Martedì 5 luglio 2022

RACCOMANDAZIONI

PARLAMENTO EUROPEO

P9_TA(2022)0275

Negoziati in vista di un accordo di cooperazione tra l'UE e Interpol

Raccomandazione del Parlamento europeo del 5 luglio 2022 al Consiglio e alla Commissione per i negoziati in vista di un accordo di cooperazione tra l'Unione europea e l'Organizzazione internazionale della polizia criminale (OIPC-INTERPOL) (2022/2025(INI))

(2023/C 47/23)

Il Parlamento europeo,

— visto l'articolo 218 del trattato sul funzionamento dell'Unione europea (TFUE),

— visto il TFUE, in particolare l'articolo 16, l'articolo 82, paragrafo 1, e l'articolo 87, paragrafo 2,

— vista la Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare gli articoli 7, 8, 47 e 52,

— visto il 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) ([1]),

— vista la 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 circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio ([2]) (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie),

— visto il 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 ([3]) (EUDPR), in particolare l'articolo 42, paragrafo 1,

— visto il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI ([4]),

— visto il regolamento (UE) 2019/1896 del Parlamento europeo e del Consiglio, del 13 novembre 2019, relativo alla guardia di frontiera e costiera europea e che abroga i regolamenti (UE) n. 1052/2013 e (UE) 2016/1624 ([5]),

— visto il regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») ([6]),

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) GU L 119 del 4.5.2016, pag. 89.
([3]) GU L 295 del 21.11.2018, pag. 39.
([4]) GU L 135 del 24.5.2016, pag. 53.
([5]) GU L 295 del 14.11.2019, pag. 1.
([6]) GU L 283 del 31.10.2017, pag. 1.

Martedì 5 luglio 2022

— visto il regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) ([7]),

— visto il parere n. 8/2021 del Garante europeo della protezione dei dati, del 25 maggio 2021, relativo alla raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati per un accordo di cooperazione tra l'UE e Interpol,

— visto lo studio del suo Dipartimento tematico Diritti dei cittadini e affari costituzionali, del febbraio 2022, dal titolo «Ensuring the rights of EU citizens against politically motivated Red Notices» (Garantire i diritti dei cittadini dell'UE contro gli «avvisi rossi» di matrice politica),

— visto il regolamento di Interpol sul trattamento dei dati,

— viste la risoluzione 2161 (2017) dell'Assemblea parlamentare del Consiglio d'Europa sul ricorso abusivo al sistema Interpol: la necessità di garanzie giuridiche più rigorose e la risoluzione 2315 (2019) sulla riforma di Interpol e sui procedimenti di estradizione: rafforzare la fiducia contrastando gli abusi,

— visto il regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio ([8]),

— visto il regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 ([9]),

— visti l'articolo 114, paragrafo 4, e l'articolo 54 del suo regolamento,

— visto il parere della commissione per gli affari esteri,

— vista la relazione della commissione per le libertà civili, la giustizia e gli affari interni (A9-0200/2022),

A. considerando che attualmente il terrorismo, la criminalità organizzata e le forme gravi di criminalità sono fenomeni sempre più dinamici, complessi, innovativi, globalizzati, mobili e spesso transnazionali, che richiedono una risposta energica e una cooperazione dell'UE più efficace e coordinata con le autorità e gli organismi internazionali di contrasto, come l'Organizzazione internazionale della polizia criminale (Interpol); che la strategia dell'UE per l'Unione della sicurezza, proposta dalla Commissione nel 2020, invita gli Stati membri a intensificare la cooperazione e il coordinamento multilaterali tra l'UE e Interpol, in quanto elemento essenziale per promuovere la cooperazione e lo scambio di informazioni; che la risoluzione del Parlamento del 17 dicembre 2020 sulla strategia dell'UE per l'Unione della sicurezza ([10]) sottolinea la necessità di una maggiore cooperazione tra gli Stati membri e di un migliore coordinamento a livello dell'UE tra tutti gli attori;

B. considerando che una cooperazione internazionale efficace, nel pieno rispetto dei diritti fondamentali, è una componente importante di un'efficace cooperazione giudiziaria e di contrasto, soprattutto su quelle forme di criminalità che implicano il trattamento e la condivisione di dati personali; che la legalità del trattamento dei dati personali è disciplinata dall'*acquis* dell'Unione in materia di protezione dei dati, e che ciò si applica anche agli accordi bilaterali con partner chiave che svolgono un ruolo importante nell'ottenere informazioni e potenziali prove da paesi terzi;

C. considerando che Interpol è la più grande organizzazione internazionale di polizia criminale esistente e svolge un ruolo importante in tutto il mondo; che Interpol si fonda sulla cooperazione intergovernativa; che nel dicembre 2021 il Consiglio ha adottato un mandato negoziale per l'avvio di negoziati da parte della Commissione, nell'aspettativa di concludere, entro la fine del 2022, un accordo internazionale a nome dell'UE volto a rafforzare la cooperazione con

([7]) GU L 295 del 21.11.2018, pag. 138.
([8]) GU L 135 del 22.5.2019, pag. 27.
([9]) GU L 135 del 22.5.2019, pag. 85.
([10]) GU C 445 del 29.10.2021, pag. 140.

Interpol, compreso l'accesso alle sue banche dati e il rafforzamento della cooperazione operativa; che è di fondamentale importanza garantire che l'accordo finale metta in atto misure solide per garantire il rispetto dei principi relativi al trattamento dei dati personali quali sanciti nell'*acquis* dell'Unione in materia di protezione dei dati, nonché la correttezza dei dati personali ricevuti attraverso tale cooperazione, e per assicurare che ogni futura cooperazione e scambio di dati personali rispetti i diritti fondamentali, compreso il diritto alla protezione dei dati e alla vita privata;

D. considerando che l'UE e Interpol intrattengono una cooperazione di lunga data in una serie di settori connessi all'applicazione della legge attraverso l'attuazione operativa del ciclo programmatico dell'UE / EMPACT (piattaforma multidisciplinare europea di lotta alle minacce della criminalità) e con il sostegno alle attività degli Stati membri in cooperazione con agenzie dell'UE quali l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), l'Agenzia europea della guardia di frontiera e costiera (Frontex), l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto, l'Osservatorio europeo delle droghe e delle tossicodipendenze e l'Agenzia dell'UE per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, sulla base di accordi o accordi di lavoro; che il 5 novembre 2001 Europol e Interpol hanno firmato un accordo operativo seguito da un memorandum d'intesa che consente il trasferimento di dati personali tramite i rispettivi ufficiali di collegamento; che il 27 maggio 2009 Frontex ha firmato con Interpol un accordo di lavoro che istituisce un quadro di cooperazione con l'obiettivo di facilitare la prevenzione, l'individuazione e la lotta alla criminalità transfrontaliera, e di migliorare la sicurezza delle frontiere per combattere l'immigrazione illegale, il traffico di persone e la tratta di esseri umani;

E. considerando che i singoli Stati membri dell'UE, in qualità di paesi membri di Interpol, possono accedere direttamente alle su 19 banche dati, che contengono informazioni potenzialmente utili su persone, beni rubati, armi e minacce; che tali banche dati contengono milioni di dati con informazioni che potrebbero contribuire direttamente alla lotta contro la criminalità organizzata, le forme gravi di criminalità e il terrorismo; che Frontex, Eurojust e l'EPPO non hanno attualmente accesso a tali banche dati, in linea con i loro mandati — né direttamente né sulla base di un sistema di riscontro positivo/negativo — a causa della mancanza di un accordo con Interpol, richiesto a tal fine dalle norme Interpol sul trattamento dei dati;

F. considerando che l'attuale cooperazione tra l'UE e Interpol è già stretta nell'ambito della lotta al terrorismo; che tale cooperazione dovrebbe essere intensificata ed estesa a nuovi settori; che le procedure dovrebbero essere migliorate, accelerate e razionalizzate per rispondere a una serie di esigenze operative indispensabili al fine di facilitare un rapido accesso alle informazioni relative alla criminalità organizzata, alle forme gravi di criminalità e al terrorismo, e di attuare gli esistenti atti giuridici dell'Unione;

G. considerando che l'UE è il principale donatore di fondi a Interpol, fondi che sono destinati principalmente agli scambi di informazioni nel settore dell'applicazione della legge, ma anche alle attività di cooperazione e di sviluppo delle capacità in materia di gestione delle frontiere, nonché a progetti e programmi miranti a contrastare una serie di attività terroristiche e di forme gravi di criminalità; che ciò conferisce all'UE un ruolo importante nel migliorare il funzionamento di Interpol e, in particolare, la sua trasparenza e la sua responsabilità;

H. considerando che il nuovo accordo dovrebbe istituire un quadro moderno e coerente per la cooperazione degli organi e delle agenzie dell'UE con Interpol, sulla base delle modalità di cooperazione già esistenti; che l'accordo dovrebbe essere conforme ai requisiti generali della Carta, all'*acquis* applicabile dell'Unione in materia di protezione dei dati, segnatamente l'EUDPR e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, ai requisiti e alle garanzie specifici in materia di protezione dei dati stabiliti negli atti di base che istituiscono gli organi, le agenzie e i sistemi informatici dell'UE, nonché alla pertinente giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) e alle norme in materia di diritti fondamentali;

I. considerando che l'accordo dovrebbe rispondere a esigenze operative, tenendo conto dei più recenti sviluppi nella lotta al terrorismo e alla criminalità transfrontaliera, transnazionale, grave e organizzata; che l'accordo fornisce la base giuridica per lo scambio di informazioni operative, compresi i dati personali, e per l'accesso alle pertinenti banche dati Interpol da parte degli organi e delle agenzie dell'Unione in linea con il loro mandato, a condizione che l'accordo sia giuridicamente vincolante e applicabile nei confronti di tutte le parti e che includa tutte le necessarie garanzie in materia di protezione dei dati;

J. considerando che non è stata effettuata alcuna valutazione d'impatto sui diritti fondamentali in relazione alla raccomandazione della Commissione;

K. considerando che l'adozione, nel maggio 2019, del quadro giuridico dell'Unione per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della giustizia e degli affari interni ha dato l'avvio a colloqui esplorativi tra l'UE e Interpol sulla necessità di concludere un accordo di cooperazione; che nell'UE esiste attualmente un'infrastruttura di dati avanzata e condivisa per la cooperazione di polizia e giudiziaria, l'asilo e la migrazione, nonché per le frontiere e i visti; che tale infrastruttura, nonché i sistemi IT e le banche dati dell'UE che la costituiscono consentono una condivisione delle informazioni con paesi terzi od organizzazioni internazionali limitata e altamente regolamentata;

L. considerando che il nuovo accordo dovrebbe disciplinare la cooperazione tra Interpol ed Europol, l'EPPO, Eurojust e Frontex, e consentire a tali organi e agenzie e agli Stati membri di accedere direttamente, per fini strettamente legati allo svolgimento dei loro compiti, come disciplinato dai loro rispettivi atti di base, a due banche dati di Interpol, ossia le banche dati sui documenti di viaggio rubati e smarriti (SLTD) e sui documenti di viaggio associati a segnalazioni (TDAWN), attraverso il portale di ricerca europeo (ESP), nel rispetto dei requisiti dell'UE in materia di protezione dei dati e dei diritti fondamentali;

M. considerando che, in base alla costituzione di Interpol, quest'ultima è obbligata a non assistere o aiutare i paesi membri che agiscono in violazione del diritto internazionale in materia di diritti umani;

N. considerando che organizzazioni governative, internazionali e non governative continuano a segnalare che alcuni paesi membri abusano del sistema di notifica e segnalazione di Interpol per perseguire gli oppositori politici, i difensori nazionali dei diritti umani, gli avvocati, gli attivisti della società civile e i giornalisti, in violazione delle norme internazionali in materia di diritti umani e del regolamento stesso di Interpol; che, secondo le relazioni della Commissione e di organizzazioni della società civile, Interpol ha riformato e rafforzato i suoi processi di revisione degli «avvisi rossi», nonché i suoi sistemi di sostegno agli uffici centrali nazionali nei paesi membri, ha riformato l'istituzione e il funzionamento della commissione per il controllo dei fascicoli, che attua il suo meccanismo di denuncia, ha nominato un responsabile della protezione dei dati e attuato un programma di apprendimento e condivisione delle conoscenze; che, nonostante tali riforme, sussistono ancora gravi preoccupazioni legate ai possibili abusi del sistema di Interpol con un impatto sui diritti fondamentali, dato che anche relazioni recenti continuano a sottolineare la necessità di maggiori misure di salvaguardia giuridica, di una maggiore trasparenza e di una migliore attuazione delle riforme; che i meccanismi di aggiornamento delle informazioni relative agli «avvisi rossi» e alle segnalazioni presentano sfide considerevoli, dato che a volte rimangono attive nelle banche dati nazionali nonostante siano state aggiornate e rimosse dal Segretariato generale di Interpol; che sia le fonti scritte sia i colloqui con organizzazioni governative e non governative lasciano intendere che il processo di verifica di Interpol continua a essere disomogeneo;

O. considerando che l'articolo 3 della costituzione di Interpol vieta qualsiasi intervento o attività di natura politica, militare, religiosa o razziale; che negli ultimi anni si è continuato ad assistere ad abusi in casi di alto profilo in numerosi Stati membri di Interpol; che le estradizioni di matrice politica hanno spesso origine dal rilascio abusivo di un avviso rosso o di una «segnalazione di persona ricercata» per mezzo di Interpol; che Interpol mette a disposizione poche informazioni sul modo in cui revisiona gli avvisi rossi, sulla sua capacità amministrativa per farlo e sui risultati di tali revisioni, il che porta a una mancanza di trasparenza riguardo al modo in cui Interpol si adopera per contrastare efficacemente gli avvisi rossi di matrice politica; che gli Stati membri e altre organizzazioni internazionali hanno un accesso limitato alle informazioni relative alla gestione complessiva degli avvisi rossi e delle segnalazioni; che non è disponibile alcuna informazione sui paesi che fanno richiesta di tali avvisi, su quante richieste sono accettate e respinte, sulle motivazioni del respingimento, su quali paesi ottengono risultati migliori o peggiori in termini di accettazione o respingimento delle richieste e sullo sviluppo di tali pratiche nel tempo; che ciò rende impossibile valutare la qualità del processo di valutazione del Segretariato generale di Interpol, il lavoro degli uffici centrali nazionali o la qualità delle richieste presentate dai paesi;

P. considerando che il Parlamento, nella sua risoluzione del 16 settembre 2021 sul caso di Ahmed Mansoor, difensore dei diritti umani, negli Emirati arabi uniti [11], ha espresso profonda preoccupazione per la candidatura e la nomina a presidente di Interpol dell'ispettore generale del ministero degli Interni degli Emirati arabi uniti, il Maggiore Generale Ahmed Nasser al-Raisi, e ha invitato i membri dell'Assemblea generale di Interpol, in particolare gli Stati membri dell'UE, a esaminare debitamente le accuse di violazioni dei diritti umani mosse nei suoi confronti; che l'11 maggio 2022 in Francia sono state avviate indagini contro il presidente di Interpol per presunti atti di tortura;

---

[11] GU C 117 dell'11.3.2022, pag. 109.

Q. considerando che la cooperazione tra l'Unione europea e Interpol è sostenuta dalla fiducia nel sistema e nelle procedure interne di Interpol; che la fiducia nel sistema degli avvisi rossi e delle segnalazioni di Interpol si basa sulla prevenzione e sul rapido trattamento di un loro uso indebito da parte di paesi che cercano di sfruttare i sistemi di Interpol a fini politici e di repressione; che Interpol deve garantire che i dati personali trattati internamente attraverso i suoi sistemi siano conformi ai diritti umani e allo Stato di diritto;

R. considerando che numerosi paesi autoritari continuano a essere membri di Interpol; che negli ultimi anni i regimi autoritari sono riusciti a sfruttare politicamente il sistema degli avvisi rossi e delle segnalazioni, perseguitando persone al di fuori della loro giurisdizione e sottoponendole a restrizioni reali, concrete e invasive alle loro vite e i ai loro diritti fondamentali;

S. considerando che l'invasione dell'Ucraina da parte della Russia è una minaccia diretta alla cooperazione nell'attività di contrasto internazionale e che il suo accesso continuo alle banche dati Interpol è una minaccia all'integrità della cooperazione dell'UE con Interpol; che la Russia ha emesso un numero molto elevato di avvisi rossi e segnalazioni in tutto il mondo ed è responsabile della diffusione del maggior numero di avvisi rossi di matrice politica, anche nei confronti di cittadini dell'UE, come i giudici, i pubblici ministeri e gli investigatori lituani che indagano sugli eventi di Vilnius del 13 gennaio 1991; che oltre alla Russia anche altri paesi hanno usato il sistema di avvisi rossi per prendere di mira a livello politico i propri cittadini;

1. ricorda che i valori, i diritti fondamentali e l'acquis dell'Unione in materia di protezione dei dati, nello specifico il regolamento EUDPRe la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, devono costituire la base della politica dell'Unione in materia di cooperazione nell'attività di contrasto, garantendo la conformità ai principi di necessità, proporzionalità, legalità e presunzione di innocenza, così come l'assunzione di responsabilità e il ricorso giurisdizionale, assicurando nel contempo l'effettiva protezione delle persone, in particolare di quelle più vulnerabili; ricorda, inoltre, che il rispetto di tali diritti e principi, compresi il diritto alla vita privata e la protezione dei dati personali, dovrebbe essere al centro dello sviluppo della digitalizzazione nel settore della giustizia e della sicurezza, così come dello sviluppo del quadro di interoperabilità; sottolinea che tali principi dovrebbero essere al centro dei negoziati tra l'UE e Interpol su un accordo di cooperazione;

2. sottolinea la necessità assoluta di basare l'accordo con Interpol sul pieno rispetto della Carta, dell'acquis dell'Unione in materia di protezione dei dati e dei requisiti e delle misure di salvaguardia specifici in materia di protezione dei dati codificati negli atti di base che istituiscono le pertinenti agenzie, organismi e sistemi IT su larga scala dell'UE nonché i rispettivi mandati; sottolinea pertanto che la decisione del Consiglio sull'eventuale conclusione del previsto accordo dovrebbe basarsi anche sull'articolo 16 TFUE;

3. osserva che, prima di adottare la raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati per un accordo di cooperazione tra l'Unione europea e Interpol, la Commissione non ha effettuato una valutazione d'impatto sui diritti fondamentali in merito alla necessità e alla proporzionalità di ciascuna misura prevista o alla fattibilità giuridica di tutte le misure previste nell'ambito di un unico accordo globale;

4. raccomanda alla Commissione di seguire la differenziazione del Consiglio tra gli ambiti delle attività di contrasto, della cooperazione giudiziaria in materia penale e della sicurezza alle frontiere come elemento della gestione delle frontiere;

5. raccomanda che la Commissione garantisca l'accesso alle diverse banche dati di Interpol sulla base delle esigenze e in conformità degli ambiti di competenza stabiliti nei rispettivi mandati dei diversi organi e organismi dell'UE; ricorda che le banche dati di Interpol contengono milioni di informazioni che potrebbero potenzialmente contribuire alla lotta contro la criminalità; ricorda tuttavia che sussistono problemi documentati, che dovrebbero essere affrontati, in merito all'accuratezza, all'affidabilità e all'origine dei dati all'interno di tali banche dati;

6. sottolinea che la Commissione dovrebbe garantire un accesso controllato alle banche dati di Interpol da parte degli Stati membri e degli organi e organismi dell'UE e che dovrebbe assicurare anche le misure di salvaguardia concrete, specifiche, efficaci e necessarie per ciascun tipo di cooperazione incluso nell'accordo previsto al fine di garantire il pieno rispetto dell'acquis dell'Unione in materia di protezione dei dati, delle misure di salvaguardia e dei requisiti specifici in materia di protezione dei dati sanciti dalle basi giuridiche degli organi e organismi dell'Unione e dei sistemi informatici su

larga scala dell'UE, e dei diritti fondamentali; sottolinea che, per quanto riguarda l'accesso controllato alle banche dati, l'accordo dovrebbe almeno rispettare le garanzie già previste dai regolamenti sull'interoperabilità ([12]), dalla base giuridica del regolamento sul sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) ([13]) e dal regolamento (UE) 2016/794;

7. raccomanda alla Commissione di negoziare con Interpol in merito ai requisiti per standard elevati di qualità e verificabilità delle informazioni contenute nelle banche dati Interpol e per la trasparenza delle fonti delle informazioni;

8. si attende una particolare vigilanza durante i negoziati in considerazione della sensibilità dei dati personali contenuti nelle varie banche dati e del fatto che la maggior parte dei paesi terzi membri di Interpol non offre un livello adeguato di protezione dei dati e non è parte di un accordo internazionale a norma dell'articolo 218 TFUE che consenta lo scambio di dati personali operativi con l'UE;

9. esorta la Commissione a introdurre le necessarie misure di salvaguardia e garanzie robuste per garantire il rispetto dei diritti fondamentali e dei requisiti dell'UE in materia di protezione dei dati, al fine di autorizzare l'unità centrale di ETIAS, istituita all'interno di Frontex, e gli Stati membri dell'UE ad accedere alle banche dati di Interpol SLTD e TDAWN, attraverso l'ESP, e, se necessario, ad attuare efficacemente il regolamento concernente il sistema di informazione visti (VIS) ([14]), come successivamente rivisto, che consente agli Stati membri dell'UE di accedere, attraverso l'ESP, alle banche dati di Interpol SLTD e TDAWN nell'esaminare le domande di visto o di permesso di soggiorno; insiste che, in caso di attacco, nessuna informazione sia condivisa con Interpol o con il titolare dei dati contenuti nelle banche dati di Interpol, e ricorda che, come previsto nei regolamenti ETIAS e VIS, i due sistemi non faranno controlli incrociati con le banche dati Interpol finché ciò non sarà concordato e garantito nella pratica;

10. raccomanda che l'accordo previsto stabilisca chiaramente quali organi e organismi dell'UE dovrebbero avere i diritti di accesso alle banche dati di Interpol, specificando quali banche e per quali compiti e fini specifici; ritiene che l'accordo previsto non dovrebbe creare un obbligo per le agenzie dell'UE di cooperare con Interpol al di là di quanto già disciplinato nel diritto dell'Unione pertinente;

Protezione dei dati, trattamento e conservazione dei dati personali, ricorso giurisdizionale

11. invita la Commissione a garantire che l'accordo rispetti l'acquis dell'UE in materia di protezione dei dati e tuteli i diritti e le libertà fondamentali delle persone garantendo un livello di protezione dei dati personali trattati nell'ambito di tale accordo sostanzialmente equivalente a quello del diritto primario e derivato dell'UE; sottolinea che l'accordo di cooperazione previsto non dovrebbe portare a un indebolimento dei diritti e delle libertà fondamentali delle persone fisiche, in particolare dei loro diritti alla protezione dei dati e alla vita privata, e dovrebbe prevedere un ricorso effettivo per le violazioni di tali diritti;

12. sottolinea che l'accordo dovrebbe garantire che i dati personali trasferiti siano adeguati, pertinenti e limitati a quanto è necessario e proporzionato per la finalità per la quale sono trasferiti, conformemente all'acquis dell'Unione in materia di protezione dei dati; evidenzia inoltre che dovrebbe prevedere la possibilità di introdurre eventuali limitazioni all'accesso o all'uso, compresa una restrizione a ulteriori trasferimenti, o alla cancellazione dei dati al momento del trasferimento; sottolinea inoltre che agli interessati siano garantiti diritti effettivi e azionabili;

13. ritiene necessario prevedere che i fini per i quali i dati possono essere trasferiti siano indicati chiaramente nell'accordo e che sia vietato qualsiasi ulteriore trattamento di dati incompatibile con la finalità iniziale; ritiene che l'accordo debba indicare chiaramente che non sono consentite le decisioni basate unicamente sul trattamento automatizzato di informazioni personali senza coinvolgimento umano;

([12]) Regolamento (UE) 2019/817 e regolamento (UE) 2019/818.

([13]) Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1).

([14]) Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (GU L 218 del 13.8.2008, pag. 60).

14. sottolinea che l'accordo previsto dovrebbe illustrare chiaramente le procedure relative all'obbligo di notifica da parte di Interpol in caso di una violazione dei dati personali e la descrizione delle informazioni minime da fornire con la notifica della violazione; invita la Commissione a garantire, nell'accordo, che Interpol informi le agenzie competenti dell'UE e le autorità degli Stati membri, comprese le autorità nazionali per la protezione dei dati, in caso di violazione dei dati personali, senza indebito ritardo e, ove possibile, entro 72 ore;

15. raccomanda che la sorveglianza dei dati consultati sia gestita da uno o più organismi indipendenti responsabili della protezione dei dati con poteri di indagine e di intervento effettivi e con il potere di trattare le denunce dei singoli individui riguardanti l'uso dei loro dati personali;

16. raccomanda che la Commissione garantisca che Interpol non conservi i dati più a lungo di quanto sia necessario per la finalità per la quale sono stati trasferiti; si aspetta, in tale contesto, che l'accordo stabilisca norme chiare e specifiche sulla conservazione, compresi i limiti di conservazione, sulla revisione, sulla rettifica e sulla cancellazione dei dati personali;

17. esorta la Commissione a garantire diritti effettivi e azionabili a un ricorso in sede amministrativa e giudiziaria e a un ricorso effettivo a tutti gli interessati, ossia a qualsiasi persona i cui dati siano trattati nell'ambito dell'accordo in questione;

18. sottolinea che l'accordo chiarisce esplicitamente che Interpol non disporrà dell'accesso diretto o indiretto reciproco alle banche dati dell'UE;

Interoperabilità

19. sottolinea che la cooperazione nell'attività di contrasto e la condivisione delle informazioni sono strumenti importanti per combattere la criminalità e il terrorismo e perseguire la giustizia, ma devono essere mirate e soggette a misure di salvaguardia e vigilanza appropriate e predefinite; sottolinea inoltre che esse dovrebbero affrontare le sfide in materia di diritti fondamentali, in particolare migliorando la qualità dei dati, attenuando le distorsioni, individuando gli errori ed evitando qualsiasi forma di discriminazione nel processo decisionale;

20. raccomanda di prestare particolare attenzione alle sfide in materia di diritti fondamentali e alla necessità di adeguate misure di attenuazione e di meccanismi di non discriminazione, nonché di migliorare la qualità e la protezione dei dati in vista dell'istituzione di quadri per lo sviluppo futuro di una connessione potenziata tra i sistemi di informazione dell'UE e di Interpol nei settori della cooperazione di polizia e giudiziaria, dell'asilo e della migrazione, nonché della gestione integrata delle frontiere e dei visti, fornendo un quadro legislativo fondamentale per gli sviluppi attuali e futuri dell'infrastruttura digitale dell'UE;

21. raccomanda che, alla luce delle norme che disciplinano l'accesso ai dati personali e la condivisione delle informazioni nei diversi sistemi e nelle diverse banche dati dell'UE, i termini del futuro accordo di cooperazione con Interpol prevedano le misure di salvaguardia e le garanzie necessarie per dare agli Stati membri e alle agenzie competenti dell'UE un accesso controllato alle banche dati di Interpol tramite l'ESP, ove necessario per lo svolgimento dei loro compiti, in linea con i loro diritti di accesso e con il diritto unionale o nazionale che disciplina tale accesso e nel pieno rispetto dei requisiti dell'UE in materia di protezione dei dati e dei diritti fondamentali;

22. ricorda che le banche dati Interpol contengono un grande volume di dati sui documenti di viaggio dei cittadini di paesi terzi e che il ricorso ad esse potrebbe ridurre al minimo le lacune informative, aumentare le corrispondenze positive e, di conseguenza, migliorare i risultati operativi dell'ETIAS e del regolamento VIS riveduto; mette in evidenza che l'accordo di cooperazione con Interpol dovrebbe fornire la base giuridica necessaria, comprese le misure di salvaguardia e le garanzie in materia di protezione dei dati, e consentire all'ESP di connettersi direttamente alle banche dati Interpol; sottolinea che l'accordo di cooperazione dovrebbe pertanto fornire anche lo spazio per stabilire collegamenti sicuri tra l'ESP e l'ETIAS, da un lato, e l'infrastruttura informatica di Interpol, dall'altro, in modo da consentire l'accesso alle banche dati Interpol;

23. sottolinea che, in linea con l'attuale quadro dell'UE, il nuovo accordo dovrebbe assicurare che qualsiasi interrogazione automatizzata delle banche dati Interpol SLTD e TDAWN tramite l'ESP nel contesto dell'interoperabilità sia effettuata in modo tale che nessuna informazione sia rivelata allo Stato titolare della segnalazione Interpol;

Trasferimento di dati e trasferimenti successivi

24. ricorda che, conformemente all'acquis dell'UE in materia di protezione dei dati, il trasferimento di dati dall'Unione verso paesi terzi e organizzazioni internazionali è consentito solo se i destinatari di tali informazioni sono in grado di garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello dell'Unione; sottolinea in questo contesto che, in assenza di una decisione di adeguatezza su Interpol, l'accordo dovrebbe costituire la base giuridica che consente il trasferimento di dati personali a Interpol, a condizione che sia giuridicamente vincolante e applicabile nei confronti di tutte le parti firmatarie e che includa misure di salvaguardia appropriate in materia di protezione dei dati;

25. sottolinea che il trasferimento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, e dati relativi alla salute e alla vita sessuale o all'orientamento sessuale di un individuo dovrebbe essere consentito solo in circostanze eccezionali e se tale trasferimento è strettamente necessario e proporzionato in singoli casi per prevenire o combattere reati che rientrano nell'ambito di applicazione dell'accordo; pone l'accento sul fatto che l'accordo deve fornire misure di salvaguardia adeguate per affrontare i rischi specifici del trattamento di categorie speciali di dati, in particolare per i minori e le vittime di reati;

26. raccomanda di limitare l'applicazione delle deroghe per i trasferimenti successivi dei dati personali ai casi di cui al capitolo V del regolamento EUDPR; sottolinea che i requisiti specifici di cui ai regolamenti che istituiscono le agenzie e gli organismi dell'UE interessati devono essere pienamente rispettati, comprese le disposizioni specifiche relative al trasferimento di dati operativi da parte di Europol e di EPPO;

27. raccomanda che l'accordo garantisca che i trasferimenti di dati personali debbano essere soggetti a obblighi di confidenzialità, nonché necessari e proporzionati per gli scopi in esso specificati, vale a dire la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati, la salvaguardia contro le minacce alla sicurezza pubblica e la protezione delle frontiere esterne;

28. raccomanda che l'accordo stabilisca esplicitamente che i dati personali trasferiti dall'UE a Interpol non saranno utilizzati per richiedere, emettere o eseguire una pena di morte o qualsiasi forma di trattamento crudele e disumano, e che tali dati personali non verranno trasferiti qualora sussistano rischi che i dati vengano utilizzati a tal fine;

«Avvisi rossi» e diffusioni

29. sottolinea, in vista della futura cooperazione, che, nonostante le recenti riforme, la trasparenza e la responsabilità rimangono una sfida a livello sia individuale che organizzativo in seno a Interpol, così come la mancanza di informazioni statistiche disponibili sul funzionamento dei suoi sistemi di avvisi e diffusioni; invita pertanto la Commissione ad assicurare impegno e garanzie da parte di Interpol affinché sviluppi ulteriormente le strutture e norme necessarie nonché gli strumenti sostanziali che consentono un trattamento coerente e trasparente delle richieste, dei riesami, delle sfide, delle rettifiche e delle cancellazioni;

30. invita la Commissione a negoziare un requisito stringente affinché Interpol migliori la trasparenza del suo sistema di revisione degli «avvisi rossi» e delle diffusioni, in particolare del ruolo e dell'operato della sua Task force «Avvisi rossi e diffusioni»; invita la Commissione a usare i negoziati con Interpol per chiedere all'organizzazione di produrre, aggiornare e mettere a disposizione strumenti sostanziali e procedurali sul trattamento giuridico degli «avvisi rossi» e delle diffusioni, garantendo un trattamento coerente e trasparente delle richieste, dei riesami, delle sfide, delle rettifiche e delle cancellazioni;

31. raccomanda, al fine di migliorare l'efficienza e di aumentare la trasparenza, di prevedere una pubblicazione annuale dei dati statistici sul trattamento degli «avvisi rossi» e delle diffusioni, che comprenda informazioni sul numero di comunicazioni, sul paese d'origine, sulla categoria del reato, sulle ragioni o motivazioni del rifiuto e sul ricorso a sanzioni nei casi di abuso; invita la Commissione a garantire che siano raccolti dati statistici sulla gestione delle richieste di «avvisi rossi» e diffusioni da parte degli Stati membri dell'UE per tutti gli Stati membri;

32. sottolinea il fatto che, nel contesto di tale accordo, Interpol dovrebbe sviluppare profili di rischio pubblici degli «avvisi rossi» e delle diffusioni, sulla base della pubblicazione statistica annuale di cui al paragrafo sopra, che consentirebbe la valutazione del rischio di abuso da parte dei paesi richiedenti, e contribuirebbe a valutare l'efficacia dei meccanismi di contrasto di Interpol;

33. invita la Commissione, nel contesto di tale accordo, a esaminare le possibili modalità in cui l'ESP potrebbe affrontare il problema degli «avvisi rossi» e delle diffusioni di matrice politica, che in pratica sarebbero uno degli strumenti che potrebbero rivelarsi efficaci contro le richieste di «avvisi rossi» per motivi politici in alcune situazioni;

34. ricorda la dichiarazione del Consiglio sugli «avvisi rossi» di Interpol per quanto riguarda l'adozione del regolamento (UE) 2022/991 del Parlamento europeo e del Consiglio ([15]), che sostiene gli sforzi profusi da Interpol per prevenire l'abuso degli «avvisi rossi» e delle diffusioni di matrice politica o le violazioni dei diritti umani e chiede uno scambio continuo e regolare al riguardo tra Interpol e i suoi uffici centrali nazionali, al fine di creare maggiore consapevolezza delle azioni che gli Stati membri dovrebbero intraprendere in cooperazione con Interpol;

35. si attende che il Consiglio mantenga il suo impegno di continuare a sostenere Interpol nella promozione delle procedure e norme esistenti per la qualità e la conformità dei dati;

36. invita la Commissione a lavorare anche internamente, sfruttando gli strumenti tecnici esistenti disponibili nel quadro di sicurezza dell'UE per stabilire un meccanismo di verifica affinché gli Stati membri dell'UE scambino informazioni sull'individuazione e l'eliminazione di «avvisi rossi» e diffusioni di matrice politica, sulle migliori pratiche in tale ambito, e sui paesi terzi con profili di rischio che creano «avvisi rossi»;

37. invita la Commissione a riconoscere il rischio che i regimi autoritari compromettano sistematicamente la cooperazione nell'attività di contrasto internazionale basata sulla fiducia abusando degli strumenti forniti da Interpol; invita la Commissione a incoraggiare Interpol ad aumentare i propri sforzi nel contrastare efficacemente questa condotta scorretta;

38. invita la Commissione a includere nell'accordo disposizioni relative al sostegno a Interpol per incrementare il personale, attualmente esiguo, che gestisce la revisione degli «avvisi rossi» e delle diffusioni all'interno della commissione per il controllo dei fascicoli e per migliorare le informazioni statistiche sul funzionamento degli «avvisi rossi» e delle diffusioni; invita la Commissione a utilizzare il ruolo e l'influenza dell'UE per sostenere miglioramenti che rafforzeranno i meccanismi di tutela degli avvisi e delle diffusioni dall'uso improprio;

Russia

39. prende atto dell'annuncio del Segretario generale di Interpol riguardante l'attuazione di misure di monitoraggio rafforzate per individuare e prevenire qualsiasi ulteriore abuso dei sistemi di Interpol da parte della Russia; continua tuttavia a nutrire preoccupazioni quanto al fatto che il monitoraggio, da solo, non attenuerà del tutto i rischi di abusi da parte della Russia; sottolinea pertanto che, date le attuali circostanze particolari, tra cui le palesi violazioni del diritto internazionale da parte della Russia e il mancato rispetto del sistema internazionale basato su regole, il comitato esecutivo e il Segretariato generale di Interpol dovrebbero adottare misure immediate e risolute per revocare i diritti di accesso della Federazione russa e della Bielorussia ai sistemi Interpol, in quanto le loro azioni rappresentano una minaccia diretta alla cooperazione internazionale in materia di applicazione della legge e costituiscono una grave violazione dei diritti fondamentali; esorta il comitato esecutivo di Interpol a preparare e proporre all'Assemblea generale le necessarie modifiche allo Statuto di Interpol per consentire la sospensione dei paesi membri e invita gli Stati membri dell'UE a sostenere tale iniziativa al fine di sospendere dall'organizzazione la Russia e altri paesi che abusano sistematicamente di Interpol per motivi politici; esorta il Segretariato generale di Interpol a presentare al comitato esecutivo una proposta di misure correttive rivolte alla Federazione russa conformemente all'articolo 131, paragrafo 3, del regolamento di Interpol in materia di trattamento dei dati, compresa la sospensione dei diritti di accesso dell'ufficio centrale nazionale russo;

40. raccomanda caldamente che la Commissione presenti misure di monitoraggio rafforzate, nel contesto di tale accordo, relative agli «avvisi rossi» e alle diffusioni rilasciati dalle autorità russe prima della guerra in Ucraina; invita la Commissione a fornire consulenza agli Stati membri sulle misure specifiche da applicare per quanto riguarda gli «avvisi rossi» e le diffusioni rilasciati dalle autorità russe prima della guerra in Ucraina e nel contesto attuale;

([15]) Regolamento (UE) 2022/991 del Parlamento europeo e del Consiglio dell'8 giugno 2022 che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali, e il ruolo di Europol in materia di ricerca e innovazione (GU L 169 del 27.6.2022, pag. 1).

Osservazioni conclusive

41. chiede che l'accordo preveda la possibilità di una sua sospensione o denuncia in caso di qualsiasi violazione delle sue disposizioni, in particolare quelle in materia di dati personali a opera di una delle parti, precisando che i dati personali che rientrano nell'ambito di applicazione dell'accordo trasferiti prima della sua sospensione o denuncia possono continuare a essere trattati conformemente alle condizioni dell'accordo stesso;

42. ritiene che l'accordo previsto dovrebbe contenere una clausola su una relazione di riesame della Commissione tre anni dopo la sua entrata in vigore, e successivamente ogni tre anni, che valuti l'effettiva attuazione dell'accordo e il suo rispetto dei diritti fondamentali; reputa importante che l'accordo preveda un meccanismo di monitoraggio e riesami periodici per valutarne il funzionamento in relazione alle esigenze operative delle pertinenti agenzie dell'Unione, comprese le statistiche sul numero di criminali arrestati e condannati con l'ausilio dei dati Interpol, così come la sua conformità alla protezione dei dati e ad altri diritti fondamentali;

43. raccomanda, come confermato dalla CGUE nel suo parere dell'8 settembre 2016 sul progetto di accordo tra il Canada e l'Unione europea sul trasferimento dei dati del codice di prenotazione dei passeggeri aerei dall'Unione al Canada, che i visti dell'accordo includano tutte le pertinenti basi giuridiche sostanziali, compreso l'articolo 16 TFUE;

44. raccomanda che qualsiasi risoluzione delle controversie da negoziare rientri nella giurisdizione ultima della CGUE;

45. invita la Commissione a riferire al Parlamento, sia periodicamente che ogniqualvolta richiesto, in merito alla conduzione e all'esito dei negoziati; ricorda che il Parlamento ha potere di consenso sulla conclusione dell'accordo di cooperazione previsto e che dovrebbe pertanto essere coinvolto da vicino nel processo negoziale; invita la Commissione a garantire che la rendicontazione al Parlamento faccia parte dei meccanismi di monitoraggio e valutazione previsti nell'accordo di cooperazione;

o

o o

46. incarica la sua Presidente di trasmettere la presente raccomandazione al Consiglio, alla Commissione, nonché all'Organizzazione internazionale della polizia criminale (OIPC-INTERPOL).