EDPB-GEPD

Parere congiunto 5/2021

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)

18 giugno 2021

Sintesi

Il 21 aprile 2021 la Commissione europea ha presentato la propria proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (in appresso «la proposta»). L'EDPB e il GEPD valutano positivamente i timori espressi dal legislatore nell'affrontare la questione dell'utilizzo dell'intelligenza artificiale (IA) all'interno dell'Unione europea (UE) e sottolineano che la proposta ha **implicazioni** estremamente rilevanti per la **protezione dei dati**.

L'EDPB e il GEPD rilevano che la **base giuridica** della proposta è innanzi tutto l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). Inoltre, la proposta è basata altresì sull'articolo 16 del TFUE nella misura in cui contiene disposizioni specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in particolare restrizioni dell'uso dei sistemi di IA per l'identificazione biometrica da remoto «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto. L'EDPB e il GEPD rammentano che, in linea con la giurisprudenza della Corte di giustizia dell'Unione europea (CGUE), l'articolo 16 del TFUE costituisce una base giuridica appropriata nei casi in cui la protezione dei dati personali rappresenti uno degli obiettivi o dei componenti essenziali delle norme adottate dal legislatore dell'UE. L'applicazione dell'articolo 16 del TFUE comporta altresì la **necessità di garantire un controllo indipendente della conformità** ai requisiti per il trattamento dei dati personali, come prescritto anche dall'articolo 8 della Carta dei diritti fondamentali dell'UE.

Per quanto riguarda l'**ambito di applicazione della proposta**, l'EDPB e il GEPD valutano molto positivamente che esso sia stato ampliato alla messa a disposizione e all'utilizzo dei sistemi di IA da parte delle istituzioni, degli organi o delle agenzie dell'UE. Tuttavia, l'**esclusione della cooperazione internazionale in materia di contrasto dall'ambito di applicazione** della proposta suscita gravi preoccupazioni nell'EDPB e nel GEPD, considerato che comporta un rischio significativo di elusione (ad esempio nel caso di paesi terzi o di organizzazioni internazionali che gestiscono applicazioni ad alto rischio su cui fanno affidamento le autorità pubbliche dell'UE).

L'EDPB e il GEPD **accolgono con favore l'approccio basato sul rischio** su cui si fonda la proposta. Tuttavia, tale approccio dovrebbe essere chiarito e il concetto di «rischio per i diritti fondamentali» andrebbe uniformato all'RGPD e al regolamento (UE) 2018/1725 (EUDPR), poiché entrano in gioco aspetti correlati alla protezione dei dati personali.

L'EDPB e il GEPD concordano con la proposta laddove afferma che la classificazione di un **sistema di IA come ad alto rischio non significa necessariamente che esso sia lecito** di per sé e possa essere impiegato dall'utente così com'è. È possibile che il titolare del trattamento **sia tenuto a rispettare requisiti ulteriori previsti dalla legislazione dell'UE in materia di protezione dei dati**. Inoltre, la conformità agli obblighi giuridici previsti dalla legislazione dell'Unione (compresa quella in materia di protezione dei dati) dovrebbe essere una precondizione per l'autorizzazione all'immissione sul mercato europeo in qualità di prodotto munito della marcatura CE. A tal fine l'EDPB e il GEPD ritengono che **nel capo 2 del titolo III dovrebbe essere incluso l'obbligo di garantire la conformità all'RGPD e all'EUDPR**. Inoltre, l'EDPB e il GEPD reputano necessario adattare la procedura di valutazione della conformità prevista dalla proposta in modo tale che i terzi effettuino sempre valutazioni ex ante della conformità dei sistemi di IA ad alto rischio.

Considerato il rischio elevato di discriminazione, la proposta vieta le pratiche volte a determinare il «punteggio sociale» (*social scoring*) se attuate «per un determinato periodo di tempo» ovvero «da parte delle autorità pubbliche o per loro conto». Tuttavia, anche le società private come i media sociali e i fornitori

di servizi cloud possono trattare grandi quantità di dati personali e ricorrere a pratiche di punteggio sociale. Di conseguenza, **il futuro regolamento sull'IA dovrebbe proibire qualsiasi tipo di punteggio sociale**.

L'identificazione biometrica da remoto delle persone fisiche in spazi accessibili al pubblico comporta un rischio elevato di intrusione nella vita privata delle persone, con gravi ripercussioni sull'aspettativa dei cittadini di godere dell'anonimato nei luoghi pubblici. Per questi motivi l'EDPB e il GEPD **chiedono che sia introdotto un divieto generale di qualsiasi utilizzo dell'IA a fini di riconoscimento automatico delle caratteristiche umane in spazi accessibili al pubblico**, come il volto ma anche l'andatura, le impronte digitali, il DNA, la voce, le sequenze di battute su tastiera e altri segnali biometrici o comportamentali, in qualsiasi contesto. Un altro **divieto** raccomandato riguarda i **sistemi di IA che categorizzano le persone in insiemi, a partire dai dati biometrici,** in base all'etnia, al genere, all'orientamento politico o sessuale oppure in base ad altri motivi di discriminazione ai sensi dell'articolo 21 della Carta. Inoltre, l'EDPB e il GEPD ritengono che l'utilizzo dell'IA per **dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato.**

L'EDPB e il GEPD valutano positivamente la **designazione del GEPD quale autorità competente e autorità di vigilanza del mercato preposta alla vigilanza sulle istituzioni, le agenzie e gli organi dell'UE**. Tuttavia, il ruolo e i compiti del GEPD dovrebbero essere precisati meglio, specificamente per quanto riguarda il suo ruolo di autorità di vigilanza del mercato. Inoltre, il futuro regolamento sull'IA dovrebbe stabilire con chiarezza che le **autorità di controllo sono indipendenti** nell'esecuzione dei loro compiti di vigilanza e contrasto.

La designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe un approccio normativo più armonizzato e contribuirebbe a un'interpretazione coerente delle disposizioni in materia di trattamento dei dati, evitando così applicazioni contrastanti tra i vari Stati membri. Di conseguenza, l'EDPB e il GEPD ritengono che **le autorità per la protezione dei dati dovrebbero essere designate come autorità nazionali di controllo a norma dell'articolo 59 della proposta.**

La proposta assegna alla Commissione un ruolo predominante nel comitato europeo per l'intelligenza artificiale (CEIA). Tale ruolo è in contrasto con la necessità di un organismo europeo per l'IA che sia indipendente da qualsiasi influenza politica. Per garantirne l'indipendenza, il futuro regolamento sull'IA dovrebbe attribuire **al CEIA maggiore autonomia** e garantire che esso possa agire di propria iniziativa.

Vista la diffusione dei sistemi di IA nel mercato unico e la probabilità che si verifichino casi transfrontalieri, è imprescindibile assicurare un'applicazione coerente delle norme e una corretta ripartizione delle competenze tra le autorità nazionali di controllo. L'EDPB e il GEPD suggeriscono di prevedere, **per ciascun sistema di IA, un meccanismo che garantisca un punto di contatto unico per le persone interessate dalla legislazione e per le società**.

Per quanto riguarda gli **spazi di sperimentazione,** l'EDPB e il GEPD **raccomandano di precisarne l'ambito di applicazione e gli obiettivi**. La proposta dovrebbe altresì indicare chiaramente che la base giuridica degli spazi di sperimentazione dev'essere conforme ai requisiti di cui al vigente quadro per la protezione dei dati.

Il **sistema di certificazione** descritto nella proposta è **privo di un chiaro collegamento con la legislazione dell'UE in materia di protezione dei dati** e con altre normative dell'UE e degli Stati membri applicabili a ciascuna «area» dei sistemi di IA ad alto rischio; inoltre, non considera i **principi della minimizzazione dei dati e della loro protezione fin dalla progettazione** come uno degli aspetti da valutare **prima di ottenere la marcatura CE**. Pertanto l'EDPB e il GEPD raccomandano di modificare la proposta in modo

tale da chiarire il rapporto tra i certificati emessi a norma del regolamento citato e le certificazioni, i sigilli e le marcature relativi alla protezione dei dati. Infine, le autorità per la protezione dei dati dovrebbero essere coinvolte nella preparazione e nell'istituzione di norme armonizzate e specifiche comuni.

Per quanto riguarda i **codici di condotta**, l'EDPB e il GEPD reputano che sia **necessario chiarire** se la protezione dei dati personali debba essere considerata uno dei relativi «requisiti supplementari», nonché garantire che le «specifiche e soluzioni tecniche» non confliggano con le regole e i principi del vigente quadro dell'UE per la protezione dei dati.

INDICE

Il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati

Visto l'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE ([1]).

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018 ([2]).

Vista la richiesta di parere congiunto del Garante europeo della protezione dei dati e del Comitato europeo per la protezione dei dati, del 22 aprile 2021, sulla proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale),

HANNO ADOTTATO IL SEGUENTE PARERE CONGIUNTO.

1 INTRODUZIONE

1. L'avvento dei sistemi di intelligenza artificiale (in appresso «l'IA») rappresenta un passo molto importante nell'evoluzione delle tecnologie e nel modo in cui gli esseri umani interagiscono con esse. L'IA consiste in una serie di tecnologie fondamentali che modificheranno profondamente la nostra vita quotidiana, dal punto di vista sia sociale sia economico. Si prevede che nei prossimi anni saranno adottate decisioni fondamentali in materia di IA, in quanto tale tecnologia ci aiuta a superare alcune delle maggiori sfide che oggi dobbiamo fronteggiare in molti ambiti: dalla salute alla mobilità, dall'amministrazione pubblica all'istruzione.

2. Tuttavia, i progressi attesi non sono esenti da rischi. In realtà, i rischi sono molto rilevanti laddove si consideri che tuttora non disponiamo di alcuna esperienza relativamente a gran parte degli effetti di natura individuale e sociale dei sistemi di IA. Generare contenuti, fare previsioni o adottare decisioni in maniera automatica, come fanno i sistemi di IA, per mezzo di tecniche di apprendimento automatico o regole di inferenza logica e probabilistica è cosa diversa rispetto alle modalità con cui queste stesse attività sono svolte dagli esseri umani attraverso il ragionamento creativo o teorico, nella piena consapevolezza della responsabilità delle relative conseguenze.

3. L'IA amplierà la quantità di previsioni che si possono fare in molti ambiti – a cominciare dalle correlazioni quantificabili tra i dati, che sono invisibili all'occhio umano ma ben visibili alle macchine – semplificandoci la vita e risolvendo un gran numero di problemi; allo stesso tempo, però, verrà ridotta la nostra capacità di dare un'interpretazione causale dei risultati, al punto di

([1]) GU L 295 del 21.11.2018, pag. 39.
([2]) Nel presente documento, per «Stati membri» s'intendono gli «Stati membri del SEE».

mettere seriamente in discussione i concetti di trasparenza, controllo umano, rendicontabilità e responsabilità dei risultati.

4. In molti casi, nell'IA i dati (personali e non personali) sono la premessa essenziale delle decisioni autonome, con inevitabili conseguenze sulla vita delle persone a vari livelli. È questo il motivo per cui l'EDPB e il GEPD affermano vigorosamente già in questa fase che la proposta di regolamento che istituisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale; in appresso «la proposta») ([3]) ha **rilevanti implicazioni per la protezione dei dati.**

5. Affidare alle macchine il compito di prendere decisioni sulla base di dati comporterà rischi per i diritti e le libertà delle persone che incideranno sulla loro vita privata e potrebbero nuocere a categorie sociali o persino a intere società. L'EDPB e il GEPD sottolineano che i diritti alla vita privata e alla protezione dei dati personali, che sono in conflitto con il presupposto dell' autonomia decisionale da parte delle macchine su cui si fonda il concetto stesso di IA, costituiscono un pilastro dei valori dell'UE quali riconosciuti nella Dichiarazione universale dei diritti dell'uomo (articolo 12), nella Convenzione europea dei diritti dell'uomo (articolo 8) e nella Carta dei diritti fondamentali dell'Unione europea (in appresso «la Carta»; articoli 7 e 8). Riconciliare la prospettiva di crescita prospettata dalle applicazioni basate sull'IA con la centralità e la supremazia degli esseri umani rispetto alle macchine è un obiettivo molto ambizioso, ma nondimeno necessario.

6. L'EDPB e il GEPD valutano positivamente il coinvolgimento nella stesura del regolamento di tutte le parti interessate della catena di valori dell'IA, nonché l'introduzione di obblighi specifici per i fornitori di soluzioni, dato che svolgono un ruolo rilevante per i prodotti che usano i loro sistemi. Tuttavia, le responsabilità delle varie parti – utenti, fornitori, importatori o distributori dei sistemi di IA – devono essere circoscritte e attribuite chiaramente. In particolare, durante il trattamento dei dati personali occorre prestare un'attenzione speciale alla coerenza tra questi ruoli e responsabilità e i concetti di titolare del trattamento e responsabile del trattamento dei dati quali utilizzati nel quadro della protezione dei dati, trattandosi di due insiemi normativi non congruenti.

7. Con soddisfazione dell'EDPB e del GEPD, la proposta riserva un posto importante al concetto di sorveglianza (o supervisione) umana (articolo 14). Tuttavia, come già rilevato, a causa del forte impatto potenziale di taluni sistemi di IA sulle persone o su categorie di persone, l'effettiva centralità degli esseri umani dovrebbe fondarsi su una supervisione umana altamente qualificata e sulla liceità del trattamento, nella misura in cui tali sistemi si fondino sul trattamento di dati personali ovvero li trattino per svolgere le proprie funzioni, al fine di assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato.

8. Inoltre, a causa dell'impiego massivo di dati che caratterizza molte applicazioni basate sull'IA, la proposta dovrebbe promuovere l'adozione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita a ogni livello, incoraggiando l'effettiva attuazione

([3]) COM(2021) 206 final.

dei principi in materia di protezione dei dati (quali previsti dall'articolo 25 dell'RGPD e dall'articolo 27 dell'EUDPR) per mezzo di tecnologie all'avanguardia.

9. Infine, l'EDPB e il GEPD sottolineano che il presente parere congiunto è emesso esclusivamente a titolo di analisi preliminare della proposta, senza pregiudizio per eventuali valutazioni e pareri successivi relativi agli effetti della proposta stessa e alla sua compatibilità con la legislazione dell'UE in materia di protezione dei dati.

2 ANALISI DEI PRINCIPI FONDAMENTALI DELLA PROPOSTA

2.1 Ambito di applicazione della proposta e rapporto con il quadro giuridico vigente

10. Secondo la relazione di accompagnamento, la **base giuridica** della proposta è costituita innanzitutto dall'articolo 114 del TFUE, che prevede l'adozione di misure destinate ad assicurare l'instaurazione e il funzionamento del mercato interno ([4]). Inoltre, la proposta si fonda sull'articolo 16 del TFUE *in quanto contiene talune regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento di dati personali*, in particolare restrizioni all'utilizzo di sistemi di IA per l'identificazione biometrica da remoto «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto ([5]).

11. L'EDPB e il GEPD rammentano che, in linea con la giurisprudenza della CGUE, l'articolo 16 del TFUE costituisce una base giuridica adeguata quando la protezione dei dati personali è una delle finalità o delle componenti essenziali delle norme adottate dal legislatore dell'Unione ([6]). L'applicazione dell'articolo 16 del TFUE comporta inoltre la necessità di garantire un controllo indipendente della conformità ai requisiti in materia di trattamento dei dati personali, come richiesto altresì dall'articolo 8 della Carta.

12. Il GEPD e l'EDPB rammentano che esiste già un quadro complessivo per la protezione dei dati, che è stato adottato sulla base dell'articolo 16 del TFUE e comprende il regolamento generale sulla protezione dei dati (RGPD) ([7]), il regolamento sulla protezione dei dati personali per le istituzioni, gli organi e gli organismi dell'Unione (EUDPR) ([8]) e la direttiva sulla protezione dei dati nelle attività di contrasto (LED) ([9]). Secondo la proposta, soltanto le

([4]) Relazione, pag. 5.
([5]) Relazione, pag. 6. Cfr. anche il considerando (2) della proposta.
([6]) Parere del 26 luglio 2017, *PNR Canada*, procedura di parere 1/15, ECLI:EU:C:2017:592, punto 96.
([7]) 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) (GU L 119 del 4.5.2016, pag. 1).
([8]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).
([9]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera

restrizioni aggiuntive al trattamento di dati biometrici in essa contenute possono essere considerate fondate sull'articolo 16 del TFUE e, pertanto, sulla medesima base giuridica dell'RGPD, dell'EUDPR o della LED. Ciò ha rilevanti implicazioni per il rapporto tra la proposta e l'RGPD, l'EUDPR e la LED in termini più generali, come spiegato di seguito.

13. Per quanto riguarda l'**ambito di applicazione della proposta**, l'EDPB e il GEPD valutano molto positivamente il fatto che contempli anche l'uso dei sistemi di IA da parte delle istituzioni, degli organi o delle agenzie dell'UE. Considerato che l'utilizzo dei sistemi di IA da parte di tali entità può anche avere un impatto significativo sui diritti fondamentali delle persone fisiche, come accade negli Stati membri dell'UE, è indispensabile che il nuovo quadro normativo dell'IA si applichi sia agli Stati membri dell'UE sia alle sue istituzioni e ai suoi organi e organismi, al fine di garantire un approccio coerente in tutta l'Unione. Dato che le istituzioni, gli organi e gli organismi dell'UE possono agire sia come fornitori sia come utenti dei sistemi di IA, il GEPD e l'EDPB reputano che sia del tutto appropriato includere tali entità nell'ambito di applicazione della proposta, sulla base dell'articolo 114 del TFUE.

14. Tuttavia, l'EDPB e il GEPD nutrono gravi preoccupazioni circa l'esclusione della cooperazione internazionale in materia di contrasto dall'ambito di applicazione della proposta, a norma dell'articolo 2, paragrafo 4, della stessa. Tale esclusione comporta un notevole rischio di elusione (ad esempio nel caso dei paesi terzi o delle organizzazioni internazionali che gestiscono applicazioni ad alto rischio sulle quali fanno affidamento le autorità pubbliche nell'UE).

15. In molti casi lo sviluppo e l'utilizzo dei sistemi di IA comporterà il trattamento di dati personali. Garantire la chiarezza del rapporto tra questa proposta e la vigente legislazione dell'UE in materia di protezione dei dati è della massima importanza. La proposta fa salvi e integra l'RGPD, l'EUDPR e la LED. Benché i considerando della proposta specifichino che l'utilizzo dei sistemi di IA deve in ogni caso essere conforme alla normativa sulla protezione dei dati, **l'EDPB e il GEPD raccomandano vivamente di precisare, all'articolo 1, che la legislazione dell'Unione in materia di protezione dei dati personali** – in particolare l'RGPD, l'EUDPR, la direttiva ePrivacy ([10]) e la LED – si applica a qualsiasi trattamento di dati personali che rientri nell'ambito di applicazione della proposta stessa. Un corrispondente considerando dovrebbe parimenti chiarire che la proposta non mira a incidere sull'applicazione della vigente normativa dell'UE che disciplina il trattamento dei dati personali, compresi i compiti e i poteri delle autorità di controllo indipendenti preposte alla vigilanza sul rispetto di tale normativa.

2.2 Approccio basato sul rischio

16. L'EDPB e il GEPD **accolgono con favore l'approccio basato sul rischio** su cui si fonda la proposta. La proposta si applica a qualsiasi sistema di IA, compresi quelli che, pur non

circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

([10]) 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), modificata dalle direttive 2006/24/CE e 2009/136/CE.

comportando il trattamento di dati personali, possono tuttavia incidere sugli interessi o sui diritti e sulle libertà fondamentali.

17. L'EDPB e il GEPD rilevano che alcune delle disposizioni contenute nella proposta non prendono in considerazione i rischi per categorie di persone o per la società nel suo complesso (ad esempio effetti collettivi di particolare rilevanza come la discriminazione di gruppo o la manifestazione di opinioni politiche in spazi accessibili al pubblico). L'EDPB e il GEPD raccomandano che anche i rischi derivanti dall'IA per la società e le relative categorie siano valutati e attenuati.

18. L'EDPB e il GEPD sono del parere che dovrebbe essere chiarito l'approccio basato sul rischio adottato nella proposta **uniformando all'RGPD** il concetto di «rischio per i diritti fondamentali» per quanto riguarda gli aspetti correlati alla protezione dei dati personali. Che si tratti di utenti finali, semplici interessati o altre persone coinvolte dal sistema di IA, l'assenza nel testo della proposta di qualsiasi riferimento alla persona sulla quale si producono gli effetti del sistema di IA si configura come una grave carenza. Infatti, gli obblighi degli operatori nei confronti delle persone interessate dovrebbero emanare più concretamente dalla tutela del singolo e dei suoi diritti. Pertanto, l'EDPB e il GEPD sollecitano i legislatori ad affrontare esplicitamente nella proposta la questione dei **diritti e dei mezzi di ricorso a disposizione delle persone** soggette ai sistemi di IA.

19. L'EDPB e il GEPD prendono atto della scelta di fornire un elenco esaustivo **dei sistemi di IA ad alto rischio**. Una tale scelta rischia di avere effetti polarizzanti ostacolando l'individuazione ulteriore di situazioni fortemente rischiose, con la conseguenza di minare l'approccio basato sul rischio su cui si fonda complessivamente la proposta. Inoltre, l'elenco dei sistemi di IA ad alto rischio riportato in dettaglio negli allegati II e III della proposta non contempla alcune tipologie d'uso che comportano rischi significativi, come l'utilizzo dell'IA per il calcolo di premi assicurativi, la valutazione di trattamenti medici o la ricerca in campo medico. L'EDPB e il GEPD sottolineano altresì che gli allegati citati dovranno essere aggiornati periodicamente per garantire l'adeguatezza del loro ambito di applicazione.

20. La proposta richiede ai **fornitori** dei sistemi di IA di effettuare una valutazione del rischio; tuttavia, nella maggior parte dei casi i titolari del trattamento (dei dati) saranno gli **utenti** più che i fornitori dei sistemi di IA (ad esempio un utente di un sistema di riconoscimento facciale è un «titolare del trattamento» e pertanto non è vincolato dagli obblighi previsti dalla proposta per i fornitori di sistemi di IA ad alto rischio).

21. Inoltre, **un fornitore non sempre sarà in grado di valutare tutti gli utilizzi** del proprio sistema di IA. Quindi, la valutazione del rischio iniziale sarà di natura più generale rispetto a quella effettuata dall'utente del sistema di IA. Anche se la valutazione del rischio iniziale a opera del fornitore non classifica il sistema di IA come «ad alto rischio» ai sensi della proposta, non si dovrebbe escludere **una successiva valutazione (più granulare)** (valutazione d'impatto sulla protezione dei dati) a norma dell'articolo 35 dell'RGPD, dell'articolo 39 dell'EUDPR o dell'articolo 27 della LED, **che dovrebbe essere effettuata dall'utente del sistema** tenendo conto del contesto dell'utilizzo e dei casi d'uso specifici. La valutazione della possibilità che un determinato trattamento sia tale da comportare un rischio elevato ai sensi dell'RGPD,

dell'EUDPR e della LED deve essere eseguita indipendentemente dalla proposta. Per contro, la classificazione di un sistema di IA come «ad alto rischio» a causa del suo impatto sui diritti fondamentali ([11]) **comporta la presunzione dell'esistenza di un «rischio elevato» ai sensi dell'RGPD, dell'EUDPR e della LED nella misura in cui vi sia trattamento dei dati personali.**

22. **L'EDPB e il GEPD concordano con la proposta laddove specifica che la classificazione di un sistema di IA come ad alto rischio non significa necessariamente che esso sia di per sé lecito e possa essere utilizzato dall'utente in quanto tale. È possibile che il titolare del trattamento sia tenuto a rispettare requisiti ulteriori previsti dalla legislazione dell'UE in materia di protezione dei dati.** Inoltre, occorre analizzare il ragionamento alla base dell'articolo 5 della proposta secondo cui, diversamente dai sistemi vietati, i sistemi ad alto rischio possono essere ammissibili in linea di principio; tale ragionamento deve essere cassato dalla proposta, in particolare perché la marcatura CE auspicata non implica che il trattamento dei dati personali associato sia lecito.

23. Tuttavia, la conformità agli obblighi giuridici previsti dalla legislazione dell'Unione (compresa quella in materia di protezione dei dati personali) dovrebbe essere un prerequisito per ottenere l'autorizzazione all'immissione sul mercato europeo come prodotto munito della marcatura CE. A tal fine l'EDPB e il GEPD **raccomandano di includere nel capo 2 del titolo III della proposta l'obbligo di garantire la conformità all'RGPD e all'EUDPR**. L'adempimento di tali obblighi sarà verificato (da un organismo di audit indipendente) prima dell'attribuzione della marcatura CE, in conformità del principio di rendicontabilità. Nel contesto di questa valutazione a opera di terzi, assumerà particolare rilevanza la valutazione d'impatto iniziale di competenza del fornitore.

24. Tenendo conto delle complessità derivanti dallo sviluppo dei sistemi di IA, va rilevato che le caratteristiche tecniche di tali sistemi (ad esempio il tipo di approccio all'IA) potrebbero comportare rischi maggiori. Pertanto qualsiasi valutazione del rischio dei sistemi di IA dovrebbe considerare **le caratteristiche tecniche** unitamente ai **casi d'uso specifici e al contesto** in cui tali sistemi operano.

25. Alla luce di quanto precede, l'EDPB e il GEPD raccomandano di specificare nella proposta che **il fornitore** deve effettuare una iniziale valutazione del rischio del sistema di IA in questione **tenendo conto dei casi d'uso** [da specificare nella proposta, ad esempio integrando l'allegato III, punto 1, lettera a), laddove i casi d'uso dei sistemi biometrici di IA non sono menzionati], e che l'**utente** del sistema di IA deve effettuare, nella sua qualità di titolare del trattamento ai sensi della legislazione dell'UE in materia di protezione dei dati (se pertinente), la valutazione d'impatto sulla protezione dei dati come dettagliatamente previsto

([11]) L'Agenzia dell'Unione europea per i diritti fondamentali (FRA) ha già esaminato la necessità di condurre valutazioni d'impatto sui diritti fondamentali nei casi di utilizzo dell'IA o di tecnologie collegate. Nella sua relazione del 2020 «Getting the future right – Artificial intelligence and fundamental rights» (Preparare un futuro giusto: intelligenza artificiale e diritti fondamentali) la FRA ha individuato alcune insidie nascoste nell'utilizzo dell'IA, ad esempio nella strategia predittiva, nelle diagnosi mediche, nei servizi sociali e nella pubblicità mirata, sottolineando che le organizzazioni pubbliche e private dovrebbero eseguire valutazioni del modo in cui l'IA potrebbe nuocere ai diritti fondamentali, al fine di attenuare l'impatto negativo sulle persone.

dall'articolo 35 dell'RGPD, dall'articolo 39 dell'EUDPR e dall'articolo 27 della LED, considerando non soltanto le caratteristiche tecniche e **il caso d'uso**, ma **anche il contesto specifico** in cui l'IA è destinata a operare.

26. Inoltre dovrebbero essere chiariti alcuni dei termini citati nell'allegato III della proposta, come le espressioni «servizi privati essenziali» o il riferimento ai fornitori di piccole dimensioni che utilizzano l'IA per valutare la solvibilità per uso proprio.

2.3 Usi vietati dell'IA

27. L'EDPB e il GEPD ritengono che le **forme di IA invasive** – specialmente quelle che potrebbero violare la dignità umana – debbano essere considerate sistemi di IA vietati a norma dell'articolo 5 della proposta, invece di essere semplicemente classificate «ad alto rischio» nell'allegato III della stessa, come quelle di cui al n. 6. Ciò vale in particolare per le comparazioni di dati che interessano, su larga scala, anche le persone che non sono state o sono state solo in piccola misura oggetto di osservazione da parte della polizia, nonché per i trattamenti non conformi al principio di limitazione delle finalità ai sensi della legislazione in materia di protezione dei dati. L'utilizzo dell'IA nelle attività di polizia e di contrasto richiede regole specifiche, precise, prevedibili e proporzionate che devono tenere conto degli interessi delle persone coinvolte e degli effetti sul funzionamento di una società democratica.

28. L'articolo 5 della proposta rischia di sostenere solo a parole i «valori» e il divieto di sistemi di IA che siano in conflitto con tali valori. Infatti, i criteri citati all'articolo 5 per classificare i sistemi di IA come vietati **limitano l'ambito di applicazione del divieto** in misura tale che il divieto stesso rischia di diventare irrilevante nella pratica [ad esempio: «in un modo che provochi o possa provocare [...] un danno fisico o psicologico» nell'articolo 5, paragrafo 1, lettere a) e b); limiti previsti per le autorità pubbliche nell'articolo 5, paragrafo 1, lettera c); formulazione vaga dei punti i) e ii) della lettera c); limitazione all'identificazione biometrica da remoto «in tempo reale» senza alcuna definizione chiara ecc.].

29. In particolare, l'utilizzo dell'IA a fini di «punteggio sociale», come previsto dall'articolo 5, paragrafo 1, lettera c), della proposta, può essere causa di discriminazione ed è in contrasto con i valori fondamentali dell'UE. La proposta vieta tali pratiche soltanto quando sono applicate «per un determinato periodo di tempo» ovvero «da parte delle autorità pubbliche o per loro conto». Tuttavia, considerato che anche società private, in particolare i media sociali e i fornitori di servizi cloud, possono trattare grandi quantità di dati personali e applicare tali pratiche, **la proposta dovrebbe vietare qualsiasi tipo di punteggio sociale**. Va rilevato che, nel contesto delle attività di contrasto, l'articolo 4 della LED limita già ora in maniera significativa simili attività, quando addirittura non le vieta.

30. L'**identificazione biometrica da remoto** delle persone in spazi accessibili al pubblico comporta un rischio elevato di intrusione nella vita privata delle persone. Pertanto l'EDPB e il GEPD **reputano necessario un approccio più severo**. L'utilizzo di sistemi di IA potrebbe comportare gravi problemi di proporzionalità poiché potrebbe richiedere il trattamento di dati di un numero indiscriminato e sproporzionato di interessati al fine di identificare solo poche persone (ad esempio passeggeri in aeroporti e stazioni ferroviarie). Inoltre, la natura «**senza**

attrito» dei sistemi di identificazione biometrica da remoto comporta problemi di trasparenza e solleva questioni correlate alla base giuridica del trattamento a norma della legislazione dell'UE (la LED, l'RGPD, l'EUDPR e le altre normative applicabili). Restano tuttora irrisolti il problema della corretta informazione delle persone in merito a detto trattamento e la questione dell'esercizio efficace e tempestivo dei loro diritti. Lo stesso vale per le **gravi e irreversibili conseguenze sulla** (ragionevole) **aspettativa dei cittadini di restare anonimi negli spazi accessibili al pubblico**, che comportano direttamente una compromissione dell'esercizio della libertà di espressione, di riunione e di associazione, nonché della libertà di circolazione.

31. L'articolo 5, paragrafo 1, lettera d), della proposta contiene un dettagliato **elenco di casi eccezionali** in cui l'identificazione biometrica da remoto «in tempo reale» in spazi accessibili al pubblico è permessa a fini di attività di contrasto. L'EDPB e il GEPD ritengono che **questo approccio sia viziato** sotto numerosi aspetti, come spiegato di seguito. In primo luogo, non è chiaro quali circostanze dovrebbero essere considerate «ritardi significativi» né in che modo esse possano fungere da fattore di mitigazione, considerando che un sistema di identificazione di massa è in grado di identificare migliaia di persone in pochissime ore. Inoltre, l'invasività del trattamento non sempre dipende dal fatto che l'identificazione sia eseguita in tempo reale oppure no. L'identificazione biometrica da remoto a posteriori nel contesto di una manifestazione di protesta politica può avere un pesante effetto dissuasivo sull'esercizio dei diritti e delle libertà fondamentali, come la libertà di riunione e di associazione e, più in generale, sui principi fondanti della democrazia. In secondo luogo, l'invasività del trattamento non dipende necessariamente dalle sue finalità. L'utilizzo di questo sistema per finalità diverse, come la sicurezza privata, comporta le stesse minacce per i diritti fondamentali al rispetto della vita privata e della vita familiare e alla protezione dei dati personali. Infine, anche con le limitazioni previste il numero potenziale di persone sospette o autori di reati sarà quasi sempre abbastanza elevato da giustificare l'utilizzo continuo di sistemi di IA per individuare tali persone sospette, a dispetto delle ulteriori condizioni di cui all'articolo 5, paragrafi da 2 a 4, della proposta. Il ragionamento alla base della proposta sembra non tenere conto del fatto che, nel monitoraggio di aree all'aperto, gli obblighi previsti dalla legislazione dell'UE in materia di protezione dei dati devono essere adempiuti in riferimento non soltanto alle persone sospette, ma a tutte quelle di fatto monitorate.

32. Per tutti questi motivi l'EDPB e il GEPD **sollecitano l'inclusione di un divieto generale di qualsiasi uso dell'IA a fini di riconoscimento automatico, in spazi accessibili al pubblico, delle caratteristiche umane – come il volto ma anche l'andatura, le impronte digitali, il DNA, la voce, le sequenze di battute su tastiera e altri segnali biometrici o comportamentali – in qualsiasi contesto**. L'attuale approccio della proposta mira a identificare ed elencare tutti i sistemi di IA che dovrebbero essere vietati. Quindi, per ragioni di coerenza, **i sistemi di IA per l'identificazione da remoto su larga scala in spazi online** dovrebbero essere vietati a norma dell'articolo 5 della proposta. Tenendo conto della LED, dell'EUDPR e dell'RGPD, il GEPD e l'EDPB non riescono a comprendere come questo tipo di prassi possa soddisfare i requisiti di necessità e proporzionalità, anche considerando, in ultima analisi, ciò che la CGUE e la CEDU giudicano interferenze accettabili nei diritti fondamentali.

33. Inoltre, l'EDPB e il GEPD **raccomandano di introdurre un divieto** valido sia per le autorità pubbliche sia per i soggetti privati di utilizzare **sistemi di IA che categorizzano le persone in insiemi (*clusters*), a partire dai dati biometrici (ad esempio con il riconoscimento facciale), in base all'etnia, al genere nonché all'orientamento politico o sessuale oppure in base ad altri motivi di discriminazione proibiti a norma dell'articolo 21 della Carta, ovvero** sistemi di IA la cui validità scientifica non è dimostrata o che confliggono direttamente con i valori fondamentali dell'UE [ad esempio i poligrafi, cfr. l'allegato III, punto 6, lettera b), e il punto 7, lettera a)]. Pertanto, la «**categorizzazione biometrica**» dovrebbe essere **vietata a norma dell'articolo 5**.

34. Inoltre, la circostanza per cui è un computer a stabilire o classificare il comportamento futuro di una persona**, indipendentemente dalla libertà di scelta individuale, viola la dignità umana**. I sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali dei rischi posti dalle persone fisiche al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica [cfr. l'allegato III, punto 6, lettera a)], o per prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso [cfr. l'allegato III, punto 6, lettera e)], utilizzati in conformità della finalità prevista, influenzeranno in maniera decisiva i processi decisionali in ambito giudiziario e di polizia, trasformando in tal modo la persona interessata in un oggetto. Questi sistemi di IA che incidono sull'essenza del diritto alla dignità umana dovrebbero essere vietati a norma dell'articolo 5.

35. Inoltre, l'EDPB e il GEPD ritengono che l'utilizzo dell'IA per **dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato**, ad eccezione di taluni casi d'uso ben specificati, ossia per finalità sanitarie o di ricerca (ad esempio pazienti per i quali il riconoscimento delle emozioni è rilevante), sempre applicando idonee tutele e, naturalmente, nel rispetto di tutte le altre condizioni e restrizioni relative alla protezione dei dati, compresa la limitazione delle finalità.

2.4 Sistemi di IA ad alto rischio

2.4.1 Necessità di una valutazione della conformità ex ante da parte di soggetti terzi esterni

36. L'EDPB e il GEPD valutano positivamente il fatto che i sistemi di IA che comportano rischi elevati debbano essere sottoposti a una preventiva valutazione della conformità prima di poter essere immessi sul mercato o altrimenti resi operativi nell'UE. In linea di principio, questo modello normativo è benaccetto in quanto costituisce un buon punto di equilibrio tra la disponibilità all'innovazione e un elevato livello di protezione proattiva dei diritti fondamentali. Per poterlo applicare in ambienti specifici, come i processi decisionali delle istituzioni dei servizi pubblici o in infrastrutture essenziali, è necessario stabilire le modalità con cui esaminare il codice sorgente completo.

37. Tuttavia, l'EDPB e il GEPD invitano ad adattare la procedura di valutazione della conformità di cui all'articolo 43 della proposta in modo tale da **prevedere l'obbligo generale di sottoporre i sistemi di IA ad alto rischio a una valutazione della conformità ex ante da**

parte di terzi. Benché una valutazione della conformità da parte di terzi dei trattamenti ad alto rischio di dati personali non costituisca un requisito a norma dell'RGPD o dell'EUDPR, i rischi posti dai sistemi di IA devono ancora essere compresi nella loro interezza. L'inserimento di una previsione generale di condurre una valutazione obbligatoria della conformità a opera di terzi permetterebbe, quindi, di accrescere ulteriormente la certezza del diritto e la fiducia in tutti i sistemi di IA ad alto rischio.

2.4.2 L'ambito di applicazione del regolamento deve includere anche i sistemi di IA già in uso

38. Ai sensi dell'articolo 43, paragrafo 4, della proposta, i sistemi di IA ad alto rischio dovrebbero essere sottoposti a una nuova procedura di valutazione della conformità dopo ogni modifica sostanziale. È corretto garantire che tali sistemi siano conformi ai requisiti del regolamento sull'IA durante il loro intero ciclo di vita. I sistemi di IA che sono stati immessi sul mercato o messi in servizio prima dell'applicazione del regolamento proposto (ovvero 12 mesi dopo, nel caso dei sistemi IT su larga scala elencati nell'allegato IX) sono esclusi dall'ambito di applicazione, a meno che la loro progettazione o la finalità prevista abbiano subito una «modifica significativa» (articolo 83).

39. Nondimeno, la soglia per le «modifiche significative» non è definita chiaramente. Il considerando 66 della proposta specifica una soglia più bassa per la nuova valutazione della conformità «ogniqualvolta intervenga una modifica che possa incidere sulla conformità». Sarebbe opportuno che l'articolo 83 prevedesse una soglia analoga, quanto meno per i sistemi di IA ad alto rischio. Inoltre, al fine di ovviare a qualsiasi lacuna in materia di protezione, è necessario che anche i sistemi di IA già istituiti e in funzione – dopo una determinata fase di applicazione – siano conformi a tutti i requisiti del regolamento sull'IA.

40. La sicurezza dei sistemi di IA risente anche delle molteplici possibilità di trattamento dei dati personali e dei rischi esterni. Il riferimento dell'articolo 83 a «una modifica significativa della progettazione o della finalità prevista» non comprende anche le modifiche nei rischi esterni. Pertanto, l'articolo 83 della proposta dovrebbe includere anche un riferimento ai cambiamenti degli scenari delle minacce dovuti a rischi esterni, ad esempio attacchi informatici, attacchi ostili e reclami fondati di consumatori.

41. Inoltre, dato che l'applicazione delle disposizioni dovrebbe iniziare 24 mesi dopo l'entrata in vigore del futuro regolamento, il GEPD e l'EDPB non reputano appropriato esonerare i sistemi di IA già immessi sul mercato per un periodo di tempo ancora più lungo. Benché la proposta preveda anche che i requisiti del regolamento siano presi in considerazione nella valutazione di ciascun sistema IT su larga scala, come stabilito dagli atti legislativi elencati nell'allegato IX, l'EDPB e il GEPD ritengono che i requisiti relativi alla messa in servizio dei sistemi di IA dovrebbero essere applicabili a decorrere dalla data di applicazione del futuro regolamento.

2.5 Governance e comitato europeo per l'IA

2.5.1 Governance

42. L'EDPB e il GEPD valutano positivamente la designazione del GEPD come autorità competente e autorità di vigilanza del mercato preposta alla sorveglianza sulle istituzioni, le agenzie e gli organi dell'Unione quando tali entità rientrano nell'ambito di applicazione della proposta. Il GEPD è pronto a svolgere il suo nuovo ruolo di organismo di regolamentazione in materia di IA per l'amministrazione pubblica dell'UE. D'altro canto, il suo ruolo e i suoi compiti non sono indicati in modo sufficientemente dettagliato e dovrebbero pertanto essere precisati meglio nella proposta, con specifico riferimento al suo ruolo di autorità di vigilanza del mercato.

43. L'EDPB e il GEPD prendono atto delle risorse finanziarie che la proposta assegna al comitato e al GEPD quando esso funge da organismo di notifica. Tuttavia, l'adempimento delle nuove funzioni previste per il GEPD in qualità di organismo notificato richiederebbe risorse umane e finanziarie considerevolmente maggiori.

44. Questo perché, in primo luogo, il disposto dell'articolo 63, paragrafo 6, pur stabilendo che il GEPD «agisce in qualità di autorità di vigilanza del mercato» per le istituzioni, le agenzie e gli organismi dell'Unione nei casi in cui tali entità rientrino nell'ambito di applicazione della proposta, non chiarisce se il GEPD debba essere considerato a pieno titolo un'«autorità di vigilanza del mercato» ai sensi del regolamento (UE) 2019/1020. Tale circostanza solleva dubbi circa le funzioni e i poteri del GEPD nella sua attività concreta. In secondo luogo, e presupponendo che la precedente questione riceva una risposta affermativa, non è chiaro come il ruolo del GEPD, quale previsto dall'EUDPR, possa conciliarsi con il compito di cui all'articolo 11 del regolamento (UE) 2019/1020, che comprende «l'efficace vigilanza del mercato nei rispettivi territori per i prodotti messi in vendita [sia] online» ovvero «controlli fisici e di laboratorio basandosi su campioni congrui». Sussiste il rischio che l'assunzione della nuova serie di compiti in assenza di ulteriori precisazioni nella proposta possa mettere a rischio l'adempimento degli obblighi del GEPD in quanto garante della protezione dei dati.

45. Tuttavia, l'EDPB e il GEPD sottolineano che al momento attuale risultano essere poco chiare alcune disposizioni della proposta, che definiscono i compiti e i poteri delle differenti autorità competenti a norma del regolamento sull'IA, i loro rapporti reciproci, la loro natura e la garanzia della loro indipendenza. Mentre il regolamento (UE) 2019/1020 stabilisce che l'autorità di vigilanza del mercato deve essere indipendente, la proposta di regolamento non soltanto non impone alle autorità di controllo di essere indipendenti, ma addirittura le obbliga a relazionare alla Commissione in merito a taluni compiti svolti dalle autorità di vigilanza del mercato, che possono essere istituzioni differenti. La proposta stabilisce altresì che le autorità competenti per la protezione dei dati fungeranno da autorità di vigilanza del mercato per i sistemi di IA utilizzati a fini di attività di contrasto (articolo 63, paragrafo 5); ciò significa che anch'esse saranno sottoposte, eventualmente tramite la rispettiva autorità nazionale di controllo, agli obblighi di segnalazione alla Commissione (articolo 63, paragrafo 2), il che risulta essere incompatibile con la loro indipendenza.

46. Pertanto l'EDPB e il GEPD ritengono che le succitate disposizioni debbano essere chiarite al fine di garantirne la coerenza con il regolamento (UE) 2019/2010, l'EUDPR e l'RGPD, e che la proposta dovrebbe prevedere chiaramente che le autorità di controllo di cui al regolamento sull'IA debbano essere completamente indipendenti nell'esecuzione dei propri compiti, poiché questa sarebbe una garanzia essenziale ai fini di una supervisione e un'applicazione corrette del futuro regolamento.

47. Inoltre, l'EDPB e il GEPD desiderano rammentare che le autorità per la protezione dei dati stanno già applicando l'RGPD, l'EUDPR e la LED per quanto riguarda i sistemi di IA che interessano i dati personali, al fine di garantire la tutela dei diritti fondamentali e, più nello specifico, il diritto alla protezione dei dati. Pertanto, come richiesto dalla proposta alle autorità nazionali di controllo, le autorità per la protezione dei dati dispongono già, in una certa misura, di conoscenze in materia di tecnologie basate sull'IA, di dati e di sistemi di elaborazione degli stessi nonché di diritti fondamentali, e dispongono altresì di competenze nella valutazione dei rischi che le nuove tecnologie comportano per tali diritti fondamentali. Inoltre, se i sistemi di IA si basano sul trattamento di dati personali o li trattano, le disposizioni della proposta sono direttamente interconnesse con il quadro giuridico per la protezione dei dati: sarà questo il caso della maggior parte dei sistemi di IA compresi nell'ambito di applicazione del regolamento. Ne consegue che vi saranno interconnessioni di competenze tra le autorità di controllo previste dalla proposta e le autorità per la protezione dei dati.

48. Pertanto, la designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe un approccio normativo più armonizzato e contribuirebbe all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri. Inoltre, tutte le parti interessate della catena di valore dell'IA trarrebbero beneficio dall'esistenza di un punto di contatto unico per tutte le operazioni di trattamento dei dati personali che rientrano nell'ambito di applicazione della proposta, oltre che dalla limitazione delle interazioni tra due differenti organismi di regolamentazione dei trattamenti che sono sottoposti alla proposta e all'RGPD. Di conseguenza, l'EDPB e il GEPD ritengono che **le autorità per la protezione dei dati dovrebbero essere designate come autorità nazionali di controllo ai sensi dell'articolo 59 della proposta**.

49. In ogni caso, nella misura in cui la proposta contiene regole specifiche per la protezione delle persone fisiche con riguardo al trattamento dei dati personali adottate sulla base dell'articolo 16 del TFUE, la conformità a tali regole, in particolare alle restrizioni dell'utilizzo di sistemi di IA per l'identificazione biometrica da remoto «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, **dev'essere sottoposta al controllo di autorità indipendenti**.

50. La proposta, però, non prevede alcuna disposizione esplicita in forza della quale la competenza di garantire la conformità a queste regole spetterebbe al controllo da parte di autorità indipendenti. L'unico riferimento alle autorità di controllo competenti per la protezione dei dati a norma dell'RGPD o della LED è contenuto nell'articolo 63, paragrafo 5, della proposta, ma solo in qualità di organi di «vigilanza del mercato» e in alternativa con alcune altre autorità. L'EDPB e il GEPD ritengono che questa struttura non garantisca la conformità all'obbligo di

controllo da parte di autorità indipendenti sancito dall'articolo 16, paragrafo 2, del TFUE e dall'articolo 8 della Carta.

2.5.2 Il comitato europeo per l'IA

51. La proposta istituisce un comitato europeo per l'intelligenza artificiale (CEIA). L'EDPB e il GEPD riconoscono la necessità di un'applicazione coerente e armonizzata del quadro proposto nonché del coinvolgimento di esperti indipendenti nell'elaborazione della politica dell'UE in materia di IA. Allo stesso tempo la proposta prevede di assegnare un ruolo predominante alla Commissione. Infatti, la Commissione non soltanto farebbe parte del CEIA, ma lo presiederebbe e vi deterrebbe anche un diritto di veto sull'adozione del suo regolamento interno. Ciò è in contrasto con la necessità di un organismo europeo per l'IA che sia indipendente da qualsiasi influenza politica. Pertanto, l'EDPB e il GEPD ritengono che il futuro regolamento sull'IA dovrebbe attribuire **maggiore autonomia al CEIA** per consentirgli di garantire effettivamente un'applicazione coerente del regolamento in tutto il mercato unico.

52. L'EDPB e il GEPD rilevano altresì che al CEIA non è attribuito alcun potere in merito all'applicazione del regolamento proposto. Eppure, vista la diffusione dei sistemi di IA nel mercato unico e la probabilità che si verifichino casi transfrontalieri, è imprescindibile assicurare un'applicazione armonizzata e una corretta ripartizione delle competenze tra le autorità di controllo nazionali. L'EDPB e il GEPD raccomandano pertanto di specificare nel futuro regolamento sull'IA i meccanismi di cooperazione tra le autorità di controllo nazionali. L'EDPB e il GEPD suggeriscono di imporre un meccanismo in grado di garantire un punto di contatto unico per le persone fisiche interessate dalla legislazione e per le società, per ciascun sistema di IA, e, nel caso delle organizzazioni la cui attività coinvolge oltre la metà degli Stati membri dell'UE, di autorizzare il CEIA a designare l'autorità nazionale che sarà responsabile dell'applicazione del regolamento sull'IA per il sistema di IA in questione.

53. Inoltre, tenendo conto della natura indipendente delle autorità che costituiranno il comitato, esso deve avere il potere di agire di propria iniziativa e non limitandosi a fornire consulenza e assistenza alla Commissione. L'EDPB e il GEPD sottolineano dunque la necessità di ampliare la missione affidata al comitato, la quale, peraltro, non corrisponde ai compiti elencati nella proposta.

54. Per conseguire le finalità indicate, il **CEIA deve disporre di poteri sufficienti e adeguati** e se ne dovrebbe chiarire lo status giuridico. In particolare, affinché l'ambito di applicazione materiale del futuro regolamento mantenga la propria pertinenza, appare necessario coinvolgere nella sua elaborazione le autorità preposte alla relativa applicazione. Pertanto, l'EDPB e il GEPD raccomandano che il CEIA sia investito dei poteri di proporre alla Commissione modifiche dell'allegato I, che definisce le tecniche e gli approcci dell'IA, e dell'allegato III, che elenca i sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2. Inoltre, il CEIA dovrebbe essere consultato dalla Commissione prima di qualsiasi modifica di tali allegati.

55. L'articolo 57, paragrafo 4, della proposta prevede la possibilità di scambi tra il comitato e altri organismi, uffici, agenzie e gruppi consultivi dell'Unione. In virtù della sua precedente attività

nel settore dell'IA e della competenza in materia di diritti umani, l'EDPB e il GEPD raccomandano di considerare l'inclusione dell'Agenzia per i diritti fondamentali tra gli osservatori del comitato.

3 INTERAZIONE CON IL QUADRO PER LA PROTEZIONE DEI DATI

3.1 Rapporto tra la proposta e la vigente legislazione dell'UE in materia di protezione dei dati

56. Un rapporto chiaramente definito tra la proposta e la vigente legislazione in materia di protezione dei dati rappresenta un prerequisito essenziale per assicurare e preservare il rispetto e l'applicazione dell'*acquis* dell'UE nel campo della protezione dei dati personali. Detta legislazione, in particolare l'RGPD, l'EUDPR e la LED, dev'essere considerata un prerequisito sulla cui base si possono elaborare ulteriori proposte legislative senza incidere sulle disposizioni esistenti o interferire con esse, anche in riferimento alla competenza delle autorità di controllo e alla governance.

57. Pertanto, a parere dell'EDPB e del GEPD è importante evitare chiaramente qualsiasi incoerenza ed eventuali conflitti con l'RGPD, l'EUDPR e la LED, non soltanto per garantire la certezza del diritto ma anche per evitare che la proposta abbia l'effetto di compromettere, direttamente o indirettamente, il diritto fondamentale alla protezione dei dati personali quale stabilito dall'articolo 16 del TFUE e dall'articolo 8 della Carta.

58. In particolare, macchine in grado di apprendere autonomamente sarebbero in grado di proteggere i dati personali delle persone fisiche soltanto se tale capacità fosse integrata fin dalla progettazione. È essenziale garantire anche la possibilità immediata di esercitare i diritti delle persone fisiche a norma dell'articolo 22 dell'RGPD (processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) o dell'articolo 23 dell'EUDPR, a prescindere dalle finalità del trattamento. A tale riguardo, i sistemi di IA devono assicurare fin dall'inizio altri diritti degli interessati, correlati a quelli alla cancellazione e alla rettifica conformemente alla legislazione in materia di protezione dei dati, a prescindere dall'approccio scelto per l'IA o dall'architettura tecnica.

59. L'utilizzo di dati personali per l'apprendimento da parte dei sistemi di IA può ingenerare distorsioni nei modelli decisionali al centro del sistema di IA. Per tali motivi dovrebbero essere richieste varie garanzie, in particolare una sorveglianza umana qualificata di tali processi, al fine di assicurare il rispetto e la tutela dei diritti degli interessati ed evitare ogni e qualsiasi conseguenza negativa per le persone. Le autorità competenti dovrebbero altresì essere in grado di proporre orientamenti per valutare le distorsioni presenti nei sistemi di IA e coadiuvare l'esecuzione della sorveglianza umana.

60. Gli interessati dovrebbero essere sempre informati dell'eventuale utilizzo dei loro dati a fini di apprendimento dell'IA e/o di previsione da parte dell'IA e della base giuridica di tale trattamento, nonché ricevere una spiegazione generale della logica (procedura) e dell'ambito

di applicazione del sistema di IA. A tale riguardo, i diritti delle persone alla limitazione del trattamento (articolo 18 dell'RGPD e articolo 20 dell'EUDPR) e alla cancellazione dei dati (articolo 16 dell'RGPD e articolo 19 dell'EUDPR) dovrebbero essere sempre garantiti in questi casi. Inoltre, il titolare del trattamento dovrebbe essere esplicitamente tenuto a informare l'interessato dei periodi previsti per l'esercizio del diritto di opposizione, limitazione, cancellazione dei dati ecc. Il sistema di IA dev'essere in grado di soddisfare tutti i requisiti per la protezione dei dati mediante idonee misure tecniche e organizzative. Il diritto alla spiegazione dovrebbe permettere una maggiore trasparenza.

3.2 Spazio di sperimentazione e ulteriore trattamento (articoli 53 e 54 della proposta)

61. Nel rispetto dei limiti giuridici ed etici esistenti, è importante promuovere l'innovazione europea mediante strumenti quali gli spazi di sperimentazione. Uno spazio di sperimentazione offre l'opportunità di fornire le tutele necessarie per creare un clima di fiducia e affidabilità nei confronti dei sistemi di IA. In ambienti complessi può essere difficile per gli operatori dell'IA ponderare adeguatamente tutti gli interessi in gioco. Specialmente nelle piccole e medie imprese con risorse limitate, operare in uno spazio di sperimentazione normativa può permettere di acquisire nozioni più velocemente e, quindi, di stimolare l'innovazione.

62. L'articolo 53, paragrafo 3, della proposta afferma che gli spazi di sperimentazione lasciano impregiudicati i poteri correttivi e di controllo. Nonostante l'utilità di tale precisazione, è nondimeno necessario definire linee di indirizzo o orientamenti sulle modalità di un corretto bilanciamento tra l'esercizio dei poteri tipici di un'autorità di controllo, da un lato, e, dall'altro, la definizione di orientamenti dettagliati tramite uno spazio di sperimentazione.

63. L'articolo 53, paragrafo 6, spiega che le modalità e le condizioni di funzionamento degli spazi di sperimentazione saranno stabiliti in atti di esecuzione. È importante definire orientamenti specifici al fine di garantire la coerenza e il sostegno nell'istituzione e nel funzionamento degli spazi di sperimentazione. Tuttavia, atti di esecuzione vincolanti potrebbero limitare la capacità di ciascuno Stato membro di adattare lo spazio di sperimentazione secondo le proprie esigenze e le prassi locali. Pertanto l'EDPB e il GEPD raccomandano piuttosto che il CEIA fornisca orientamenti per gli spazi di sperimentazione.

64. L'articolo 54 della proposta intende stabilire una base giuridica dell'ulteriore trattamento dei dati personali per lo sviluppo, nello spazio di sperimentazione normativa per l'IA, di determinati sistemi di IA nell'interesse pubblico. Rimane incerto, tuttavia, il rapporto tra l'articolo 54, paragrafo 1, della proposta e l'articolo 54, paragrafo 2, nonché il considerando 41 della proposta e, quindi, anche la vigente legislazione dell'UE in materia di protezione dei dati. Ma l'RGPD e l'EUDPR già prevedono una base consolidata per l'«ulteriore trattamento». In particolare nei casi in cui è nell'interesse pubblico consentire un ulteriore trattamento, la ricerca di un punto di equilibrio tra gli interessi del titolare del trattamento e quelli dell'interessato non deve ostacolare l'innovazione. L'articolo 54 della proposta nella sua versione attuale non affronta due questioni importanti: a) in quali circostanze e con quali criteri (aggiuntivi) sono ponderati gli interessi degli interessati; b) se questi sistemi di IA saranno utilizzati esclusivamente all'interno dello spazio di sperimentazione. L'EDPB e il GEPD valutano

positivamente l'obbligo di disciplinare mediante norme dell'Unione o dello Stato membro il trattamento dei dati personali raccolti a norma della LED in uno spazio di sperimentazione; raccomandano, tuttavia, di specificare ulteriormente le finalità in maniera tale da garantire la conformità all'RGPD e all'EUDPR, specialmente chiarendo che la base giuridica di questi spazi di sperimentazione dovrebbe essere conforme ai requisiti di cui all'articolo 23, paragrafo 2, dell'RGPD e all'articolo 25 dell'EUDPR, nonché precisando che qualsiasi utilizzo dello spazio di sperimentazione deve essere sottoposto ad accurata valutazione. Lo stesso vale anche per l'elenco completo delle condizioni di cui all'articolo 54, paragrafo 1, lettere da b) a j).

65. Alcune considerazioni aggiuntive sul riutilizzo dei dati contenute nell'articolo 54 della proposta indicano che per operare in uno spazio di sperimentazione sono necessarie molte risorse e che pertanto è realistico presupporre che solo un numero esiguo di imprese avrebbe la possibilità di partecipare. Ma la partecipazione allo spazio di sperimentazione potrebbe offrire un vantaggio in termini di competitività. Per consentire il riutilizzo dei dati è necessario valutare con attenzione le modalità di selezione dei partecipanti al fine di garantire che essi siano compresi nell'ambito di applicazione e di evitare disparità di trattamento. L'EDPB e il GEPD temono che la possibilità di riutilizzare i dati nel quadro dello spazio di sperimentazione comporti uno scostamento dall'approccio basato sulla responsabilizzazione previsto dall'RGPD, in cui è il titolare del trattamento, non l'autorità competente, a dover dimostrare la conformità.

66. Inoltre, l'EDPB e il GEPD ritengono che, alla luce degli obiettivi degli spazi di sperimentazione, ossia sviluppare, testare e convalidare sistemi di IA, tali spazi non possano rientrare nell'ambito di applicazione della LED. Anche se la LED prevede il riutilizzo dei dati a fini di ricerca scientifica, i dati trattati per tale finalità secondaria saranno soggetti alle disposizioni del RGPD o dell'EUDPR, non più della LED.

67. Non è chiaro che cosa sarà compreso in uno spazio di sperimentazione normativa. Sorge l'interrogativo se lo spazio di sperimentazione normativa proposto includa un'infrastruttura informatica in ciascuno Stato membro, con alcune basi giuridiche aggiuntive per l'ulteriore trattamento, o se esso si limiti a organizzare l'accesso a competenze e orientamenti normativi. L'EDPB e il GEPD sollecitano il legislatore a precisare questo concetto nella proposta e a indicare chiaramente nella medesima che lo spazio di sperimentazione normativa non implica per le autorità competenti l'obbligo di fornire l'infrastruttura tecnica. In ogni caso, è necessario fornire alle autorità competenti le risorse umane e finanziarie in conformità a tale chiarimento.

68. Infine, l'EDPB e il GEPD desiderano far presente lo sviluppo dei sistemi di IA transfrontalieri che saranno a disposizione del mercato unico digitale europeo nel suo complesso. Nel caso di questi sistemi di IA, lo spazio di sperimentazione normativa in quanto strumento di innovazione non dovrebbe diventare un ostacolo allo sviluppo transfrontaliero. Pertanto l'EDPB e il GEPD raccomandano un approccio transfrontaliero coordinato che sia in ogni caso sufficientemente accessibile a livello nazionale per tutte le PMI e offra un quadro comune in tutta Europa senza essere troppo restrittivo. È necessario trovare un punto di equilibrio tra il

coordinamento europeo e le procedure nazionali al fine di evitare un'applicazione conflittuale del futuro regolamento sull'IA, che ostacolerebbe l'innovazione nell'intera Unione europea.

3.3 Trasparenza

69. L'EDPB e il GEPD valutano positivamente il fatto che i sistemi di IA ad alto rischio saranno registrati in una banca dati pubblica (come previsto negli articoli 51 e 60 della proposta). Tale banca dati dovrebbe essere considerata un'opportunità per fornire al pubblico informazioni sull'ambito di applicazione del sistema di IA e sui difetti e gli incidenti noti che potrebbero comprometterne il funzionamento, nonché sui rimedi adottati dai fornitori per porvi rimedio.

70. Un principio fondamentale della democrazia è il ricorso a un meccanismo di bilanciamento fra istanze contrapposte. Pertanto, la non applicabilità dell'obbligo di trasparenza ai sistemi di IA usati a fini di prevenzione, accertamento, indagine e perseguimento di reati costituisce un'eccezione di portata troppo ampia. Occorre fare una distinzione tra i sistemi di IA usati a fini di accertamento e prevenzione e quelli mirati all'indagine e al perseguimento di reati. Le tutele per le attività di prevenzione e accertamento devono essere più solide in considerazione della presunzione di innocenza. Inoltre, l'EDPB e il GEPD deplorano l'assenza di caveat nella proposta, assenza che potrebbe essere interpretata come un via libera all'utilizzo anche di sistemi o applicazioni di IA ad alto rischio non validati.

71. Nei casi in cui, anche in una democrazia ben funzionante, per motivi di segretezza è possibile garantire al pubblico soltanto poca o nessuna trasparenza, dovrebbero essere messe in atto tutele; inoltre, i sistemi di IA citati dovrebbero essere registrati presso l'autorità di controllo competente assicurando a quest'ultima la trasparenza.

72. Garantire la trasparenza nei sistemi di IA è un obiettivo molto difficile da conseguire. L'approccio interamente quantitativo di molti sistemi di IA al processo decisionale, che è intrinsecamente diverso dall'approccio umano fondato principalmente sul ragionamento teorico e per nessi causali, può confliggere con la necessità di ottenere una previa spiegazione comprensibile dei risultati prodotti dalla macchina. Il regolamento dovrebbe promuovere modalità nuove, più proattive e tempestive per informare gli utenti dei sistemi di IA in merito allo status (decisionale) in cui si trova il sistema in ogni momento, predisponendo allarmi rapidi su risultati potenzialmente nocivi affinché le persone i cui diritti e le cui libertà potrebbero essere compromessi dalle autonome decisioni della macchina siano in grado di reagire o impugnare le decisioni in questione.

3.4 Trattamento di categorie particolari di dati e dati relativi a reati

73. Il trattamento di categorie particolari di dati a fini di attività di contrasto è disciplinato dalle disposizioni del quadro dell'UE in materia di protezione dei dati, compresa la LED e le rispettive trasposizioni a livello nazionale. Nel considerando 41 si afferma che la proposta non dovrebbe essere intesa come un fondamento giuridico generale per il trattamento dei dati personali, comprese le relative categorie particolari. Allo stesso tempo, però, l'articolo 10, paragrafo 5, della proposta così recita: «i fornitori di tali sistemi possono trattare categorie particolari di dati personali». Inoltre, questa stessa disposizione prescrive tutele aggiuntive, di cui cita anche alcuni

esempi. Così facendo, la proposta sembra interferire con l'applicazione dell'RDPD, della LED e dell'EUDPR. Pur valutando positivamente il tentativo di prevedere tutele adeguate, l'EDPB e il GEPD ritengono necessario un approccio normativo più coerente poiché le attuali disposizioni non sembrano essere sufficientemente chiare per poter costituire una base giuridica per il trattamento di categorie particolari di dati e devono essere integrate da misure di tutela supplementari tuttora da valutare. Inoltre, nel caso dei dati personali raccolti mediante trattamenti che ricadono nell'ambito di applicazione della LED, si dovranno considerare possibili tutele e limitazioni aggiuntive derivanti dalla trasposizione della LED nelle legislazioni nazionali.

3.5 Meccanismi di conformità

3.5.1 Certificazione

74. Uno dei pilastri principali della proposta è la certificazione. Il sistema di certificazione delineato nella proposta si fonda sull'intervento di più soggetti (autorità di notifica/organismi notificati/Commissione) e su una valutazione della conformità/un meccanismo di certificazione che comprende i requisiti obbligatori applicabili ai sistemi di IA ad alto rischio, nonché sulle norme armonizzate europee di cui al regolamento n. 1025/2012 e sulle specifiche comuni da definire a cura della Commissione. Questo meccanismo è diverso dal sistema di certificazione finalizzato a garantire la conformità alle regole e ai principi per la protezione dei dati di cui agli articoli 42 e 43 dell'RGPD. Tuttavia, non è chiaro in quale modo i certificati emessi da organismi notificati ai sensi della proposta possano interfacciarsi con le certificazioni, i sigilli e le marcature relativi alla protezione dei dati previsti dall'RGPD, diversamente da quanto stabilito per altri tipi di certificazioni [cfr. l'articolo 42, paragrafo 2, per le certificazioni emesse a norma del regolamento (UE) 2019/881].

75. Nella misura in cui i sistemi di IA ad alto rischio si basano sul trattamento di dati personali o li trattano per svolgere le proprie funzioni, queste incongruenze possono compromettere la certezza del diritto per tutti gli organismi interessati poiché possono generare situazioni in cui i sistemi di IA certificati ai sensi della proposta e muniti della marcatura CE di conformità potrebbero essere utilizzati, una volta immessi sul mercato o messi in servizio, in modalità non conformi alle regole e ai principi della protezione dei dati.

76. La proposta è priva di un chiaro collegamento con la legislazione in materia di protezione dei dati e con altre normative dell'UE e degli Stati membri applicabili a ciascuna «area» dei sistemi di IA ad alto rischio elencati nell'allegato III. In particolare, la proposta dovrebbe includere i principi di minimizzazione dei dati e della protezione dei dati fin dalla progettazione fra gli elementi da considerare prima di ottenere la marcatura CE, vista la possibilità di un elevato livello di interferenza dei sistemi di IA ad alto rischio nei diritti fondamentali alla tutela della vita privata e alla protezione dei dati personali, nonché l'esigenza di garantire un elevato livello di fiducia nel sistema di IA. Pertanto l'EDPB e il GEPD raccomandano di modificare la proposta in modo tale da chiarire il rapporto tra i certificati emessi a norma del regolamento in questione e le certificazioni, i sigilli e le marcature relativi alla protezione dei dati. Infine, le autorità per la protezione dei dati dovrebbero essere coinvolte nella preparazione e nella definizione di norme armonizzate e specifiche comuni.

77. In riferimento all'articolo 43 della proposta concernente la valutazione della conformità, la deroga alla procedura di valutazione della conformità di cui all'articolo 47 sembra essere alquanto ampia e comprende un numero elevato di eccezioni, ad esempio motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente e dei principali beni industriali e infrastrutturali. L'EDPB e il GEPD propongono ai legislatori di ridurre il numero di tali eccezioni.

3.5.2 Codici di condotta

78. In conformità dell'articolo 69 della proposta, la Commissione e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria da parte dei fornitori di sistemi di IA non ad alto rischio dei requisiti applicabili ai sistemi di IA ad alto rischio, oltre a requisiti supplementari. In linea con il considerando 78 dell'RGPD, l'EDPB e il GEPD raccomandano di individuare e definire sinergie tra detti strumenti e i codici di condotta previsti dall'RGPD a sostegno della conformità della protezione dei dati. In tale contesto è importante chiarire se la protezione dei dati personali debba essere considerata tra i «requisiti supplementari» che possono essere oggetto dei codici di condotta di cui all'articolo 69, paragrafo 2. È importante anche garantire che le «specifiche e soluzioni tecniche» oggetto dei codici di condotta di cui all'articolo 69, paragrafo 1, destinate a promuovere la conformità ai requisiti della proposta di regolamento sull'IA, non confliggano con le regole e i principi dell'RGPD e dell'EUDPR. In tal modo, l'adesione dei fornitori di sistemi di IA non ad alto rischio a questi strumenti – nella misura in cui tali sistemi si basano sul trattamento di dati personali o li trattano per svolgere le proprie funzioni – rappresenterebbe un valore aggiunto poiché garantirebbe che il titolare del trattamento e i responsabili del trattamento siano in grado di ottemperare ai rispettivi obblighi in materia di protezione dei dati quando utilizzano questi sistemi.

79. Allo stesso tempo, il quadro giuridico per un'IA affidabile risulterebbe integrato dall'introduzione dei codici di condotta e si promuoverebbe in tal modo la fiducia in un utilizzo di questa tecnologia sicuro, conforme alla legge e rispettoso dei diritti fondamentali. Tuttavia, la progettazione di tali strumenti dovrebbe essere potenziata prevedendo meccanismi atti a verificare che i suddetti codici forniscano «specifiche e soluzioni tecniche» efficaci e stabiliscano «obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi» come parte integrante dei codici stessi. Inoltre, l'assenza di qualsiasi riferimento a meccanismi di monitoraggio (obbligatori) per i codici di condotta, intesi a verificare che i fornitori di sistemi di IA non ad alto rischio si conformino alle rispettive disposizioni, nonché la possibilità per i singoli fornitori di redigere (e applicare essi stessi) i suddetti codici (cfr. la sezione 5.2.7 della relazione) potrebbero indebolire ulteriormente l'efficacia e l'applicabilità di questi strumenti.

80. Infine, l'EDPB e il GEPD chiedono chiarimenti in merito alle iniziative che la Commissione può prevedere, ai sensi del considerando 81 della proposta, «per agevolare la riduzione degli ostacoli tecnici allo scambio transfrontaliero di dati per lo sviluppo dell'IA».

4 CONCLUSIONE

81. Pur valutando positivamente la proposta della Commissione e ritenendo che un regolamento quale quello proposto sia necessario per garantire i diritti fondamentali dei cittadini e dei residenti dell'UE, l'EDPB e il GEPD sono del parere che la proposta necessiti di adattamenti sotto diversi aspetti al fine di garantirne applicabilità ed efficienza.

82. Alla luce della complessità della proposta e delle questioni che essa intende affrontare, è ancora lungo il percorso da compiere affinché dalla proposta possa scaturire un quadro giuridico ben funzionante, in grado di integrare efficacemente l'RGPD per quanto attiene alla protezione dei diritti umani fondamentali, promuovendo nel contempo l'innovazione. L'EDPB e il GEPD restano a disposizione per continuare a offrire il proprio sostegno in questo percorso.

Bruxelles, 18 giugno 2021

Per il comitato europeo per la protezione dei dati	Per il Garante europeo della protezione dei dati
La Presidente	Il Garante
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI