Consiglio dell'Unione europea

Bruxelles, 12 settembre 2022
(OR. en)

12302/22

Fascicolo interistituzionale: 2021/0106(COD)

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

PARERE DEL SERVIZIO GIURIDICO[1]

Origine:	Servizio giuridico
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale – Adeguatezza delle basi giuridiche degli articoli 114 e 16 TFUE in relazione alle disposizioni applicabili alle autorità di contrasto e giudiziarie

I. INTRODUZIONE

1. La proposta di regolamento stabilisce regole armonizzate per l'immissione sul mercato e la messa in servizio di sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione ("proposta di regolamento")[2].

[1] Il presente documento contiene una consulenza legale tutelata dall'articolo 4, paragrafo 2 del regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione, e non resa accessibile al pubblico dal Consiglio dell'Unione europea. Il Consiglio si riserva tutti i diritti di legge riguardo a qualsiasi pubblicazione non autorizzata.

[2] Doc. 8115/21.

2. Nella riunione del gruppo "Telecomunicazioni e società dell'informazione" del 7 aprile 2022, il servizio giuridico del Consiglio ("SGC") è intervenuto sulla questione dell'adeguatezza della doppia base giuridica (articoli 16 e 114 TFUE) per la proposta di regolamento sui sistemi di intelligenza artificiale ("sistemi di IA"). Le spiegazioni hanno confermato che gli articoli 16 e 114 TFUE sono le basi giuridiche corrette per la proposta e che il ricorso all'articolo 87, paragrafo 2, TFUE, anziché all'articolo 114 TFUE, non è appropriato. Su richiesta del gruppo, il presente parere riporta per iscritto e sviluppa ulteriormente l'intervento tenuto dal rappresentante dell'SGC nel corso della medesima riunione.

3. I sistemi di IA sono definiti all'articolo 3, paragrafo 1, della proposta di regolamento. In generale, corrispondono a taluni tipi di software. La proposta di regolamento si applica sia ai fornitori che immettono sul mercato sistemi di IA che ai fornitori che mettono in servizio sistemi di IA. Inoltre, la proposta di regolamento si applica anche agli utenti. Un fornitore può essere una persona fisica o giuridica o un'autorità pubblica/un organismo pubblico che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o di metterlo in servizio con il proprio nome o marchio. Un utente può essere una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità.

4. In base alle definizioni di cui all'articolo 3, le autorità di contrasto e le autorità giudiziarie potrebbero qualificarsi come fornitori e/o utenti di un sistema di IA. I sistemi di IA la cui finalità prevista, quale definita dal fornitore, sia l'attività di contrasto o l'amministrazione della giustizia sono classificati come sistemi ad alto rischio ai sensi dell'allegato III. In quanto tali, sono soggetti a requisiti essenziali (gestione dei rischi, prove, governance dei dati, documentazione tecnica, trasparenza, sorveglianza umana, accuratezza, robustezza e cibersicurezza) e a obblighi (quali sistemi di gestione della qualità, documentazione tecnica, valutazione della conformità, misure correttive, dovere di informazione, obblighi di importatori e distributori), nonché a norme e valutazione della conformità. Tali regole armonizzate si ispirano a quelle che si applicano alla sicurezza dei prodotti nella direttiva 2006/42/CE (macchine)[3] e nel regolamento (UE) 2017/745 (dispositivi medici)[4].

5. Per quanto riguarda i sistemi di IA che comportano l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, essi rientrano nella categoria dei sistemi di IA vietati. Tale divieto di utilizzo dei sistemi di IA è tuttavia soggetto a eccezioni. L'uso di tali sistemi può infatti essere autorizzato o meno dagli Stati membri. Se i sistemi sono autorizzati, sono soggetti a restrizioni e tutele dettagliate per limitarne l'uso allo stretto necessario e per garantire il diritto fondamentale alla protezione dei dati personali. Tali restrizioni e tutele sono previste nella proposta di regolamento sulla base dell'articolo 16 del trattato sul funzionamento dell'Unione europea ("TFUE") e devono essere integrate dal diritto nazionale. L'articolo 5, paragrafo 1, lettera d), e paragrafi 2, 3 e 4 della proposta di regolamento costituiscono una *lex specialis* rispetto alla direttiva 2016/680 (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie), che è stata adottata sulla base dell'articolo 16, paragrafo 2, TFUE.

---

[3] Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24).

[4] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

Conformemente all'articolo 5, paragrafo 1, lettera d), gli obiettivi di tali sistemi si limitano a quanto segue:

i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;

iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione relativa al mandato d'arresto europeo[5], punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

A norma dell'articolo 5, paragrafo 3, l'uso di tali tecnologie a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso.

A norma dell'articolo 5, paragrafo 4, uno Stato membro può decidere di autorizzare l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto e stabilire le necessarie regole dettagliate per la richiesta, il rilascio e l'esercizio delle autorizzazioni preventive, nonché per i reati ad esse relativi.

6. Le basi giuridiche della proposta di regolamento sono l'articolo 16 TFUE (protezione dei dati di carattere personale) e l'articolo 114 TFUE (funzionamento del mercato interno). Si pone pertanto la questione dell'adeguatezza di tali basi giuridiche in relazione alle regole armonizzate applicabili ai sistemi di IA forniti o utilizzati dalle autorità di contrasto e dalle autorità giudiziarie.

[5] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

7. Il presente parere si concentra anzitutto sull'adeguatezza della base giuridica dell'articolo 114 TFUE, nel particolare contesto delle autorità di contrasto menzionate in diverse disposizioni della proposta di regolamento, ossia per quanto riguarda i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico e i sistemi di IA ad alto rischio di cui all'allegato III, punto 6. Pertanto, affronta la questione se l'articolo 87, paragrafo 2, TFUE (cooperazione di polizia) sia una base giuridica più adeguata, rispetto all'articolo 114 TFUE (sezione II), per coprire la fornitura e l'uso di sistemi di IA da parte delle autorità di contrasto. Per analogia, la conclusione della presente nota può essere applicata alle autorità giudiziarie di cui all'allegato III per quanto riguarda i sistemi di IA ad alto rischio.

8. La presente nota esamina altresì l'adeguatezza dell'articolo 16 TFUE quale base giuridica supplementare e l'applicazione dei protocolli 21 e 22 nel contesto dell'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto (sezione III).

II. ADEGUATEZZA DELLA BASE GIURIDICA DELL'ARTICOLO 114 TFUE

9. Secondo una giurisprudenza consolidata, la base giuridica di un atto dell'Unione non dipende dal convincimento di un'istituzione circa lo scopo perseguito, ma deve essere determinata secondo criteri oggettivi, suscettibili di sindacato giurisdizionale, tra i quali figurano in particolare lo scopo e il contenuto dell'atto. Se l'esame di un atto dimostra che esso persegue una duplice finalità o che ha una doppia componente e se una di queste è identificabile come principale o preponderante, mentre l'altra è solo accessoria, tale atto deve fondarsi su una sola base giuridica, ossia quella richiesta dalla finalità o componente principale o preponderante. Solo eccezionalmente, una volta stabilito che l'atto persegue al contempo più finalità, intrinsecamente legate, senza che una di esse assuma importanza secondaria e indiretta rispetto all'altra, tale atto potrà basarsi sulle varie basi giuridiche di pertinenza, a meno che tali basi giuridiche prescrivano procedure che sono incompatibili l'una con l'altra. Occorre inoltre rilevare che l'articolo 114, paragrafo 1, prima frase, TFUE chiarisce che le disposizioni dell'articolo si applicano "[s]*alvo che i trattati non dispongano diversamente*". Di conseguenza, il ricorso all'articolo 114 TFUE è giustificato solo nel caso in cui non esista una disposizione più specifica che possa costituire la base giuridica per l'adozione dell'atto di cui trattasi[6]. Laddove esista nel trattato una disposizione più specifica che possa costituire la base giuridica dell'atto di cui trattasi, quest'ultimo deve fondarsi su tale disposizione[7].

---

6 Parere dell'SGC del 17 maggio 2016, ST 9007/16, punto 6.

7 Sentenza del 29 aprile 2004, *Commissione/Consiglio*, C-338/01, ECLI:EU:C:2004:253, punto 60.

A. OBIETTIVO DELLA PROPOSTA DI REGOLAMENTO

10. Il regolamento proposto armonizza l'immissione sul mercato, la messa in servizio e l'uso di un particolare tipo di software (sistemi di IA). Il fatto che le autorità pubbliche e gli operatori privati possano essere fornitori o utenti di tali sistemi di IA non è di per sé incompatibile con la base giuridica dell'articolo 114 TFUE[8].

11. Inoltre, il fatto che le autorità di contrasto o coloro che agiscono per loro conto possano essere tra i fornitori o gli utenti di tali sistemi di IA non è sufficiente a giustificare il ricorso alla base giuridica dell'articolo 87 TFUE. Lo scopo e il contenuto della proposta di regolamento devono essere analizzati al fine di stabilire se ciò sia necessario.

12. La proposta di regolamento mira in generale, anche per quanto riguarda i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico e i sistemi di IA ad alto rischio, a garantire un livello di protezione costante ed elevato in tutta l'Unione, evitando nel contempo divergenze che ostacolano la libera circolazione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno. Stabilisce obblighi uniformi per gli operatori e garantisce la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno (considerando 2). Più specificatamente, la proposta di regolamento stabilisce regole che disciplinano l'immissione sul mercato e la messa in servizio di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi (considerando 5). Nel complesso, la proposta mira a istituire un'IA affidabile fin dalla progettazione, applicabile in modo generalizzato, con una serie completa di regole che riguardano lo sviluppo, la commercializzazione e l'uso di prodotti, servizi e sistemi basati sull'IA. Dato che l'IA è già integrata in un gran numero di servizi e prodotti e continuerà a esserlo in futuro, la proposta segue una logica del mercato interno definendo un "quadro per la sicurezza dei prodotti" basato su una serie di quattro categorie di rischio. Essa impone requisiti per l'accesso al mercato e la certificazione dei sistemi di IA ad alto rischio mediante una procedura di marcatura CE obbligatoria.

---

[8] Cfr. parere giuridico dell'SGC (ST 11395/14, punti da 39 a 41) e precedenti come la direttiva (UE) 2016/2102 e le direttive 2014/24/UE, 2014/25/UE e 2014/23/UE.

13. Nessuno degli obiettivi dichiarati della proposta di regolamento fa riferimento alla garanzia di obiettivi di sicurezza pubblica. Anche se gli obiettivi di sicurezza pubblica devono essere conseguiti indirettamente attraverso il processo di armonizzazione dell'immissione sul mercato/della messa in servizio/dell'uso dei sistemi di IA da parte delle autorità di contrasto, la Corte[9], interpretando l'articolo 87, paragrafo 2, TFUE alla luce dell'articolo 67 TFUE, ha precisato che, affinché un atto dell'Unione sia fondato, alla luce della sua finalità e del suo contenuto, sul primo di tali articoli, detto atto deve essere direttamente collegato agli obiettivi enunciati all'articolo 67 TFUE (ossia, in questo caso, la prevenzione della criminalità e la cooperazione di polizia). Ciò è escluso nel contesto della proposta di regolamento, in quanto le uniche regole armonizzate sull'uso di tali sistemi da parte delle autorità di contrasto sono 1) regole in materia di sicurezza dei prodotti che si applicano in modo uniforme a tutti i fornitori e a tutti gli utenti in relazione all'immissione sul mercato/alla messa in servizio o all'uso dei sistemi di IA oppure 2) regole in materia di protezione dei dati personali per le quali è stata aggiunta la base giuridica dell'articolo 16 TFUE (cfr. parte III in appresso).

14. In un altro caso[10], anche se l'obiettivo della modifica della direttiva sulle armi da fuoco consisteva nel garantire un livello più elevato di sicurezza pubblica in relazione alla minaccia terroristica e ad altre forme di criminalità, la Corte ha dichiarato che l'armonizzazione degli aspetti relativi alla sicurezza delle merci è uno degli elementi essenziali per garantire il buon funzionamento del mercato interno, dal momento che normative divergenti in tale materia sono idonee a creare ostacoli agli scambi[11].

---

9 Sentenza del 6 maggio 2014, *Commissione europea/Parlamento europeo e Consiglio dell'Unione europea*, C-43/12, ECLI:EU:C:2014:298.

10 Sentenza del 3 dicembre 2019, *Repubblica ceca/Parlamento europeo*, C-482/17, ECLI:EU:C:2019:1035.

11 Ibid., punto 57: "*Orbene, poiché la particolarità delle armi da fuoco consiste, contrariamente a quanto asserito dalla Repubblica di Polonia, nella loro pericolosità non soltanto per gli utilizzatori, ma anche per il grande pubblico, come la Corte ha già rilevato al punto 54 della sentenza del 23 gennaio 2018, Buhagiar e a., C- 267/16, EU:C:2018:26, considerazioni di pubblica sicurezza risultano, come ricordato dal quinto considerando della direttiva 91/477, indispensabili nell'ambito di una normativa sull'acquisizione e sulla detenzione di tali merci*". Cfr. anche sentenza del 23 gennaio 2018, *Albert Buhagiar e altri/Minister for Justice*, C-267/16, ECLI:EU:C:2018:26, punto 54: "*Sul punto occorre osservare che, visto il rischio per la sicurezza delle persone rappresentato dalle armi da fuoco, la loro libera circolazione ha potuto essere raggiunta solo per mezzo di una disciplina rigorosa delle condizioni del loro trasferimento tra Stati membri, tra cui figura il principio dell'autorizzazione preventiva rilasciata dagli Stati membri interessati da un trasferimento delle merci citate*".

15. Gli obiettivi della proposta di regolamento, tra cui l'articolo 5, paragrafo 1, lettera d), e paragrafi 2, 3 e 4, sull'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto e le disposizioni relative ai sistemi di IA ad alto rischio di cui all'allegato III, punto 6, non sono direttamente collegati a un obiettivo di sicurezza pubblica. Al contrario, la proposta risponde alle principali preoccupazioni relative al modo in cui i sistemi di IA incidono sulla salute, sulla sicurezza e sui diritti fondamentali. Pertanto, le disposizioni pertinenti sono direttamente collegate all'obiettivo di garantire condizioni di parità nell'immissione sul mercato/nella messa in servizio o nell'uso dei sistemi di IA nel mercato interno, proteggendo nel contempo la salute, la sicurezza e i diritti fondamentali degli utenti.

16. Alla luce di quanto precede, l'obiettivo principale della proposta di regolamento è migliorare il funzionamento del mercato interno ai sensi dell'articolo 114 TFUE e gli obiettivi di cui all'articolo 67 TFUE sono solo indirettamente e incidentalmente collegati a tale obiettivo principale.

B. CONTENUTO DELLA PROPOSTA DI REGOLAMENTO

17. La proposta di regolamento contiene essenzialmente regole concernenti quanto necessario per immettere un prodotto specifico (un software di IA) sul mercato (o per metterlo in servizio) in modo da garantire che tale prodotto sia sicuro e che i diritti fondamentali siano rispettati. Introduce una serie completa di regole che riguardano lo sviluppo, la commercializzazione e l'uso di prodotti, servizi e sistemi basati sull'IA. La proposta di regolamento non obbliga le autorità di contrasto a utilizzare un sistema di IA legalmente immesso sul mercato, né disciplina direttamente il modo in cui le autorità di contrasto dovrebbero utilizzare tale sistema di IA. Definisce invece chiaramente le situazioni in cui l'uso previsto è considerato ad alto rischio semplicemente perché il sistema di IA sarà utilizzato dalle autorità di contrasto o dalle autorità giudiziarie.

18. A tale riguardo, l'articolo 29 della proposta di regolamento contiene disposizioni che riguardano le condizioni per l'uso di sistemi di IA ad alto rischio, ma tali disposizioni non hanno carattere settoriale, hanno una portata limitata (principalmente sulle istruzioni per l'uso del prodotto) e sono intrinsecamente legate agli obblighi imposti agli sviluppatori di sistemi di IA ai sensi della proposta di regolamento. Viene inoltre lasciato agli Stati membri un certo margine di manovra per fissare ulteriori regole sull'uso di tali sistemi di IA ad alto rischio. Per quanto riguarda i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto (articolo 5), la proposta di regolamento disciplina in parte l'uso di tali sistemi dal punto di vista della protezione dei dati sulla base dell'articolo 16 TFUE (cfr. parte III).

19. Inoltre, solo gli Stati membri possono decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di detti sistemi di identificazione biometrica remota "in tempo reale". Spetterà al diritto nazionale stabilire le condizioni specifiche relative a tale uso, nel rispetto dei criteri e delle tutele generali di cui al regolamento: l'autorizzazione preventiva di un'autorità giudiziaria o amministrativa, la richiesta, il rilascio e l'esercizio delle autorizzazioni preventive, nonché l'indicazione dei reati in relazione ai quali tali sistemi possono essere utilizzati.

20. I sistemi di IA sono un particolare tipo di software. Le regole armonizzate applicabili all'immissione sul mercato o alla messa in servizio/all'uso di sistemi di IA sono quindi regole armonizzate analoghe a quelle in materia di sicurezza dei prodotti. Si applicano in modo uniforme senza distinzione tra utenti pubblici e utenti privati. Secondo i pertinenti considerando della proposta di regolamento, è pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno. Ciò può essere conseguito stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno, sulla base dell'articolo 114 TFUE[12].

21. La proposta di regolamento contiene diversi riferimenti alle attività di contrasto, alla gestione del controllo delle frontiere e all'amministrazione della giustizia nell'allegato III sui sistemi di IA ad alto rischio (rispettivamente punti 6, 7 e 8). Tali riferimenti includono un elenco dettagliato ed esaustivo corrispondente all'articolo 6, paragrafo 2, in aggiunta ad altri sistemi ad alto rischio in relazione ai rischi per la sicurezza del prodotto di cui all'articolo 6, paragrafo 1. In effetti, a norma dell'articolo 6, paragrafo 1, alcuni sistemi di IA sono da considerarsi ad alto rischio per definizione, in ragione della loro gravità attesa e dei rischi elevati che presentano in termini di diritti fondamentali, salute e sicurezza. Tra gli altri sistemi considerati ad alto rischio elencati nell'allegato III figurano l'istruzione, la gestione delle infrastrutture critiche, l'occupazione, l'identificazione e la categorizzazione biometrica, nonché l'accesso ai servizi pubblici e servizi privati essenziali.

---

[12] Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di intelligenza artificiale per promuovere lo sviluppo, l'uso e l'adozione dell'intelligenza artificiale nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo, è opportuno stabilire regole che disciplinino l'immissione sul mercato e la messa in servizio di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi (cfr. considerando 2 e 5 della proposta).

22. Tuttavia, tali regole sui sistemi di IA ad alto rischio non stabiliscono se le autorità di contrasto e le autorità giudiziarie (o quelle di altri settori identificati) debbano utilizzare o meno tali sistemi. La proposta di regolamento produrrà solo indirettamente i suoi effetti sull'effettivo sviluppo dei sistemi di IA che possono essere utilizzati dalle autorità di contrasto e sui sistemi di IA in uso attualmente e in futuro. Pertanto, le regole si riferiscono a sistemi di IA "*destinati a essere utilizzati*" da tali autorità (cfr. ad esempio articolo 3, punto 12, articolo 8, paragrafo 2, e allegato III). La designazione di un determinato sistema di IA come ad alto rischio comporta l'applicazione di una serie specifica di regole in materia di gestione dei rischi, governance dei dati e specifiche tecniche. Gli utenti di tali sistemi di IA ad alto rischio devono rispettare le istruzioni per l'uso, conservare i log ed effettuare valutazioni d'impatto sulla protezione dei dati.

23. Inoltre, nel diritto dell'Unione o nel diritto nazionale possono essere stabiliti obblighi degli utenti diversi da quelli relativi alle istruzioni per l'uso, lasciando impregiudicata la discrezionalità dell'utente nell'organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore (articolo 29, paragrafo 2, della proposta di regolamento). Tali regole apportano ulteriori tutele in materia di diritti fondamentali per i sistemi di IA ad alto rischio.

24. Alla luce di quanto precede, è opportuno sottolineare che la proposta di regolamento non contiene regole volte a consentire o a impedire che un sistema di IA ad alto rischio immesso sul mercato sia utilizzato dalle autorità di contrasto. Per effetto delle regole proposte, a un sistema di IA sviluppato o utilizzato dalle autorità di contrasto sarà applicata un'etichetta distinta (ad alto rischio) in funzione dell'uso previsto. Tale uso sarebbe disciplinato dal diritto nazionale e, in una certa misura, deciso dalle stesse autorità di contrasto. In effetti, all'articolo 29 la proposta di regolamento stabilisce (limitatamente alle istruzioni per l'uso) condizioni minime per l'uso relative ai sistemi di IA ad alto rischio, compresi quelli elencati ai punti 6, 7 e 8 dell'allegato III, che saranno integrate dal diritto nazionale. Pertanto, in linea con la giurisprudenza della Corte, è opportuno distinguere tra, da un lato, la finalità perseguita dalla proposta di regolamento — che non è quella di disciplinare l'uso dei sistemi di IA da parte delle autorità di contrasto — e, dall'altro, gli effetti che può produrre indirettamente[13], che sono irrilevanti ai fini dell'analisi dell'adeguatezza della base giuridica.

25. I punti 6, 7 e 8 (rispettivamente sulle attività di contrasto, la migrazione e l'amministrazione della giustizia) non sono predominanti tra i sistemi di IA ad alto rischio. Peraltro, secondo la proposta di regolamento, un sistema di IA ad alto rischio non corrisponde necessariamente a uno di quelli elencati nell'allegato III. La maggior parte dei sistemi ad alto rischio sono infatti quelli elencati genericamente all'articolo 6, paragrafo 1, lettere a) e b) della proposta di regolamento (in relazione alla sicurezza dei prodotti). Altri sistemi di IA ad alto rischio figurano nell'allegato III ai punti 1 (identificazione biometrica), 2 (infrastrutture critiche), 3 (istruzione e formazione professionale) e 4 (occupazione, gestione dei lavoratori e accesso al lavoro autonomo), che riguardano settori diversi dalla giustizia e affari interni ("GAI"). Tutti gli utenti di tali sistemi di IA ad alto rischio sono soggetti a un regime uniforme stabilito non in considerazione del loro status specifico (se sono, ad esempio, un operatore economico o un'autorità pubblica), ma dal punto di vista della protezione della salute, della sicurezza e dei diritti fondamentali.

---

13 Cfr. sentenza della Corte del 21 giugno 2018, *Repubblica di Polonia/Parlamento europeo, Consiglio dell'Unione europea*, C-5/16, ECLI:EU:C:2018:483, punti da 63 a 68, e sentenza della Corte del 22 giugno 2022, *Leistritz AG/LH*, C-534/20, ECLI:EU:C:2022:495, punto 28.

26. La proposta di regolamento contiene pertanto regole armonizzate in materia di immissione sul mercato, messa in servizio e uso dei sistemi di IA, siano essi utilizzati da operatori privati o da autorità pubbliche, comprese, incidentalmente[14], le autorità di contrasto e le autorità giudiziarie.

27. A parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, che è soggetto a norme specifiche sul trattamento dei dati personali (cfr. parte III in appresso), la proposta di regolamento non contiene regole armonizzate sull'uso di sistemi di IA ad alto rischio. Come spiegato ai precedenti punti 18 e 19, il riferimento all'uso di sistemi di IA ad alto rischio si riferisce essenzialmente alle istruzioni per l'uso del prodotto (articolo 29) ed è collegato agli obblighi imposti agli sviluppatori. Come sottolineato al punto 22, spetta al diritto nazionale e alle autorità nazionali decidere se le autorità di contrasto o le autorità giudiziarie possano o meno utilizzare un sistema di IA ad alto rischio immesso legalmente sul mercato a norma del regolamento proposto.

28. Pertanto, l'articolo 87, paragrafo 2, TFUE, in particolare la lettera a), non costituisce una base giuridica adeguata per la proposta di regolamento. Le regole contenute nella proposta non promuovono né ostacolano la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio di informazioni pertinenti. Semplicemente, allorquando tali attività saranno svolte dalle autorità di contrasto, sarà necessario rispettare una serie di condizioni armonizzate non specifiche per tutelare i diritti degli utenti. Analogamente, gli obiettivi dichiarati nella proposta di regolamento non comprendono lo sviluppo di tecniche investigative comuni. I requisiti proposti sull'uso di sistemi di IA ad alto rischio non riguardano in modo specifico il settore GAI né la cooperazione di polizia stricto sensu quale definita nel TFUE.

---

14 Cfr. parere della Corte A-1/19 sulla *Convenzione di Istanbul*, ECLI:EU:C:2021:198, segnatamente punti 298 e 301.

29. Per quanto riguarda le disposizioni dell'articolo 5, paragrafo 4, della proposta di regolamento, uno Stato membro può ancora decidere di autorizzare l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto. Qualora decida in tal senso, lo Stato membro ha il dovere di stabilire le necessarie regole dettagliate per la richiesta, il rilascio e l'esercizio delle autorizzazioni preventive, nonché per i reati ad esse relativi ai fini dell'indagine o del perseguimento per cui è autorizzato l'uso[15]. Alla luce dell'esito delle discussioni in seno al Consiglio, tali regole proposte non comporterebbero il conferimento di nuovi poteri alle rispettive autorità nazionali. Al contrario, il ricorso a meccanismi esistenti o a eventuali meccanismi futuri è limitato al fine di garantire la tutela del diritto alla vita privata e ai dati personali.

30. Alla luce di quanto precede, l'articolo 114 TFUE è l'unica base giuridica adeguata per regole armonizzate sui sistemi di IA ad alto rischio, compresi quelli utilizzati dalle autorità di contrasto e dalle autorità giudiziarie, e qualsiasi base giuridica GAI di cui alla parte terza, titolo V, TFUE, quale l'articolo 87 TFUE per quanto riguarda tali regole armonizzate, non è né giustificata né adeguata.

[15] Vale la pena segnalare che l'articolo 5, paragrafo 4, della proposta presenta alcune caratteristiche simili all'articolo 15, paragrafo 1, della direttiva 2002/58 relativa alla vita privata e alle comunicazioni elettroniche, che prevede, in particolare, la possibilità per gli Stati membri di derogare a taluni divieti stabiliti dal diritto dell'Unione. In forza della giurisprudenza costante, le disposizioni nazionali che consentono la deroga a tale divieti rientreranno necessariamente nell'ambito di applicazione del diritto dell'Unione che, a sua volta, determinerà l'applicazione della Carta.

III. ADEGUATEZZA DELL'ARTICOLO 16 TFUE QUALE BASE GIURIDICA SUPPLEMENTARE

31. La proposta di regolamento cita l'articolo 16 TFUE come base giuridica per quanto concerne il trattamento dei dati personali nell'ambito delle attività di contrasto; i considerando 25 e 26 includono un riferimento all'articolo 6 bis del protocollo n. 21 e all'articolo 2 bis del protocollo n. 22 per quanto riguarda il trattamento dei dati personali nel settore della prevenzione della criminalità. Secondo la Commissione, l'articolo 16 TFUE dovrebbe fungere da base giuridica esclusivamente per le disposizioni che pongono restrizioni concernenti il trattamento dei dati biometrici personali in modo complementare rispetto alla direttiva 2016/680 ("direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie"). L'articolo 5, paragrafo 1, lettera d), è formulato come un divieto di principio cui si applicano tre eccezioni. In concreto, è vietato l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che tale uso sia strettamente necessario per: a) effettuare ricerche mirate di potenziali vittime di reato; b) prevenire un attacco terroristico imminente o un attacco imminente all'incolumità fisica/alla vita di una persona; c) localizzare o identificare o portare avanti un'azione penale nei confronti di un autore o un sospettato di un reato grave (con riferimento al mandato d'arresto europeo). Ulteriori requisiti di cui all'articolo 5, paragrafi 2, 3 e 4, riguardano tale uso specifico dei sistemi di IA da parte delle autorità di contrasto, in particolare per quanto concerne una valutazione della necessità e della proporzionalità, un'autorizzazione preventiva (tranne in situazioni di urgenza) e una decisione degli Stati membri di autorizzare o meno a livello nazionale l'uso specifico di strumenti di IA in siffatte situazioni.

32. Le disposizioni dettagliate di cui all'articolo 5 che disciplinano un uso specifico degli strumenti di IA non solo hanno lo scopo di integrare il vigente quadro legislativo dell'Unione (la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, a sua volta basata sull'articolo 16 TFUE), ma richiedono altresì un quadro nazionale di attuazione.

33. In sostanza, sebbene sia formulata come un divieto, la norma specifica di cui all'articolo 5 può essere descritta come intesa a definire un quadro rigoroso ed eccezionale per il monitoraggio generalizzato "in tempo reale", da parte di strumenti di IA, di individui in spazi aperti a fini di identificazione. Il divieto, al di là del semplice utilizzo di telecamere per la registrazione, fa riferimento all'uso di strumenti di IA per il riconoscimento automatico delle caratteristiche umane in spazi accessibili al pubblico (ad esempio dei volti ma anche dell'andatura, delle impronte digitali, del DNA, della voce, dell'azionamento dei tasti e di altri segnali biometrici o comportamentali). Ciò implica anche, in concomitanza, il rilevamento e l'identificazione delle persone mediante confronto/controllo analitico dei dati. Inoltre, la regola deve essere valutata anche alla luce del fatto che può essere consentita anche l'identificazione "in tempo reale" da parte di utenti privati negli spazi pubblici (ad esempio per eventi come le partite di calcio).

34. Ulteriori chiarimenti forniti dalla Commissione sembrano indicare che ad oggi nessuno Stato membro, o forse solo un numero molto limitato di Stati membri, ha disciplinato tale questione specifica al fine di consentire alle autorità di contrasto di utilizzare gli strumenti di IA nel rilevamento "in tempo reale" di individui negli spazi pubblici. Tuttavia, in termini pratici, sebbene non siano state fornite prove concrete a dimostrazione della necessità di operare un cambiamento nelle pratiche e negli strumenti esistenti, sembra evidente che in futuro le tecniche di indagine, i metodi di polizia scientifica e le norme in materia di raccolta delle prove dovranno integrare questo approccio basato su divieti ed eccezioni.

35. Per quanto riguarda la base giuridica, le disposizioni che pongono restrizioni concernenti il trattamento dei dati biometrici personali in modo complementare (rispetto alla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) sembrano perseguire l'obiettivo di proteggere i dati personali stabilendo tutele adeguate. Tale obiettivo è indissolubilmente legato a quello delle disposizioni rientranti nell'ambito di applicazione dell'articolo 114 TFUE, senza che una di esse assuma importanza secondaria e indiretta rispetto all'altra. La proposta di regolamento mira a stabilire un quadro generale relativo ai sistemi di IA seguendo un approccio basato sul rischio. In questo contesto, la regolamentazione orizzontale dei sistemi di IA può includere tutele rigorose applicabili allo specifico sistema di IA di rilevamento "in tempo reale". Tale specifico sistema di IA contenente tutele adeguate per la protezione dei dati personali è pertanto indissolubilmente legato all'obiettivo generale di migliorare il funzionamento del mercato interno e non riveste importanza secondaria o indiretta rispetto a quest'ultimo. La proposta di regolamento dovrebbe pertanto essere fondata su una duplice base, conformemente alla giurisprudenza pertinente (cfr. punto 9).

36. Resta tuttavia da stabilire quale base giuridica debba essere utilizzata per disciplinare il trattamento dei dati personali ai fini dell'uso dei sistemi di cui all'articolo 5, paragrafo 1, lettera c), e all'articolo 5, paragrafi da 2 a 4, del regolamento proposto. Infatti, l'articolo 87, paragrafo 2, lettera a), TFUE costituisce una base giuridica per le misure adottate dai servizi incaricati dell'applicazione della legge specializzati nel settore della prevenzione o dell'individuazione dei reati e delle relative indagini, per quanto riguarda la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni.

37. Tuttavia, come spiegato dall'avvocato generale nel parere PNR Canada (A1/15), l'articolo 16 TFUE, da un lato, e l'articolo 87, paragrafo 2, lettera a), TFUE, nonché l'articolo 82, paragrafo 1, lettera d), TFUE, dall'altro, non possono essere legati da un rapporto di tipo gerarchico "*lex generalis – lex specialis*"[16]. L'articolo 16, paragrafo 2, TFUE è l'unica disposizione applicabile alle norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle autorità di contrasto degli Stati membri nell'esercizio di attività di prevenzione della criminalità. Il semplice fatto che l'articolo 5 faccia riferimento all'elenco dei reati gravi di cui alla decisione quadro sul mandato d'arresto europeo non modifica questa valutazione: detto riferimento non significa che la decisione quadro di cui sopra si applichi in quanto tale[17]. Si tratta semplicemente di una tecnica legislativa per stilare un elenco dei reati gravi senza dover creare un allegato separato.

38. Resta il fatto che la norma di cui all'articolo 5 è stabilita non come mezzo per delimitare ulteriormente le condizioni di applicazione di tali misure relative al settore GAI, bensì al fine di garantire che in futuro qualsiasi uso dell'identificazione biometrica "in tempo reale" da parte dei sistemi di IA risponda adeguatamente alle preoccupazioni in materia di diritti fondamentali e, in primo luogo, alla necessità di fare in modo che i dati biometrici siano raccolti e trattati nel rispetto del diritto alla vita privata e ai dati personali.

A tale riguardo, il regolamento non mira a stabilire una nuova procedura obbligatoria specifica per il settore GAI, ma si basa piuttosto su mezzi procedurali collaudati per garantire il rispetto dei diritti fondamentali.

---

16 Cfr. conclusioni dell'avvocato generale P. Mengozzi dell'8 settembre 2016, *Progetto di accordo tra il Canada e l'Unione europea*, parere 1/15, ECLI:EU:C:2016:656, punti da 112 a 120.

17 Per quanto riguarda l'attuazione di detto elenco di reati gravi da parte degli Stati membri, cfr. sentenza della Corte del 21 giugno 2022, *Ligue des droits humains/Conseil des ministres*, C-817/19, ECLI:EU:C:2022:65, punti da 150 a 152.

39. Se l'articolo 16 TFUE costituisce una base giuridica supplementare adeguata, ciò solleva questioni relative all'applicazione, rispettivamente, degli articoli 6 bis e 2 bis dei protocolli n. 21 e n. 22. Come spiegato ai considerando 25 e 26 della proposta, ciò significa che, quando le autorità di contrasto in Irlanda o in Danimarca utilizzano sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di prevenzione della criminalità, e laddove l'Irlanda o la Danimarca non siano vincolate dalle corrispondenti regole in materia di cooperazione di polizia o di cooperazione giudiziaria in materia penale, questi due Stati membri non sono vincolati dall'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, della proposta di regolamento. Questo non implica che l'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, contenga regole in materia di cooperazione di polizia, ad esempio sulla condivisione delle informazioni tra le autorità di contrasto: significa semplicemente che l'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, della proposta di regolamento, analogamente alla direttiva 2016/680 (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie), che è *lex generalis* adottata sulla base dell'articolo 16 TFUE, disciplina il trattamento dei dati biometrici personali nel particolare contesto dei sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di prevenzione della criminalità, e niente di più. La proposta della Commissione a tale riguardo segue l'approccio adottato dal legislatore dell'Unione per la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie e, in quanto tale, conferma pertanto che in questo contesto il ricorso all'articolo 87, paragrafo 2, TFUE non è giustificato.

40. L'aggiunta dell'articolo 16 TFUE all'articolo 114 TFUE in questo caso è giustificata dal fatto che l'articolo 5, paragrafo 1, lettera d), e paragrafi 2 e 3, è l'unico punto che disciplina l'uso di un sistema di IA autorizzato che interferisce con il diritto alla protezione dei dati personali, che è *lex specialis* rispetto al quadro generale di protezione dei dati. Tali norme di *lex specialis* in materia di protezione dei dati che incidono sull'uso di tali sistemi di IA sensibili non possono essere considerate di importanza secondaria o indiretta rispetto alla base giuridica relativa al mercato interno. Pertanto, l'aggiunta dell'articolo 16 TFUE quale base giuridica è sufficientemente giustificata nella proposta di regolamento e il ricorso all'articolo 87, paragrafo 2, lettera a), TFUE non è adeguato.

IV. CONCLUSIONE

41. Alla luce di quanto precede, il servizio giuridico del Consiglio ritiene che:

a) il ricorso agli articoli 16 e 114 TFUE quali basi giuridiche della proposta di regolamento è giustificato e appropriato;

b) il ricorso all'articolo 87, paragrafo 2, TFUE o a qualsiasi altra base giuridica relativa al settore GAI non è giustificato o appropriato in relazione alle regole armonizzate applicabili ai sistemi di IA che possono essere forniti o utilizzati dalle autorità di contrasto o dalle autorità giudiziarie.