineando i contributi positivi derivanti dall'utilizzo delle nuove tecnologie, ha ritenuto di accogliere le istanze, affermando che nel caso di specie sussiste la violazione dei principi di imparzialità, pubblicità e trasparenza in quanto la logica sottesa al procedimento risulta essere ignota impedendo di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo.

dell'intelligenza. Questo a partire dalla consapevolezza che tali tecnologie, fermo restando il loro straordinario ed indiscutibile contributo allo sviluppo delle moderne società, "plasmano" il futuro sfruttando dati provenienti dal passato. In potenziale antitesi con il normale processo evolutivo della persona, tutelato costituzionalmente, l'intelligenza artificiale opera, infatti, rielaborando informazioni e dati accumulati nel corso del tempo per anticipare o prevedere comportamenti futuri, in completa assenza di quegli elementi di imprevedibilità, capacità di discernimento e di apprendimento per esperienza che sono alla base dell'evoluzione della personalità degli individui.

Alla luce di tale visione, al fine di limitare gli effetti distorsivi dell'impiego di tali tecnologie, si è affermata a livello europeo l'idea che sia necessario "indirizzare" lo sviluppo dell'intelligenza artificiale mediante la previsione di una serie di norme di natura etica finalizzate a garantire uno sviluppo antropocentrico delle nuove tecnologie. Come evidenziato nella Risoluzione del Parlamento europeo del 2017¹³, «gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui» considerano l'automatizzazione dei processi decisionali uno strumento di supporto e non di prevaricazione dell'azione degli esseri umani. In altri termini, fermo restando l'inevitabile necessità di sfruttare le opportunità provenienti dal nuovo panorama digitale, le tecnologie dovrebbero essere sempre pensate come mezzi a disposizione dell'uomo, finalizzate a migliorare il livello qualitativo della vita degli individui, considerati sia come singoli sia come comunità, senza mai pretendere - o meglio consentire - di sostituirli ad essi. In tale prospettiva, mutuando una definizione particolarmente nota nel quadro normativo europeo in materia di tutela di dati personali, si impone la necessità di introdurre nel dinamico panorama delle nuove tecnologie quello che potrebbe essere definito un principio di "etica by design". La consapevolezza che l'interdipendenza uomo-macchina risulterà essere sempre più intensa nel corso degli anni spinge, infatti, a ritenere fondamentale stabilire oggi, che siamo ai primordi di tale evoluzione, il ruolo e i limiti di tali tecnologie allorquando vengono immesse per la prima volta all'interno dei processi produttivi aziendali ovvero a disposizione dei meccanismi decisionali della pubblica amministrazione, nonché quando contribuiscono alle attività di

¹³ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

erogazione dei servizi pubblici o entrano nella quotidianità dei singoli individui tramite l'acquisto di dispositivi connessi.

In quest'ottica la Commissione Europea ha avviato a partire dal 2018 una specifica strategia volta a garantire che l'implementazione di tali tecnologie avvenga in maniera affidabile, sicura ed eticamente sostenibile. L'obiettivo è quello di realizzare un'azione coordinata a livello europeo che assicuri il più ampio sfruttamento delle potenzialità dell'IA garantendo al contempo che il relativo sviluppo sia incentrato sull'uomo e destinato al bene comune con il fine ultimo di migliorare il benessere e la libertà degli individui. Tali misure hanno previsto, in primo luogo, la sottoscrizione da parte di 25 Stati membri della Dichiarazione sulla cooperazione in materia di IA¹⁴ al fine di garantire un approccio condiviso orientato al perseguimento della massimizzazione degli investimenti in tale settore, la creazione di uno spazio europeo dei dati, la promozione del talento e dell'apprendimento permanente e lo sviluppo di soluzioni di IA etiche ed affidabili. Nel giugno 2018 si è proceduto, poi, alla creazione dell'*High Level Expert Group* che recentemente, in data 8 aprile 2019, ha diffuso un documento dal titolo "*Ethics Guidelines for Trustworthy AI*"¹⁵. Frutto del lavoro di 52 esperti,¹⁶ le linee guida mirano a promuovere la diffusione di un'intelligenza artificiale affidabile grazie al contemporaneo agire di tre fattori essenziali: il rispetto dell'articolato quadro normativo in materia; la garanzia dei principi e dei valori etici e la solidità dei sistemi AI da un punto di vista tecnico e sociale.

In particolare, al fine di garantire un effettivo utilizzo ottimale di tali tecnologie, evitando il verificarsi di eventi che possano compromettere il libero esercizio dei diritti fondamentali, le linee guida individuano sette elementi chiave da rispettare nel concreto sviluppo dei sistemi basati sull'IA.

¹⁴ *Declaration of cooperation on Artificial Intelligence (AI)* siglata il 10 aprile 2018 da 25 Stati europei, Norvegia, Svizzera e Commissione Europea. Il testo della Dichiarazione è reperibile al link <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence>.

¹⁵ Le linee guida redatte dal Gruppo di esperti possono essere scaricate sul sito della Commissione Europea al seguente indirizzo <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

¹⁶ Il Gruppo si compone di 52 esperti nominati a seguito di una procedura di selezione aperta e provenienti dal mondo accademico, dall'industria e dalla società civile. Il loro compito è quello di sostenere la strategia europea in materia di intelligenza artificiale attraverso la formulazione di raccomandazioni relative alle questioni etiche, legali e sociali connesse all'IA, comprese le emergenti sfide economiche-sociali.

Il primo, denominato "Azione e sorveglianza umana", prevede che l'IA debba essere destinata allo sviluppo di società eque, offrendo sostegno all'attività umana senza mai compromettere l'esercizio dei diritti fondamentali, né limitare o alterare l'autonomia degli individui. La "Robustezza e sicurezza" evidenzia, invece, come l'affidabilità dell'IA dipende dall'adozione di algoritmi sicuri, attendibili e sufficientemente robusti e dalla predisposizione di apposite misure che consentano di intervenire in maniera celere in caso di errori ed incongruenze. Il terzo elemento riporta l'attenzione sulla tutela delle informazioni: con la categoria "Riservatezza e *governance* dei dati", infatti, il gruppo di esperti afferma che il coinvolgimento di dati personali deve sempre avvenire nel pieno rispetto dei diritti fondamentali del soggetto interessato attraverso la predisposizione di una serie di misure che consentano allo stesso di seguire l'utilizzo dei dati lungo tutto il ciclo di vita dell'IA. Strettamente collegata a quest'ultimo elemento vi è la "Trasparenza" che impone la tracciabilità dei sistemi di IA in ogni fase del loro ciclo di vita.

"Diversità, non discriminazione ed equità" costituiscono il quinto elemento chiave dello sviluppo dei sistemi IA ed evidenziano come la loro implementazione debba avvenire nel pieno rispetto delle capacità, delle competenze e delle necessità degli individui interessati ed essere a loro volta sempre accessibili. Il sesto elemento, invece, denominato "Benessere sociale e ambientale" sottolinea anche la necessità di utilizzare i sistemi IA al fine di garantire un efficace ed efficiente progresso della società e consentire uno sfruttamento sostenibile dell'ambiente. Infine, l'ultimo elemento è costituito dalla "Responsabilità intesa anche come *accountability*": l'implementazione dell'Intelligenza artificiale deve prevedere obbligatoriamente misure finalizzate a valutare la responsabilità ed il livello di *accountability* dei sistemi utilizzati, nonché dei risultati ottenuti.

Il rispetto simultaneo di tali sette elementi secondo la Commissione Europea consentirà la realizzazione di sistemi IA affidabili, in grado di garantire un utilizzo sicuro ed ottimale delle relative tecnologie nel pieno rispetto dei principi e dei diritti fondamentali degli individui. Inoltre, al fine di garantire che tali principi non rimangano incompiuti, ma siano effettivamente impiegati nello sviluppo ed utilizzo concreto di tecnologie basate sull'IA, le linee guida prevedono anche una lista di azioni operative per ognuno dei sette punti evidenziati, denominata *Trustworthy AI Assessment List*, in modo da offrire agli operatori strumenti concreti per la valutazione effettiva dell'affidabilità dei

sistemi utilizzati e favorire interventi tempestivi nel caso in cui vengano riscontrati elementi di criticità.

Rileva sottolineare in tale sede, infine, che il documento redatto dalla Commissione Europea segue solo di pochi mesi l'adozione delle "Linee guida in materia di intelligenza artificiale e protezione dei dati" redatte dal Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, che dal 2016 è presieduto dal Garante italiano¹⁷. Seguendo il medesimo filo conduttore, il testo, approvato a Strasburgo il 25 gennaio 2019, sottolinea all'art. 1 che la tutela della dignità umana e delle libertà fondamentali, in particolare il diritto alla protezione dei dati personali, sono essenziali nello sviluppo e nell'adozione di applicazioni IA. Rivolto soprattutto agli sviluppatori, ai produttori ed ai fornitori di servizi, il documento sottolinea la necessità di adottare un approccio di tipo preventivo basato sulla valutazione *ex ante* del possibile impatto, anche indiretto o involontario, di tali sistemi sul libero e consapevole esercizio dei diritti fondamentali.

4. Le linee guida in materia di Intelligenza Artificiale alla luce del Regolamento (EU) 2016/679.

Accountability, governance dei dati e preventiva valutazione di impatto non solo rappresentano alcuni dei parametri fondamentali individuati nelle *Guidelines for Trustworthy AI*, ma costituiscono anche gli elementi cardine del Regolamento europeo in materia di protezione dei dati personali (GDPR) che, come è noto, è entrato in vigore a partire dal 25 maggio 2018. Il nuovo quadro normativo, infatti, al fine di garantire che gli individui possano disporre sempre del pieno controllo dei propri dati personali, stabilisce un sistema peculiare di obblighi a carico del titolare del trattamento, il quale ai sensi dell'art. 24, è tenuto a predisporre misure tecniche ed organizzative adeguate per assicurare, ed essere in grado di dimostrare, che l'attività sia effettuata sempre nel pieno rispetto del GDPR. Dette misure debbono essere messe in atto ancor prima del rilascio delle informazioni personali e riguardare l'intero ciclo di utilizzo del

¹⁷ *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) - Guidelines on Artificial Intelligence and Data Protection*. Il testo in italiano è consultabile sul sito del Garante per la protezione dei dati personali al link <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096716>.

dato. In tal senso, è possibile affermare che i parametri della "Robustezza e sicurezza", della "Riservatezza e *governance* dei dati" e della "Responsabilità intesa anche come *accountability*" trovano piena realizzazione nel GDPR negli obblighi connessi alla *privacy by design* e *by default* di cui all'art. 25, nei principi di minimizzazione, liceità, correttezza e trasparenza di cui all'art. 5, nonché nella previsione del *Data protection impact assessment* e negli interventi prescritti ai sensi dell'art. 32 in caso di eventi di *data breach*. L'art. 35, in particolare, stabilisce esplicitamente che in caso di attività di trattamento particolarmente delicate, tra le quali rientra anche la valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, il titolare è tenuto ad eseguire una valutazione di impatto al fine di verificare se il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, tenuto conto della natura dell'ambito di applicazione, del contesto e delle finalità previste.

Continuando in questa opera di raffronto tra le linee guida redatte dalla Commissione in materia di intelligenza artificiale e Regolamento europeo i parametri denominati "Azione e sorveglianza umana", "Trasparenza" e "Diversità, non discriminazione ed equità" trovano, invece, piena realizzazione nel Capo III dedicato ai diritti dell'interessato. Si tratta di un vasto ed articolato sistema di norme a tutela dei soggetti che mettono a disposizione i propri dati personali, che vanno dal diritto di informazione (artt. 13-14) e di accesso (art.15) alla possibilità di richiedere la rettifica (art.16) o la cancellazione degli stessi (art.17), fino all'opportunità prevista di opporsi in qualsiasi momento (art.21). Con riferimento proprio al diritto di opposizione riconosciuto e garantito all'interno del nuovo quadro normativo, ai fini dell'analisi dell'applicazione dei sistemi basati sull' IA alla luce del GDPR rileva sicuramente esaminare quanto previsto in materia di processi decisionali esclusivamente automatizzati relativi alle persone fisiche. Come evidenziato in precedenza, infatti, il legislatore europeo ha distinto tale peculiare trattamento dalla più generale attività di profilazione, prevedendo per esso una disciplina differenziata. Alla luce del *based risk approach* che ispira l'intero GDPR e del maggiore rilievo attribuito al momento del consenso rispetto a quanto precedentemente stabilito dalla direttiva 95/46/CE, in linea con quanto indicato dall'*Article 29 Data Protection Working Party* nell'opinione 15/2011¹⁸ la

¹⁸ ARTICLE 29 WORKING PARTY, *Opinion 15/2011 on the definition of consent* (WP187).

profilazione, infatti, necessita di una manifestazione di volontà da parte dell'interessato che sia libera, specifica, informata ed inequivocabile. Diversa disciplina è invece destinata ai trattamenti in cui il processo decisionale si sostanzia in una decisione basata unicamente su un trattamento automatizzato, vale a dire in assenza di un qualsiasi intervento umano. In tale ambito, indipendentemente dal fatto che l'attività sia finalizzata o meno a profilare un individuo, il legislatore europeo stabilisce all'art.14 l'obbligo a carico del titolare di informare l'interessato, nonché di fornire informazioni significative sulla logica utilizzata, sull'importanza e sulle conseguenze previste per lo stesso. Strettamente collegato a tale previsione opera, come precedentemente evidenziato, il divieto di adozione di decisioni basate unicamente sul trattamento automatizzato qualora queste producano effetti giuridici che riguardano il soggetto interessato ovvero che incidano significativamente sulla sua persona. L'obiettivo del legislatore è evidentemente quello di garantire che un soggetto sottoposto ad una decisione rilevante per l'esercizio delle proprie libertà fondamentali, si pensi ad esempio al rifiuto automatico dell'accensione di un prestito bancario o l'esclusione diretta da un processo di selezione lavorativa, possa sempre essere consapevole dei meccanismi e delle logiche che hanno condotto a quel determinato risultato ed opporsi a tale tipo di trattamento. A tal fine, l'art. 22 stabilisce il diritto di ogni soggetto di non essere sottoposto a valutazioni di tale tipo a meno che la decisione sia necessaria per la conclusione o l'esecuzione di un contratto; sia autorizzata dal diritto dell'Unione o dello Stato membro; ovvero si basi sul consenso esplicito dell'interessato.

Nel peculiare e complesso bilanciamento tra la necessità di implementare una procedura decisionale interamente automatizzata e l'esigenza di garantire e tutelare la corretta evoluzione della personalità dell'individuo, libera dai potenziali effetti distorsivi o discriminatori che potrebbero derivare dal mancato intervento dell'uomo, la terza ipotesi, prevedendo un consenso esplicitamente rilasciato e quindi caratterizzato da elementi ulteriori rispetto alla manifestazione di volontà richiesta per una normale profilazione, pone maggiori criticità. L'obbligo di un atto volitivo di tal tipo, caso unico insieme al trattamento di dati sensibili *ex art. 9* e al trasferimento di informazioni personali verso un paese terzo o un'organizzazione internazionale in assenza di adeguate garanzie *ex art. 49*, evidenzia sicuramente l'importanza che viene posta dal legislatore europeo sulla effettiva capacità di controllo dei dati personali da parte degli interessati e sulla relativa possibilità per gli stessi di

opporsi al loro trattamento ogni qualvolta vengano utilizzati sistemi che non prevedono il coinvolgimento di esseri umani. Tuttavia, nonostante tale rilievo, il Regolamento risulta lacunoso proprio nella definizione concreta di "consenso esplicito".

Nel silenzio del nuovo quadro normativo, le linee guida redatte dal WP29 in materia di consenso stabiliscono che tale ulteriore impegno dovrebbe generalmente sostanziarsi nel rilascio di un'approvazione scritta e firmata dalla parte interessata. Nel caso, invece, di attività che si realizzano mediante piattaforme e siti *on line*, il consenso esplicito richiederebbe la compilazione dell'interessato di un modulo specifico ovvero il caricamento di un documento personale. È evidente che lo sforzo interpretativo compiuto dal gruppo dei regolatori europei risulta particolarmente apprezzato in un contesto in cui ogni singolo vuoto normativo rischia di aprire la strada ad una potenziale lesione dei diritti fondamentali. Tuttavia, in un panorama caratterizzato dal ruolo sempre più rilevante di sistemi basati sull' IA, la mancanza di una disciplina chiara ed inequivocabile rende estremamente elevato il rischio che tale disposizione si sostanzi in una norma facilmente eludibile. La previsione di un consenso esplicito in assenza di specifiche indicazioni sul come esso debba concretizzarsi, infatti, lo priva di quella indispensabile forza volitiva necessaria a renderlo distinto e separato da una normale manifestazione di assenso, favorendo l'adozione di forme di consenso standardizzate da parte dei titolari dei trattamenti basati su processi decisionali interamente automatizzati.

Questo finisce inevitabilmente col determinare una breccia nel nuovo panorama di tutela dei dati personali che, come ampiamente noto, fonda le proprie radici proprio sul recupero del pieno controllo delle informazioni personali da parte degli interessati, ponendo particolare attenzione sull'intero procedimento di formazione del consenso al fine di garantire che l'individuo sia sempre consapevole, informato e libero da ogni sorta di influenza esterna in grado di alterare l'autenticità della sua volontà¹⁹.

5. Conclusioni.

¹⁹ In base al considerando 32) del Regolamento (UE) 679/2016, infatti, al fine di garantire che l'approvazione del trattamento sia liberamente concessa e informata in modo soddisfacente, "dovrebbe essere fornita da un chiaro atto affermativo che stabilisca un'indicazione liberamente concessa, specifica, informata e inequivocabile del consenso dell'interessato al trattamento di dati personali che lo riguardano, come ad esempio una dichiarazione scritta, anche per via elettronica, o una dichiarazione orale".

Nella ricerca di un adeguato equilibrio tra tutela dei diritti fondamentali ed evoluzione delle nuove tecnologie un'attenzione particolare deve oggi essere rivolta all'uso dell'Intelligenza Artificiale, la cui diffusione, in assenza di appropriate regole, è potenzialmente in grado di limitare l'esercizio delle libertà tradizionalmente riconosciute come pilastro fondamentale di ogni società democratica. Come evidenziato nel lavoro, al fine di garantire siffatto obiettivo si è affermata la convinzione a livello europeo che l'utilizzo di tali strumenti debba essere indirizzato principalmente verso il soddisfacimento delle esigenze di miglioramento del livello qualitativo della vita dell'uomo, sia come singolo sia come membro di una comunità organizzata, allontanando al contempo ogni possibile rischio di lesione della sfera personale degli individui causata da una illegittima compressione delle proprie libertà di scelta e delle relative possibilità di autodeterminazione. Secondo una logica di "etica by design", l'implementazione dell'IA dovrebbe, infatti, essere guidata da una serie di norme etiche di riferimento dirette ad evitare che i principi ed i valori democratici vengano irrimediabilmente sacrificati in nome dell'efficienza dei processi produttivi e del connesso valore economico delle informazioni personali, ormai considerate il "petrolio" del nuovo scenario digitale²⁰.

In tale peculiare panorama, le *Guidelines for Trustworthy AI* adottate dalla Commissione Europea nell'aprile 2019 costituiscono un primo importante tassello verso la concreta realizzazione di tale percorso evolutivo. Ad esse, infatti, si deve innanzitutto il merito di aver individuato una serie di regole generali, valedoli *erga omnes*, la cui applicazione su larga scala dovrebbe contribuire nell'immediato futuro a creare un ecosistema contraddistinto da un impiego dell'Intelligenza Artificiale affidabile ed eticamente sostenibile.

Inoltre, alla luce dell'inevitabile intreccio esistente tra regolazione delle nuove tecnologie e tutela dei dati personali, le linee guida si caratterizzano per una positiva continuità con le norme introdotte dal Regolamento europeo 679/2016. Questo soprattutto con riguardo ai principi della "Robustezza e della sicurezza" e della "Responsabilità intesa anche come *accountability*" il cui contenuto riflette pienamente il "*risk based approach*" che contraddistingue l'attuale quadro normativo in materia.

²⁰ Questa è la definizione indicata dall'attuale Presidente del Garante italiano per la protezione dei dati personali, Antonello Soro, in occasione di un'intervista relativa all'attuale debolezza delle imprese nei confronti di attacchi di carattere cyber. L'intervista è reperibile sul sito del Garante, documento *web* n. 8136779, *Le imprese sono troppo deboli nelle difese contro gli hacker*, del 26 marzo 2018.

Maggiori criticità, invece, come evidenziato, si riscontrano sul versante del coinvolgimento consapevole dei soggetti interessati. Si tratta di un aspetto estremamente delicato che richiede un sollecito intervento da un punto di vista regolativo visto che uno degli elementi di maggiore rischiosità celate dietro l'impiego delle nuove tecnologie risiede proprio nella difficoltà per i soggetti interessati di comprendere pienamente le dinamiche che guidano il funzionamento di determinati algoritmi con evidente pregiudizio per il valore del consenso espresso, troppo spesso lontano da quella "manifestazione di volontà libera, specifica, informata e inequivocabile" richiesta dal Regolamento (UE) 679/2016²¹. In un panorama in cui cruciale si rileva il controllo dei propri dati personali al fine di evitare situazioni di utilizzo illegittimo ed indesiderato degli stessi, una disciplina nebulosa proprio in materia di consenso, soprattutto con riferimento a quello esplicito richiesto nei casi di processi decisionali automatizzati, rischia di rendere estremamente fragili le fondamenta su cui si poggia l'intero impianto normativo delineato dal legislatore europeo, con risvolti estremamente critici in termini di protezione dei diritti fondamentali e di tutela della dignità degli individui.

Infine, l'ampiezza dei sette elementi chiave individuati dalle *Guidelines for Trustworthy AI* evidenziano come il processo di realizzazione di una Intelligenza Artificiale di tipo antropocentrico possa considerarsi ad oggi ancora agli stadi iniziali, richiedendo necessariamente un agire trasversale ampiamente condiviso tra più settori ed operante su diversi livelli di azione. Accanto, infatti, al fondamentale ruolo del legislatore sovranazionale e di quelli nazionali ai quali spetta il delicato compito di intervenire in maniera sollecita nel regolamentare una materia in continuo divenire avendo sempre come obiettivo finale la tutela dei diritti fondamentali e la protezione della dignità degli individui interessati dalle attività di trattamento dei dati, emerge la necessità di un coinvolgimento consapevole dei soggetti che progettano tali tecnologie. Questo al fine di garantire che principi come la *privacy by design* e la *privacy by default* e, parallelamente, gli obiettivi della robustezza e della affidabilità individuati dalle stesse Linee guida in materia si traducano in risultati concreti e non si limitino a rimanere buoni propositi sulla carta.

²¹ Ai sensi dell'art. 4, par. 11, infatti il consenso dell'interessato deve sostanziarsi in «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

Stesso discorso vale per i soggetti che implementano gli strumenti di Intelligenza Artificiale sui quali ricade il delicato sistema di *accountability* delineato dal Regolamento (EU) 679/2019. Ad essi, infatti, spetta il fondamentale compito di calare nella realtà operativa le regole stabilite dal legislatore europeo, nonché di agire in modo tempestivo in caso di violazioni che siano in grado di provocare danni fisici, materiali o immateriali alle persone fisiche e, soprattutto, di notificare eventi critici operando come indispensabile strumento di ausilio dell'attività svolta dalle autorità di controllo²².

Infine, il percorso evolutivo verso una intelligenza artificiale affidabile ed eticamente sostenibile richiede anche il coinvolgimento consapevole dei destinatari dei servizi erogati attraverso il rafforzamento del parametro della "trasparenza" inteso sia in termini di conoscibilità delle logiche che guidano i contesti decisionali di tipo algoritmico così come richiesto dalle Linee guida oggetto di analisi, sia in termini di completezza delle informazioni che obbligatoriamente devono essere fornite ai soggetti interessati al fine di consentire loro di esperire i rimedi previsti dall'attuale quadro normativo in materia di tutela dei dati personali in caso di eventi lesivi dei propri diritti fondamentali.

Da quanto evidenziato deriva che solo tale agire congiunto, esplicitamente indicato nel Regolamento (EU) 679/2019 e derivabile dalla lettura combinata dei sette elementi chiave individuati dalle *Ethics Guidelines for Trustworthy AI*, consentirà di delineare nell'immediato futuro un panorama imperniato sull'utilizzo di una intelligenza artificiale di tipo antropocentrico, ispirata al principio dell'"etica by design", che, opportunamente regolamentato, permetterà di garantire l'inevitabile evoluzione delle moderne società democratiche preservando quel sistema di diritti, di libertà e di valori che di tali comunità costituisce, come è noto, il pilastro fondamentale.

²² L'art. 83 del Regolamento (UE) 679/2016 stabilisce, infatti, che in caso di violazioni il titolare del trattamento è tenuto a contattare l'autorità di controllo «senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo». Sullo stesso piano opera l'obbligo previsto dall'art. 84 secondo cui «quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche» il titolare del trattamento è tenuto a comunicare l'avvenuta violazione all'interessato senza ingiustificato ritardo.