Venerdì 21 maggio 2021

P9_TA(2021)0262

Adeguata protezione dei dati personali da parte del Regno Unito

Risoluzione del Parlamento europeo del 21 maggio 2021 sull'adeguata protezione dei dati personali da parte del Regno Unito (2021/2594(RSP))

(2022/C 15/23)

Il Parlamento europeo,

— vista la Carta dei diritti fondamentali dell'Unione europea (la «Carta»), in particolare gli articoli 7, 8, 16, 47 e 52,

— vista la sentenza della Corte di giustizia dell'Unione europea (CGUE) del 16 luglio 2020 nella causa C-311/18, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems (sentenza Schrems II) ([1]),

— vista la sentenza della CGUE del 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems/Data Protection Commissioner (sentenza Schrems I) ([2]),

— vista la sentenza della CGUE del 6 ottobre 2020 nella causa C-623/17, Privacy International/Secretary of State of Foreign and Commonwealth affairs ([3]),

— vista la sua risoluzione del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni ([4]),

— vista la sua risoluzione del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy ([5]),

— vista la sua risoluzione del 25 ottobre 2018 sull'utilizzo dei dati degli utenti Facebook da parte di Cambridge Analytica e l'impatto sulla protezione dei dati ([6]),

— vista la sua risoluzione del 20 maggio 2021 sulla sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020 — Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems («Schrems II») — Causa C-311/18 ([7]),

— vista la sua risoluzione del 26 novembre 2020 sulla revisione della politica commerciale dell'UE ([8]),

— visto l'accordo sugli scambi commerciali e la cooperazione, del 31 dicembre 2020, tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra ([9]),

— vista la sua risoluzione del 28 aprile 2021 sull'esito dei negoziati UE-Regno Unito ([10]),

— 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 (regolamento generale sulla protezione dei dati) ([11]) (RGPD),

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C 2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) GU C 378 del 9.11.2017, pag. 104.
([5]) GU C 118 dell'8.4.2020, pag. 133.
([6]) GU C 345 del 16.10.2020, pag. 58.
([7]) Testi approvati, P9_TA(2021)0256.
([8]) Testi approvati, P9_TA(2020)0337.
([9]) GU L 444 del 31.12.2020, pag. 14.
([10]) Testi approvati, P9_TA(2021)0141.
([11]) GU L 119 del 4.5.2016, pag. 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 ([12]) (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie),

— vista la 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 ([13]),

— viste la proposta di regolamento del Parlamento europeo e del Consiglio, del 10 gennaio 2017, presentata dalla Commissione e concernente il rispetto della vita privata e la tutela dei dati personali nelle comunicazioni elettroniche (COM(2017)0010) e la relativa posizione del Parlamento europea adottata il 20 ottobre 2017 ([14]),

— viste le raccomandazioni del comitato europeo per la protezione dei dati (*European Data Protection Board* — EDPB), tra cui la sua dichiarazione del 9 marzo 2021 sul regolamento relativo alla vita privata e alle comunicazioni elettroniche e le sue raccomandazioni 01/2020, del 10 novembre 2020, sulle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE,

— visti i criteri di riferimento per l'adeguatezza adottati dal Gruppo dell'Articolo 29 per la tutela dei dati il 6 febbraio 2018 e approvati dall'EDPB,

— viste le raccomandazioni 01/2021 dell'EDPB, del 2 febbraio 2021, sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie,

— visti i progetti di decisioni di adeguatezza pubblicati dalla Commissione il 19 febbraio 2021, una ai sensi dell'RGPD ([15]) e l'altra ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie ([16]),

— visti i pareri 14/2021 e 15/2021 dell'EDPB, del 13 aprile 2021, concernenti il progetto di decisione di esecuzione della Commissione europea a norma della direttiva (UE) 2016/680 sull'adeguata protezione dei dati personali nel Regno Unito,

— viste la Convenzione europea dei diritti dell'uomo (CEDU) e la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del Consiglio d'Europa, nonché il suo protocollo di modifica («Convenzione 108+»), di cui il Regno Unito è parte,

— visto il regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione,

— visto l'articolo 132, paragrafo 2, del suo regolamento,

— vista la proposta di risoluzione della commissione per le libertà civili, la giustizia e gli affari interni,

A. considerando che la possibilità di trasferire dati personali a livello transfrontaliero ha il potenziale per essere un motore fondamentale dell'innovazione, della produttività e della competitività economica, oltre a rivestire un'importanza cruciale per la cooperazione efficace nella lotta contro la criminalità organizzata transfrontaliera, le forme gravi di criminalità e il terrorismo, che dipende in misura crescente dallo scambio di dati personali;

B. considerando che la CGUE, nella sentenza Schrems I, ha sottolineato come l'accesso indiscriminato da parte delle autorità di intelligence al contenuto delle comunicazioni elettroniche violi l'essenza del diritto alla riservatezza delle comunicazioni di cui l'articolo 7 della Carta, e che gli Stati Uniti non prevedono, in violazione dell'articolo 47 della Carta, mezzi di ricorso sufficienti per le persone non statunitensi contro la sorveglianza di massa;

([12]) GU L 119 del 4.5.2016, pag. 89.
([13]) GU L 201 del 31.7.2002, pag. 37.
([14]) A8-0324/2017.
([15]) Progetto di decisione di esecuzione della Commissione a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito.
([16]) Progetto di decisione di esecuzione della Commissione a norma del regolamento (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito.

C. considerando che il Regno Unito è tradizionalmente un importante partner commerciale di molti Stati membri dell'UE e uno stretto alleato nel settore della sicurezza; che l'UE e il Regno Unito dovrebbero mantenere questa stretta cooperazione nonostante il recesso del Regno Unito dall'UE, poiché sarà vantaggiosa per entrambe le parti;

D. considerando che le imprese europee hanno bisogno di chiarezza e certezza giuridiche, dato che è sempre più importante per tutti i tipi di aziende che forniscono beni e servizi a livello internazionale poter trasferire i dati personali oltre i propri confini; che una decisione di adeguatezza nei confronti del Regno Unito ai sensi dell'RGPD è della massima importanza, dato che molte imprese europee effettuano scambi commerciali attraverso la Manica, in particolare dal momento che la Brexit è ancora molto recente e che i flussi di dati all'interno dell'Unione non hanno subito restrizioni; che la mancata adozione di un solido quadro di adeguatezza rischierebbe di perturbare i trasferimenti commerciali transfrontalieri di dati personali tra l'UE e il Regno Unito e comporterebbe elevati costi di adempimento;

E. considerando che l'accordo sugli scambi commerciali e la cooperazione include alcune garanzie e condizioni per lo scambio di dati personali pertinenti nell'ambito delle attività di contrasto; che i negoziati sui flussi di dati personali sono stati condotti parallelamente a quelli relativi all'accordo sugli scambi commerciali e la cooperazione, ma non sono stati completati entro la fine del periodo di transizione, che si è concluso il 31 dicembre 2020; che nell'accordo sugli scambi commerciali e la cooperazione è stata inclusa una «clausola passerella» come soluzione temporanea, subordinata all'impegno del Regno Unito a non modificare il suo attuale regime di protezione dei dati, al fine di garantire la prosecuzione dei flussi di dati personali tra il Regno Unito e l'UE fino all'adozione di una decisione di adeguatezza; che l'iniziale periodo di quattro mesi è stato prorogato e terminerà alla fine di giugno 2021;

F. considerando che la valutazione realizzata dalla Commissione prima di presentare il proprio progetto di decisione di esecuzione era incompleta e incoerente con i requisiti della CGUE relativi alle valutazioni di adeguatezza, come sottolineato dall'EDPB nei suoi pareri di adeguatezza, in cui consiglia alla Commissione di valutare ulteriormente gli specifici aspetti della legislazione e della prassi del Regno Unito che riguardano la raccolta in blocco di dati, la comunicazione a destinatari esteri e gli accordi internazionali in materia di scambio di informazioni di intelligence, l'ulteriore utilizzo delle informazioni raccolte a fini di contrasto e l'indipendenza dei commissari giudiziali;

G. considerando che taluni aspetti del diritto e/o della prassi del Regno Unito non sono stati presi in considerazione dalla Commissione e che ciò ha portato all'elaborazione di progetti di decisioni di esecuzione incoerenti con il diritto dell'Unione; considerando che, a norma dell'articolo 45 dell'RGPD, nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare «la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza» nonché «gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali», il che include gli accordi internazionali in altri settori che implicano l'accesso ai dati o la condivisione delle informazioni e richiede pertanto una valutazione di tali accordi internazionali;

H. considerando che la CGUE, nella sentenza «Schrems I», ha affermato chiaramente che «in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46/CE, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo» (punto 75);

I. considerando che, a norma dei trattati, le attività dei servizi di intelligence e la condivisione tra Stati membri e paesi terzi sono escluse dall'ambito di applicazione del diritto dell'Unione, poiché rientrano nella necessaria valutazione di adeguatezza del livello di protezione dei dati personali offerto dai paesi terzi, come confermato dalla CGUE nelle sentenze Schrems I e Schrems II;

J. considerando che le norme in materia di protezione dei dati si basano non solo sulla legislazione vigente ma anche sulla sua applicazione pratica, e che nell'elaborazione della sua decisione la Commissione ha valutato unicamente la legislazione senza tenere conto della sua effettiva applicazione pratica;

K. considerando che, attualmente, la Commissione riconosce che dodici paesi terzi offrono una protezione adeguata ai sensi dell'RGPD e ha recentemente concluso i colloqui a tale riguardo con la Repubblica di Corea; che il Regno Unito è il primo paese al quale la Commissione ha proposto di concedere una decisione di adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie;

L. considerando che il caso del Regno Unito è diverso da tutte le precedenti valutazioni di adeguatezza, poiché riguarda un ex Stato membro dell'UE che ha recepito le disposizioni dell'RGPD nel proprio ordinamento nazionale e ha stabilito inoltre che tutta la normativa nazionale derivante dal diritto dell'UE, ivi compresa la legislazione che recepisce la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, continuerà ad essere applicata anche dopo la fine del periodo di transizione;

I. **REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI**

Osservazioni generali

1. osserva che il Regno Unito è firmatario della CEDU e della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale; si aspetta che il Regno Unito, nonostante abbia lasciato l'Unione europea, garantisca lo stesso quadro minimo di protezione dei dati;

2. accoglie con favore l'impegno del Regno Unito a rispettare la democrazia e lo Stato di diritto, nonché a proteggere in ambito nazionale, dandovi attuazione, i diritti fondamentali quali sanciti dalla CEDU, tra cui elevati livelli di protezione dei dati; ricorda che ciò è un presupposto necessario per la cooperazione dell'UE con il Regno Unito; ricorda che, nonostante l'articolo 8 della CEDU sul diritto al rispetto della vita privata sia parte del diritto nazionale del Regno Unito in virtù dello *Human Rights Act* del 1998 e del *common law* grazie al nuovo illecito di abuso di informazioni riservate, il governo ha votato contro le iniziative volte a includere un diritto fondamentale alla protezione dei dati;

3. osserva che, per l'elaborazione di una solida normativa sulla protezione dei dati ai sensi dell'RGPD, l'Unione europea ha optato per un approccio alla governance dei dati incentrato sui diritti umani e, pertanto, esprime profonda preoccupazione per le dichiarazioni pubbliche del primo ministro del Regno Unito, il quale ha affermato che il Regno Unito cercherà di discostarsi dalle norme dell'UE in materia di protezione dei dati e di istituire propri controlli «sovrani» in questo settore; ritiene che la strategia nazionale 2020 del Regno Unito in materia di dati rappresenti un cambio di passo, dalla protezione dei dati personali verso un uso e una condivisione degli stessi più ampi, incompatibili con i principi di equità, minimizzazione dei dati e limitazione delle finalità ai sensi dell'RGPD; osserva che, nei suoi pareri sull'adeguatezza, l'EDPB ha evidenziato che ciò potrebbe comportare possibili rischi in relazione alla protezione dei dati personali trasferiti dall'Unione europea;

4. osserva che decisioni di adeguatezza valide contribuiscono in maniera importante alla protezione dei diritti fondamentali delle persone e alla certezza giuridica per le imprese; sottolinea, tuttavia, che le decisioni di adeguatezza basate su valutazioni incomplete e non opportunamente applicate dalla Commissione potrebbero avere l'effetto opposto, laddove contestate dinanzi a un organo giurisdizionale;

5. osserva che la valutazione realizzata dalla Commissione prima di presentare il proprio progetto di decisione di esecuzione era incompleta e incoerente con i requisiti della CGUE relativi alle valutazioni di adeguatezza, come sottolineato dall'EDPB nei suoi pareri di adeguatezza, in cui consiglia alla Commissione di valutare ulteriormente gli specifici aspetti della legislazione e della prassi del Regno Unito che riguardano la raccolta in blocco di dati, la comunicazione a destinatari esteri e gli accordi internazionali in materia di scambio di informazioni di intelligence, l'ulteriore utilizzo delle informazioni raccolte a fini di contrasto e l'indipendenza dei commissari giudiziali;

Applicazione dell'RGPD

6. esprime preoccupazione per la mancata, e spesso inesistente, applicazione dell'RGPD da parte del Regno Unito quando quest'ultimo ancora era membro dell'UE; rileva in particolare la mancanza, in passato, di un'adeguata applicazione da parte dell'*Information Commissioner's Office* (ICO — Ufficio del commissario per l'informazione) del Regno Unito; rimanda all'esempio dell'ICO, che ha archiviato una denuncia riguardante le tecnologie pubblicitarie dopo aver organizzato due eventi con i portatori di interessi, elaborato una relazione dal titolo «Update Report on Adtech» (Relazione di aggiornamento sulla tecnologie pubblicitarie) e affermato che il settore delle tecnologie pubblicitarie appare immaturo nella

sua comprensione degli obblighi relativi alla protezione dei dati, senza però utilizzare le sue competenze di esecuzione ([17]); esprime preoccupazione per il fatto che la mancata esecuzione sia un problema strutturale, come indicato nella politica di azione normativa dell'ICO, in cui si afferma esplicitamente che «nella maggior parte dei casi riserveremo i nostri poteri ai casi più gravi, rappresentanti le violazioni più gravi degli obblighi in materia di diritti di informazione. Tali violazioni, generalmente, sono il risultato di un atto volontario o deliberato o di una negligenza, ovvero consistono in ripetute violazioni degli obblighi relativi ai diritti all'informazione, che arrecano pregiudizio o provocano danni alle persone»; sottolinea che, in pratica, ciò ha fatto sì che non sia stato posto rimedio a un ampio numero di violazioni della legislazione sulla protezione dei dati nel Regno Unito;

7. prende atto della strategia nazionale del Regno Unito in materia di dati, aggiornata il 9 dicembre 2020, che suggerisce un passaggio dalla protezione dei dati personali a un uso e una condivisione maggiori e più ampi dei dati; rileva che tale posizione secondo cui la mancata comunicazione dei dati può avere un impatto negativo sulla società, come enunciata nella strategia, non è compatibile con i principi di minimizzazione dei dati e limitazione della finalità ai sensi dell'RGPD e del diritto primario;

8. osserva che la commissione per gli affari costituzionali nel 2004 ([18]) e la commissione per gli affari pubblici del parlamento del Regno Unito nel 2014 ([19]), hanno raccomandato di garantire l'indipendenza dell'ICO rendendolo un funzionario parlamentare che riferisce al parlamento, anziché continuare a essere nominato dal ministero per i media digitali e lo sport; deplora che non sia stato dato seguito a tale raccomandazione;

Trattamento dei dati per il controllo dell'immigrazione

9. osserva che la legislazione del Regno Unito sulla protezione dei dati prevede una deroga ad alcuni aspetti dei diritti e dei principi fondamentali in materia di protezione dei dati, tra cui il diritto di accesso, il diritto dell'interessato di sapere con chi sono condivisi i propri dati, e se tale protezione pregiudichi l'effettivo controllo dell'immigrazione; sottolinea che il monitoraggio e la conformità del ricorso all'esenzione devono essere in linea con le norme enunciate nei criteri di riferimento per l'adeguatezza, che impongono di tenere conto della prassi e del principio, specificando che è necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti a un paese terzo, ma anche il sistema vigente che garantisce l'efficacia di tali norme; riconosce che tale esenzione, che è a disposizione di tutti i titolari del trattamento dei dati nel Regno Unito, è stata approvata dall'ICO e da un tribunale, e può essere invocata solo caso per caso e applicata in base ai principi di necessità e proporzionalità; ricorda le informazioni recentemente rivelate secondo cui sono state presentate 17 780 richieste di accesso in relazione ai dati trattati dal ministero degli Interni tra il 1º aprile 2018 e il 31 marzo 2019 e riguardanti 146,75 milioni di interessati e che l'esenzione per l'immigrazione è stata utilizzata nel 2020 per oltre il 70 % delle richieste degli interessati al ministero degli Interni ([20]); sottolinea che anche nei casi in cui il ministero degli Interni ha utilizzato la deroga, l'accesso alle informazioni non è stato completamente negato ma limitato ai documenti con omissioni;

10. osserva che tale esenzione si applica ora ai cittadini dell'UE che risiedono o prevedono di risiedere nel Regno Unito; esprime profonda preoccupazione per il fatto che l'esenzione elimina le principali possibilità di responsabilità e di ricorso e sottolinea che non si tratta di un livello di protezione adeguato;

([17]) Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it* (L'ICO del Regno Unito affronta un'azione legale dopo aver archiviato una denuncia riguardante le tecnologie pubblicitarie senza prove), TechCrunch, San Francisco, 2020.

([18]) Settima relazione della commissione ad hoc per gli affari costituzionali, pubblicata dalla Camera dei Comuni il 13 giugno 2006. Il punto 108 recita: «l'ipotesi di un commissario per l'informazione che risponda direttamente al parlamento e sia da quest'ultimo finanziato presenta meriti notevoli e si raccomanda di prendere in considerazione tale cambiamento non appena si presenterà l'occasione di modificare la legislazione».

([19]) Relazione della commissione per la pubblica amministrazione dal titolo «*Who's accountable? Relationships between Government and arm's-length bodies*» (Chi è responsabile? I rapporti tra il governo e gli organismi indipendenti), pubblicata dalla Camera dei Comuni il 4 novembre 2014. Il punto 64 recita: «Il commissario per l'informazione e l'ispettorato penitenziario dovrebbero essere maggiormente indipendenti dal governo e dovrebbero riferire al parlamento. Il commissario per l'informazione, il commissario per le nomine pubbliche e il presidente della commissione per i requisiti della funzione pubblica dovrebbero diventare funzionari parlamentari, come lo sono già il difensore civico parlamentare e per i servizi sanitari, il controllore e il revisore generale».

([20]) Comunicato stampa di Open Rights Group del 3 marzo 2021 dal titolo «Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office».

11. ribadisce la sua seria preoccupazione in merito a un'eccezione ai diritti degli interessati nella politica di immigrazione del Regno Unito; ribadisce inoltre la sua posizione secondo cui l'esenzione per il trattamento dei dati personali ai fini dell'immigrazione prevista dal *Data Protection Act* del Regno Unito deve essere modificata prima di poter adottare qualsiasi valida decisione di adeguatezza, come più volte ribadito, anche nella sua risoluzione del 12 febbraio 2020 sulla proposta di mandato negoziale per un nuovo partenariato con il Regno Unito di Gran Bretagna e Irlanda del Nord ([21]) e nel parere della commissione per le libertà civili, la giustizia e gli affari interni del 5 febbraio 2021 ([22]); invita la Commissione ad adoperarsi per eliminare l'esenzione per l'immigrazione o a garantirne una riforma, così che la deroga e il ricorso alla stessa offrano garanzie sufficienti agli interessati e non violino le norme che ci si attende da un paese terzo;

Sorveglianza di massa

12. ricorda le rivelazioni sulla sorveglianza di massa da parte degli Stati Uniti e del Regno Unito, riportate dall'informatore Edward Snowden; ricorda che il programma britannico «Tempora», gestito dal *Government Communications Headquarters* (GCHQ — il quartier generale delle comunicazioni del governo) del Regno Unito, intercetta le comunicazioni in tempo reale attraverso i cavi in fibra ottica della dorsale internet e registra i dati in modo che possano essere trattati e consultati in un momento successivo; ricorda che tale sorveglianza di massa del contenuto e dei metadati delle comunicazioni avviene indipendentemente dall'esistenza di sospetti specifici o di dati obiettivo;

13. ricorda che, nelle sentenze «Schrems I» e «Schrems II», la CGUE ha statuito che l'accesso di massa al contenuto delle comunicazioni private incide sul contenuto essenziale del diritto al rispetto della vita privata e che, in questi casi, una verifica della necessità e della proporzionalità non è più necessaria; sottolinea che tali principi si applicano ai trasferimenti di dati a paesi terzi diversi dagli Stati Uniti, Regno Unito incluso;

14. ricorda la sua risoluzione del 12 marzo 2014 in cui si affermava che i programmi di sorveglianza di massa indiscriminati e non fondati su sospetti condotti dall'agenzia di intelligence GCHQ del Regno Unito sono incompatibili con i principi di necessità e proporzionalità in una società democratica e non sono adeguati ai sensi del diritto dell'UE sulla protezione dei dati; riconosce che, da allora, il Regno Unito ha realizzato una significativa riforma delle proprie leggi in materia di sorveglianza, introducendo garanzie che vanno al di là delle condizioni stabilite dalla Corte di giustizia dell'Unione europea (CGUE) nella sua sentenza Schrems II ([23]) e delle garanzie previste dalle legislazioni sulla sorveglianza della maggior parte degli Stati membri; accoglie con favore in particolare la disposizione riguardante il pieno accesso ad effettivi mezzi di ricorso giurisdizionale; ricorda che il relatore speciale delle Nazioni Unite sul diritto al rispetto della vita privata ha accolto con favore le solide garanzie introdotte con l'Investigatory Powers Act (IPA) del 2016 in termini di necessità, proporzionalità e autorizzazione indipendente di un organo giudiziario;

15. ricorda che nel settembre 2018 la Corte europea dei diritti dell'uomo ha confermato che i programmi di intercettazione e conservazione di dati di massa del Regno Unito, tra cui Tempora, sono illegali e incompatibili con le condizioni necessarie per una società democratica ([24]);

16. ritiene inaccettabile che i progetti di decisione di adeguatezza non tengano conto dell'assenza di restrizioni all'utilizzo da parte del Regno Unito dei poteri sui dati in blocco, né dell'effettivo ricorso alle operazioni di sorveglianza del Regno Unito e degli Stati Uniti, come descritto da Edward Snowden, compreso il fatto che:

a) l'ICO o gli organi giurisdizionali non effettuano un controllo sostanziale efficace sul ricorso all'esenzione per la sicurezza nazionale prevista dalla legislazione del Regno Unito relativa alla protezione dei dati;

b) le restrizioni di utilizzo dei poteri su dati in blocco da parte del Regno Unito non sono previste dalla legge stessa, come richiesto dalla CGUE (ma sono invece lasciate alla discrezione dell'esecutivo soggetta a un «rispettoso» controllo giurisdizionale);

([21]) Testi approvati, P9_TA(2020)0033.

([22]) Parere della commissione per le libertà civili, la giustizia e gli affari interni sulla conclusione, a nome dell'Unione, dell'accordo sugli scambi e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, e dell'accordo tra l'Unione europea e il Regno Unito di Gran Bretagna e Irlanda del Nord sulle procedure di sicurezza per lo scambio e la protezione di informazioni classificate, LIBE_AL(2021)680848.

([23]) Sentenza del 16 luglio 2020, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

([24]) Sentenza della Corte europea dei diritti dell'uomo del 13 settembre 2018, Big Brother Watch e altri/Regno Unito, ricorsi nn. 58170/13, 62322/14, 24960/15.

Venerdì 21 maggio 2021

c) la descrizione di «dati secondari» (metadati) nei progetti di decisione è gravemente fuorviante e non precisa che tali dati possono contenere molte informazioni ed essere altamente invasivi, e che sono soggetti a sofisticate analisi automatizzate (come dichiarato dalla CGUE nella causa «*Digital Rights Ireland*» ([25])) ma che tuttavia, ai sensi della legislazione britannica, i metadati non sono adeguatamente protetti dall'accesso indebito, dalla raccolta in blocco e dall'analisi basata sull'intelligenza artificiale da parte delle agenzie di intelligence del Regno Unito;

d) le «Five Eyes Agencies», in particolare il GCHQ e l'Agenzia nazionale per la sicurezza (NSA), condividono nella pratica tutti i dati di intelligence;

sottolinea inoltre che, per quanto riguarda gli Stati Uniti, i cittadini del Regno Unito godono di alcune garanzie informali tra il GCHQ e l'NSA; esprime profonda preoccupazione per il fatto che tali garanzie non proteggano i cittadini o i residenti dell'UE, i cui dati possono essere oggetto di trasferimenti successivi e di condivisione con l'NSA;

17. invita gli Stati membri a concludere accordi di «non spionaggio» con il Regno Unito e invita la Commissione a utilizzare i suoi scambi con le controparti britanniche per trasmettere il messaggio che, se le leggi e le pratiche di sorveglianza del Regno Unito non verranno modificate, l'unica opzione percorribile per facilitare le decisioni di adeguatezza sarebbe la conclusione di accordi di «non spionaggio» con gli Stati membri;

Trasferimenti successivi

18. sottolinea con forza il fatto che la legge del 2018 sul recesso dall'Unione europea (*European Union Withdrawal Act*) prevede che la giurisprudenza della CGUE esistente prima della fine del periodo di transizione diventi «diritto mantenuto dell'UE» e pertanto giuridicamente vincolante per il Regno Unito; sottolinea che il Regno Unito è vincolato dai principi e dalle condizioni definiti nelle sentenze Schrems I e Schrems II della CGUE per quanto riguarda la valutazione sull'adeguatezza di altri paesi terzi; esprime preoccupazione per il fatto che i tribunali del Regno Unito non applicheranno più la Carta; rileva che il Regno Unito non è più sottoposto alla giurisdizione della CGUE, la quale rappresenta l'ultimo grado di giudizio per l'interpretazione della Carta;

19. sottolinea che le norme del Regno Unito sulla condivisione dei dati personali ai sensi del *Digital Economy Act* del 2017 e sui trasferimenti successivi dei dati di ricerca chiaramente non possono considerarsi come «sostanzialmente equivalenti» alle norme stabilite nell'RGPD, come interpretate dalla CGUE;

20. esprime preoccupazione per il fatto che il Regno Unito si sia attribuito il diritto di dichiarare che altri paesi terzi o territori garantiscono un livello di protezione dei dati adeguato, indipendentemente dal fatto che l'Unione europea abbia ritenuto il paese terzo o territorio in questione in grado di offrire tale protezione; ricorda che il Regno Unito ha già dichiarato, contrariamente all'UE, che Gibilterra garantisce tale protezione; esprime profonda preoccupazione per il fatto che uno status di adeguatezza del Regno Unito porterebbe di conseguenza all'aggiramento delle norme dell'UE sui trasferimenti verso paesi o territori non ritenuti adeguati ai sensi del diritto dell'UE;

21. prende atto del fatto che il 1º febbraio 2021 il Regno Unito ha inviato una richiesta di adesione all'accordo globale e progressivo di partenariato transpacifico (CPTTP), in particolare al fine di beneficiare delle moderne norme sul commercio digitale che consentono la libera circolazione dei dati tra i membri, rimuovono gli ostacoli inutili per le imprese [ecc.]"; osserva con preoccupazione che i membri del CPTTP sono undici, otto dei quali non hanno una decisione di adeguatezza da parte dell'UE; esprime profonda preoccupazione per i potenziali trasferimenti successivi di dati personali di cittadini e residenti dell'UE verso tali paesi nel caso in cui sia concessa nei confronti del Regno Unito una decisione di adeguatezza ([26]);

([25]) Sentenza della Corte di giustizia dell'8 aprile 2014, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri, C-293/12 e C-594/12, ECLI:EU:C:2014:238.

([26]) Comunicato stampa del ministero del Commercio internazionale del Regno Unito del 30 gennaio 2021 dal titolo «*UK applies to join huge Pacific free trade area CPTPP*» (Il Regno Unito chiede di aderire alla vasta zona di libero scambio del Pacifico CPTPP).

22. esprime rammarico per il fatto che la Commissione non abbia valutato l'impatto e i rischi potenziali dell'accordo tra il Regno Unito di Gran Bretagna e Irlanda del Nord e il Giappone relativo a un partenariato economico globale, che include disposizioni sui dati personali e sul livello di protezione dei dati;

23. esprime preoccupazione in merito al fatto che, qualora il Regno Unito includa disposizioni sui trasferimenti di dati in qualsiasi futuro accordo commerciale, tra l'altro negli accordi commerciali tra USA e Regno Unito, il livello di protezione offerto dall'RGPD ne sarebbe compromesso;

II. **DIRETTIVA SULLA PROTEZIONE DEI DATI NELLE ATTIVITÀ DI POLIZIA E GIUDIZIARIE**

24. sottolinea che il Regno Unito è il primo paese per il quale la Commissione ha proposto di adottare una decisione di adeguatezza a norma della direttiva (UE) 2016/680;

25. prende atto dell'accordo di accesso transfrontaliero ai dati tra il Regno Unito e gli Stati Uniti ([27]), ai sensi del CLOUD Act statunitense, che facilita i trasferimenti a fini di contrasto; esprime profonda preoccupazione per il fatto che ciò consentirà alle autorità statunitensi di accedere indebitamente ai dati personali dei cittadini e dei residenti dell'UE; condivide la preoccupazione dell'EDPB in merito al fatto che le garanzie previste dall'accordo quadro tra l'Unione europea e gli Stati Uniti ([28]) , applicate *mutatis mutandis*, potrebbero non soddisfare i criteri di chiarezza, precisione e accessibilità delle norme per quanto riguarda l'accesso ai dati personali o che detto accordo sancisca tali garanzie in modo insufficiente a renderle efficaci e impugnabili ai sensi del diritto del Regno Unito;

26. ricorda che la sentenza C-623/17 della CGUE deve essere interpretata nel senso di precludere una normativa nazionale che consenta a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica di trasmettere in modo generale e indifferenziato alle agenzie di sicurezza e di intelligence dello Stato i dati relativi al traffico e i dati relativi all'ubicazione al fine di salvaguardare la sicurezza nazionale;

27. osserva che, in tale causa, la CGUE ha stabilito che la raccolta in blocco di dati effettuata nel Regno Unito ai sensi del *Regulation of Investigatory Powers Act* del 2000 era illegittima; rileva che la regolamentazione è stata da allora sostituita dall'*Investigatory Powers Act* (IPA 2016) con lo scopo di rafforzare i principi di necessità e proporzionalità; sottolinea che l'IPA 2016 subordina l'intercettazione al controllo giurisdizionale e autorizza le persone ad accedere ai propri dati e a presentare ricorso dinanzi al tribunale dei poteri d'indagine; deplora, tuttavia, il fatto che l'IPA 2016 continui a consentire la pratica della conservazione in blocco dei dati;

28. esprime preoccupazione per le recenti segnalazioni secondo cui un sistema di raccolta e conservazione di dati di massa fa parte di una sperimentazione condotta dal ministero degli Interni del Regno Unito nell'ambito dell'IPA 2016;

29. ricorda che, nella risoluzione del 12 febbraio 2020, il Parlamento europeo ha sottolineato che «il Regno Unito non può avere accesso diretto ai dati dei sistemi di informazione dell'UE o partecipare alle strutture di gestione delle agenzie dell'UE nello spazio di libertà, sicurezza e giustizia e che qualsivoglia tipo di condivisione di informazioni, inclusi i dati personali con il Regno Unito, dovrebbe essere soggetta a rigorose condizioni di tutela, controllo e monitoraggio, compreso un livello di protezione dei dati personali equivalente rispetto a quello previsto dal diritto dell'UE»; prende atto delle carenze individuate nel modo in cui il Regno Unito ha attuato la legge sulla protezione dei dati mentre era ancora membro dell'UE; ricorda che il Regno Unito ha registrato e conservato una copia del sistema d'informazione Schengen (SIS); si attende che le agenzie di contrasto del Regno Unito rispettino appieno le norme applicabili negli scambi di dati personali in futuro; ricorda che il Regno Unito mantiene l'accesso ad alcune banche dati dell'UE sulle attività di contrasto unicamente in base a un sistema di riscontro positivo o negativo mentre gli è giuridicamente precluso l'accesso al sistema SIS;

([27]) Accordo tra il governo del Regno Unito di Gran Bretagna e Irlanda del Nord e il governo degli Stati Uniti d'America, del 3 ottobre 2019, sull'accesso ai dati elettronici ai fini della lotta contro le forme gravi di criminalità.

([28]) Accordo tra gli Stati Uniti d'America e l'Unione europea sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati (GU L 336 del 10.12.2016, pag. 3).

Venerdì 21 maggio 2021

30. esprime preoccupazione per la rivelazione nel gennaio 2021 secondo cui 400 000 casellari giudiziari sono stati accidentalmente cancellati dal sistema informatico nazionale della polizia britannica; sottolinea che ciò non induce ad avere fiducia negli sforzi profusi dal Regno Unito per garantire la protezione dei dati ai fini di contrasto;

31. osserva che il progetto di decisione di adeguatezza valuta accuratamente i diritti di ciascuna autorità del Regno Unito alla quale il diritto nazionale attribuisce competenze di intercettazione e conservazione dei dati personali per motivi di sicurezza nazionale; accoglie inoltre con favore il fatto che le dettagliate relazioni di vigilanza sulle autorità incaricate della comunità di intelligence forniscano informazioni sulle pratiche di sorveglianza attuali del Regno Unito; invita la Commissione a valutare e monitorare ulteriormente i tipi di dati relativi alle comunicazioni che rientrano nei poteri di conservazione dei dati e di intercettazione leciti del Regno Unito;

32. rileva che l'accordo sugli scambi commerciali e la cooperazione tra l'UE e il Regno Unito include titoli riguardanti lo scambio di DNA, impronte digitali e dati di immatricolazione dei veicoli, il trasferimento e il trattamento dei dati del codice di prenotazione (PNR), la cooperazione sulle informazioni operative e la cooperazione con Europol ed Eurojust, che si applicheranno indipendentemente dalla decisione di adeguatezza; ricorda, in ogni caso, le preoccupazioni espresse nel parere della commissione per le libertà civili, la giustizia e gli affari interni del febbraio 2021 sull'accordo sugli scambi commerciali e la cooperazione in merito all'uso speciale e alla conservazione più lunga dei dati personali concessi al Regno Unito a norma dei titoli Prüm e PNR dell'accordo sugli scambi commerciali e la cooperazione, che non sono in linea con gli usi e le modalità di conservazione degli Stati membri; ricorda il diritto di adire la CGUE per chiedere la verifica della legalità del previsto accordo internazionale e, in particolare, la sua compatibilità con la tutela di un diritto fondamentale ([29]);

Conclusioni

33. invita la Commissione a garantire alle imprese dell'UE che la decisione di adeguatezza fornirà una base giuridica solida, sufficiente e orientata al futuro per i trasferimenti di dati; evidenzia l'importanza di garantire che tale decisione di adeguatezza sia considerata accettabile se riesaminata dalla CGUE e sottolinea che tutte le raccomandazioni formulate nel parere dell'EDPB dovrebbero pertanto essere recepite;

34. accoglie con favore il fatto che le decisioni di adeguatezza saranno applicabili per soli quattro anni, dal momento che il Regno Unito, che non è più uno Stato membro dell'Unione europea, potrebbe decidere di modificare la legislazione oggetto della valutazione di adeguatezza della Commissione; invita la Commissione a continuare nel frattempo a monitorare il livello di protezione dei dati nel Regno Unito, sia nel diritto che nella prassi, e a condurre una valutazione approfondita prima di rinnovare la decisione di adeguatezza nel 2025;

35. è del parere che, adottando le due decisioni di esecuzione non conformi al diritto dell'Unione, senza peraltro aver affrontato tutte le preoccupazioni espresse nella presente risoluzione, la Commissione ecceda le competenze di esecuzione attribuitele dal regolamento (UE) 2016/679 e dalla direttiva (UE) 2016/680; esprime pertanto la sua contrarietà ai due atti di esecuzione sulla base del fatto che i progetti di decisioni di esecuzione non sono conformi al diritto dell'Unione;

36. invita la Commissione a modificare i due progetti di decisioni di esecuzione al fine di garantirne la piena conformità alla legislazione e alla giurisprudenza dell'Unione europea;

37. chiede che, qualora la Commissione adotti le sue decisioni di adeguatezza in relazione al Regno Unito prima che quest'ultimo ponga rimedio alle criticità sopra menzionate, le autorità nazionali responsabili della protezione dei dati sospendano il trasferimento dei dati personali che potrebbe essere soggetto a un accesso indiscriminato da parte delle autorità di intelligence del Regno Unito;

38. invita la Commissione e le autorità competenti del Regno Unito a elaborare un piano d'azione per affrontare quanto prima le criticità identificate nei pareri dell'EDPB e altre questioni aperte inerenti alla protezione dei dati nel Regno Unito, quale presupposto per la decisione di adeguatezza finale;

39. invita la Commissione a continuare a monitorare da vicino il livello di protezione dei dati e le leggi e le pratiche sulla sorveglianza di massa nel Regno Unito; osserva che il capo V dell'RGPD prevede altre possibilità giuridiche per i trasferimenti di dati personali verso il Regno Unito; ricorda che, conformemente agli orientamenti dell'EDPB, i trasferimenti si basano su deroghe in situazioni specifiche a norma dell'articolo 49 dell'RGPD e devono avvenire in situazioni eccezionali;

([29]) Risoluzione del Parlamento europeo sul progetto di decisione della Commissione che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR — *Passenger Name Records*) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (GU C 103 E del 29.4.2004, pag. 665).

40. si rammarica del fatto che la Commissione abbia ignorato gli inviti del Parlamento a sospendere lo scudo per la privacy fino a quando le autorità statunitensi non rispetteranno le sue condizioni, e che abbia invece sempre preferito «monitorare la situazione» senza alcun risultato concreto in termini di protezione dei dati per le persone né certezza giuridica per le imprese; esorta la Commissione a imparare dai suoi errori del passato prestando attenzione agli inviti del Parlamento e degli esperti relativi alla conclusione e al monitoraggio delle precedenti decisioni di adeguatezza, e a non lasciare che sia la GCUE, sulla base delle denunce presentate dai singoli, ad occuparsi dell'adeguata applicazione della legislazione dell'Unione europea in materia di protezione dei dati;

41. invita la Commissione a monitorare da vicino la legislazione e le prassi in materia di protezione dei dati nel Regno Unito, a informare e consultare immediatamente il Parlamento in merito a qualsiasi futura modifica del regime di protezione dei dati del Regno Unito e a conferire al Parlamento un ruolo di controllo nel nuovo quadro istituzionale, anche per gli organismi pertinenti, come il comitato specializzato per la cooperazione delle autorità di contrasto e giudiziarie;

o

o o

42. incarica il suo Presidente di trasmettere la presente risoluzione alla Commissione, agli Stati membri e al governo del Regno Unito.