Parlamento europeo
2019-2024

TESTI APPROVATI

P9_TA(2023)0204

Adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati

Risoluzione del Parlamento europeo dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP))

Il Parlamento europeo,

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

– vista la sentenza della Corte di giustizia dell'Unione europea (CGUE) del 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems/Data Protection Commissioner ("Schrems I")[1],

– vista la sentenza della CGUE del 16 luglio 2020 nella causa C-311/18, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems ("Schrems II")[2],

– vista la sua indagine sulle rivelazioni fatte da Edward Snowden sulla sorveglianza elettronica di massa dei cittadini dell'UE, comprese le conclusioni contenute nella 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[3],

– vista la sua risoluzione del 26 maggio 2016 sui flussi di dati transatlantici[4],

– vista la sua risoluzione del 6 aprile 2017 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy[5],

– vista la sua risoluzione del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo

---

1 Sentenza del 6 ottobre 2015, C-362/14, Maximillian Schrems/Data Protection Commissioner, EU:C:2015:650.
2 Sentenza del 16 luglio 2020, C-311/18, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems, ECLI:EU:C:2020:559.
3 GU C 378 del 9.11.2017, pag. 104.
4 GU C 76 del 28.2.2018, pag. 82.
5 GU C 298 del 23.8.2018, pag. 73.

scudo UE-USA per la privacy[1],

– 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[2],

– visto il progetto di decisione di esecuzione della Commissione a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello adeguato di protezione dei dati personali nell'ambito del quadro UE-USA sulla privacy dei dati,

– vista l'ordinanza esecutiva n. 14086 del Presidente degli Stati Uniti, del 7 ottobre 2022, sul rafforzamento delle salvaguardie per le attività di intelligence dei segnali statunitensi,

– vista l'ordinanza esecutiva n. 12333 del Presidente degli Stati Uniti, del 4 dicembre 1981, sulle attività di intelligence statunitensi,

– visto il regolamento sul Tribunale per il riesame della protezione dei dati emesso dall'Attorney General degli Stati Uniti (regolamento AG),

– 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)[3], in particolare il capo V,

– 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[4],

– visti i criteri di riferimento per l'adeguatezza del gruppo di lavoro Articolo 29 (WP 254 rev.01) approvati dal comitato europeo per la protezione dei dati e viste le raccomandazioni 01/2020 del comitato relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, nonché le raccomandazioni 02/2020 del comitato relative alle garanzie essenziali europee per le misure di sorveglianza,

– visto il parere 5/2023 del comitato europeo per la protezione dei dati, del 28 febbraio 2023, sul progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali nell'ambito del quadro UE-USA in materia di privacy dei dati,

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

A. considerando che, nella sentenza "Schrems I", la CGUE ha annullato la decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza

---

1 GU C 118 dell'8.4.2020, pag. 133.
2 GU C 15 del 12.1.2022, pag. 176.
3 GU L 119 del 4.5.2016, pag. 1.
4 GU L 201 del 31.7.2002, pag. 37.

pubblicate dal Dipartimento del commercio degli Stati Uniti[1] e ha sottolineato che l'accesso indiscriminato delle autorità di intelligence al contenuto delle comunicazioni elettroniche viola l'essenza del diritto fondamentale alla riservatezza delle comunicazioni di cui all'articolo 7 della Carta; che la Corte ha sottolineato che, ai fini di una decisione di adeguatezza, un paese terzo deve garantire un livello di protezione non identico bensì "sostanzialmente equivalente" a quello garantito dal diritto dell'UE, il che può essere conseguito con mezzi diversi;

B. considerando che, nella sentenza "Schrems II", la CGUE ha annullato la decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy[2] e ha concluso che essa non forniva mezzi di ricorso sufficienti contro la sorveglianza di massa per i cittadini non statunitensi e che ciò viola l'essenza del diritto fondamentale a un ricorso giurisdizionale previsto dall'articolo 47 della Carta;

C. considerando che, il 7 ottobre 2022, il Presidente degli Stati Uniti d'America ha firmato l'ordinanza esecutiva n. 14086 sul rafforzamento delle salvaguardie per le attività di intelligence dei segnali statunitensi (EO 14086);

D. considerando che, il 13 dicembre 2022, la Commissione ha avviato il processo di adozione di una decisione di adeguatezza per il quadro UE-USA in materia di privacy dei dati;

E. considerando che, nell'esaminare il livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese derivanti dal suo diritto interno o dai suoi impegni internazionali, nonché la prassi intesa a garantire il rispetto di tali norme; che, se tale valutazione dovesse essere ritenuta insoddisfacente in termini di adeguatezza ed equivalenza, la Commissione dovrebbe astenersi dall'adottare una decisione di adeguatezza in quanto essa è subordinata all'attuazione delle pertinenti garanzie; che la Commissione è tenuta a sospendere l'adeguatezza qualora non vi sia più equivalenza; che il regolamento generale sulla protezione dei dati (RGPD) prevede che la valutazione pertinente sia un processo continuo che tenga conto delle modifiche delle norme e delle prassi applicabili;

F. 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 purché siano fornite garanzie adeguate; che tali trasferimenti dovrebbero essere effettuati nel pieno rispetto del diritto alla protezione dei dati personali e del diritto alla riservatezza; che uno degli scopi dell'UE è la protezione dei diritti fondamentali sanciti dalla Carta;

G. considerando che il RGPD si applica a tutte le imprese che trattano dati personali degli interessati nell'Unione, laddove le attività di trattamento siano legate all'offerta di beni o servizi destinati a suddetti interessati nell'Unione o al controllo del loro comportamento a condizione che esso avvenga all'interno dell'Unione;

H. considerando che la sorveglianza di massa, vale a dire la raccolta di dati indiscriminata

---

1 GU L 215 del 25.8.2000, pag. 7.
2 GU L 207 dell'1.8.2016, pag. 1.

e priva di garanzie per limitare le intrusioni nella vita privata delle persone, da parte di attori statali lede la fiducia riposta da cittadini e imprese europei nei servizi digitali e, per estensione, nell'economia digitale; che, sebbene alle agenzie statunitensi sia vietato procedere alla raccolta generalizzata dei dati dei cittadini statunitensi che vivono negli Stati Uniti, tale divieto non si applica ai cittadini dell'UE; che la sorveglianza di massa da parte di attori statali è illegale e compromette la fiducia riposta da cittadini e imprese dell'UE nei servizi digitali e, per estensione, nell'economia digitale;

I. considerando che i responsabili del trattamento dei dati dovrebbero sempre farsi garanti del rispetto degli obblighi in materia di protezione dei dati, ivi compresa la dimostrazione di conformità per qualsiasi trattamento dei dati, indipendentemente dalla sua natura, dalla sua portata, dal suo contesto, dagli scopi e dai rischi per gli interessati;

J. considerando che negli Stati Uniti non esiste una legislazione federale in materia di privacy e protezione dei dati; che l'ordinanza esecutiva n. 14086 introduce definizioni di concetti chiave in materia di protezione dei dati, come i principi di necessità e proporzionalità, il che costituisce un significativo passo avanti rispetto ai precedenti meccanismi di trasferimento; che il modo in cui tali principi sono interpretati richiede un monitoraggio attento; che potrebbe non essere possibile eseguire una valutazione globale delle modalità di attuazione di tali principi nell'ordinamento giuridico statunitense a causa della mancanza di trasparenza nelle procedure del Tribunale per il riesame della protezione dei dati;

1. ricorda che il rispetto della vita privata e familiare e la protezione dei dati personali sono diritti fondamentali giuridicamente applicabili e sanciti dai trattati, dalla Carta e dalla Convenzione europea dei diritti dell'uomo, nonché dalle leggi e dalla giurisprudenza; sottolinea che le decisioni di adeguatezza a norma del RGPD sono decisioni giuridiche e non scelte politiche e che i diritti alla vita privata e alla protezione dei dati non possono essere bilanciati con interessi commerciali o politici, bensì unicamente con altri diritti fondamentali;

2. prende atto degli sforzi compiuti con l'ordinanza esecutiva n. 14086 per fissare limiti alle attività statunitensi di intelligence dei segnali, applicando i principi di proporzionalità e necessità al quadro giuridico statunitense relativo all'intelligence dei segnali e fornendo un elenco di obiettivi legittimi per tali attività; osserva che tali principi sarebbero vincolanti per l'intera comunità dell'intelligence statunitense e potrebbero essere fatti valere dagli interessati nell'ambito della procedura di cui all'ordinanza esecutiva n. 14086; sottolinea che tale ordinanza esecutiva prevede miglioramenti significativi volti a garantire che tali principi siano sostanzialmente equivalenti nel diritto dell'UE; sottolinea, tuttavia, che tali principi sono elementi fondamentali e consolidati del regime di protezione dei dati dell'UE e che le loro definizioni sostanziali nell'ordinanza esecutiva n. 14086 non sono in linea con le definizioni ai sensi del diritto dell'UE e con la loro interpretazione da parte della CGUE; sottolinea inoltre che, ai fini del quadro UE-USA in materia di privacy dei dati, tali principi sarebbero interpretati unicamente alla luce del diritto e delle tradizioni giuridiche statunitensi e non del diritto e delle tradizioni giuridiche dell'UE; osserva che l'ordinanza esecutiva n. 14086 elenca 12 obiettivi legittimi che possono essere perseguiti nell'ambito della raccolta di intelligence dei segnali e 5 obiettivi per i quali è vietata la raccolta di intelligence dei segnali; osserva che l'elenco degli obiettivi legittimi di sicurezza nazionale può essere modificato e ampliato dal Presidente degli Stati Uniti senza alcun obbligo di rendere pubblici gli aggiornamenti pertinenti, né di

informare l'UE; sottolinea che l'ordinanza esecutiva n. 14086 richiede che l'intelligence dei segnali sia condotta in misura necessaria e proporzionata alla "priorità convalidata di intelligence", il che sembra essere un'interpretazione ampia di questi concetti; sottolinea che, per poter procedere a una valutazione globale dei principi di proporzionalità e necessità nel contesto dell'ordinanza esecutiva n. 14086, tali principi dovrebbero essere resi operativi e attuati nelle politiche e nelle procedure delle agenzie di intelligence statunitensi; esprime tuttavia preoccupazione per il fatto che gli analisti non siano tenuti a effettuare una valutazione della proporzionalità per ogni decisione in materia di sorveglianza;

3. osserva che l'ordinanza esecutiva n. 14086 consente, in determinati casi, la raccolta generalizzata di dati da parte dell'intelligence dei segnali, compreso il contenuto delle comunicazioni; prende atto al contempo del fatto che l'ordinanza esecutiva n. 14086 stabilisce che la raccolta mirata dovrebbe avere la priorità rispetto a quella generalizzata; rammenta che, sebbene l'ordinanza esecutiva n. 14086 contenga diverse garanzie in caso di raccolta generalizzata, essa non prevede un'autorizzazione preventiva indipendente per la raccolta generalizzata, che non è neppure contemplata dall'ordinanza esecutiva n. 12333; ricorda che, nella sentenza "Schrems II", la CGUE ha chiarito che la sorveglianza degli Stati Uniti non era conforme al diritto dell'UE in quanto non richiedeva un "criterio oggettivo" che fosse "in grado di giustificare" l'interferenza del governo nella vita privata; sottolinea che ciò comprometterebbe la finalità degli obiettivi quale salvaguardia per limitare le attività di intelligence degli Stati Uniti; ricorda che, dopo la direttiva presidenziale n. 28 (PPD-28), che ha costituito la base per la decisione di adeguatezza dello "scudo per la privacy", l'Autorità per la tutela della vita privata e delle libertà civili (PCLOB) ha pubblicato una relazione di riesame[1] e ha concluso che la PPD-28 aveva sostanzialmente mantenuto le prassi esistenti tra gli organismi di intelligence; è convinto che la direttiva presidenziale n. 28 non porrà fine alla sorveglianza elettronica di massa dei cittadini dell'UE da parte delle autorità statunitensi;

4. condivide le preoccupazioni del comitato europeo per la protezione dei dati dovute al fatto che l'ordinanza esecutiva n. 14056 non fornisce sufficienti garanzie nel caso della raccolta generalizzata di dati, vale a dire la mancanza di un'autorizzazione preventiva indipendente, la mancanza di norme chiare e rigorose in materia di conservazione dei dati, la raccolta generalizzata "temporanea" e la mancanza di garanzie più rigorose per quanto riguarda la diffusione di dati ricavati da una raccolta generalizzata; sottolinea in particolare la preoccupazione specifica che, senza ulteriori restrizioni alla diffusione nei confronti delle autorità statunitensi, le autorità di contrasto sarebbero autorizzate ad accedere a dati a cui altrimenti non avrebbero potuto accedere; ricorda che i trasferimenti successivi moltiplicano effettivamente i rischi per la protezione dei dati; prende atto del fatto che il comitato europeo per la protezione dei dati ha chiesto l'inclusione di un obbligo giuridicamente vincolante volto ad analizzare e determinare se un paese terzo offra un livello minimo di garanzie accettabile;

5. sottolinea che l'ordinanza esecutiva n. 14086 non si applica ai dati consultati dalle autorità pubbliche con altri mezzi, ad esempio attraverso il Cloud Act statunitense o il Patriot Act statunitense, mediante acquisti di dati commerciali o accordi volontari di

---

[1] PCLOB, Report to the President on the Implementation of Presidential Directive 28: Signals Intelligence Activities (Relazione destinata al Presidente sull'attuazione della direttiva presidenziale 28: attività di intelligence dei segnali).

condivisione dei dati;

6. sottolinea che il problema di fondo è la sorveglianza delle persone non statunitensi ai sensi del diritto statunitense e il fatto che i cittadini europei non dispongono di effettivi mezzi di ricorso a tale riguardo; chiede che i cittadini dell'UE dispongano degli stessi diritti e privilegi di cui godono i cittadini statunitensi con riguardo alle attività della comunità dell'intelligence statunitense e all'accesso ai tribunali statunitensi;

7. prende atto che, in linea con l'interpretazione statunitense, l'"intelligence dei segnali" comprende tutti i metodi di accesso ai dati previsti dal Foreign Intelligence Surveillance Act (FISA), inclusi quelli dei fornitori di "servizi di computing a distanza" aggiunti nel 2008 con la legge S1881a di modifica della FISA; invita la Commissione a chiarire, in seno a futuri negoziati, la definizione e l'ambito di applicazione di "intelligence dei segnali" nell'ordinanza esecutiva n. 14086; ricorda che, ai sensi della sezione 702 della FISA, il governo statunitense continua a rivendicare il potere di considerare come obiettivo qualsiasi persona non statunitense all'estero per ottenere informazioni di intelligence esterna in senso lato;

8. sottolinea che è stato creato un nuovo meccanismo di ricorso che consente agli interessati dell'UE di presentare una denuncia; insiste nel contempo sul fatto che le decisioni del Tribunale sarebbero classificate e non rese pubbliche o disponibili al denunciante, il quale sarebbe solo informato del fatto che il riesame non ha individuato alcuna violazione contemplata o che il Tribunale ha emesso una decisione che richiede un'azione adeguata, compromettendo in tal modo il suo diritto di accedere ai propri dati o di rettificarli; esprime preoccupazione per il fatto che ciò significa che una persona che avvia un procedimento non avrebbe alcuna possibilità di essere informata in merito all'esito sostanziale della causa e la decisione sarebbe definitiva; prende atto che la procedura di ricorso proposta non prevede una possibilità di ricorso dinanzi a un tribunale federale e pertanto, tra l'altro, non prevede alcuna possibilità per il denunciante di chiedere il risarcimento dei danni; invita la Commissione a proseguire i negoziati con gli Stati Uniti per realizzare i cambiamenti necessari per affrontare tali questioni;

9. osserva che l'ordinanza esecutiva n. 14086 introduce alcune garanzie per garantire l'indipendenza dei giudici del Tribunale, come riconosciuto anche dal comitato europeo per la protezione dei dati nel suo parere; sottolinea che il Tribunale fa parte del potere esecutivo e non della magistratura, e i suoi giudici sono nominati per un mandato fisso di quattro anni; sottolinea che il Presidente degli Stati Uniti può annullare le decisioni del Tribunale, anche in segreto; sottolinea che, nonostante il nuovo meccanismo di ricorso non consenta all'Attorney General degli Stati Uniti di destituire né supervisionare i giudici del Tribunale, ciò non pregiudica i pertinenti poteri del Presidente degli Stati Uniti; sottolinea che, fintanto che il Presidente degli Stati Uniti potrà rimuovere i giudici del Tribunale durante il loro mandato, la loro indipendenza non sarà garantita; osserva che, qualora adottate, la Commissione dovrebbe monitorare attentamente l'applicazione di tali garanzie di indipendenza nella pratica; sottolinea che i denuncianti sarebbero rappresentati da un "avvocato speciale" designato dal Tribunale, per il quale non vi è alcun requisito di indipendenza; invita la Commissione a garantire l'introduzione di un requisito di indipendenza nel caso di adozione di una decisione di adeguatezza; conclude che, allo stato, il Tribunale non soddisfa i requisiti di indipendenza e imparzialità di cui all'articolo 47 della Carta; osserva che, sebbene l'Autorità per la tutela della vita privata e delle libertà civili riesamini in modo indipendente il funzionamento del nuovo processo di ricorso, la portata di tale riesame

sarebbe limitata;

10. osserva che gli Stati Uniti hanno previsto un nuovo meccanismo di ricorso per le questioni relative all'accesso delle autorità pubbliche ai dati, ma rimangono dubbi sull'efficacia dei mezzi di ricorso disponibili per le questioni commerciali, che restano tali ai sensi della decisione di adeguatezza; osserva che i meccanismi volti a risolvere tali questioni sono in gran parte lasciati alla discrezione delle imprese, che possono scegliere vie di ricorso alternative, come i meccanismi di risoluzione delle controversie o il ricorso ai programmi di privacy delle imprese; invita la Commissione, nel caso in cui sia adottata una decisione di adeguatezza, a monitorare attentamente l'efficacia di tali meccanismi di ricorso;

11. osserva che le imprese europee necessitano e meritano certezza giuridica; sottolinea che la successione di meccanismi di trasferimento dei dati, in seguito abrogati dalla CGUE, ha generato costi aggiuntivi per le imprese europee; riconosce, pertanto, la necessità di garantire certezza giuridica ed evitare una situazione in cui le imprese debbano adattarsi costantemente alle nuove soluzioni giuridiche, che potrebbe essere particolarmente onerosa per le microimprese e le piccole e medie imprese; esprime preoccupazione per il fatto che, qualora adottata, la decisione di adeguatezza potrebbe (come i suoi precedenti) essere annullata dalla CJUE, determinando una persistente mancanza di certezza giuridica, ulteriori costi e disagi per i cittadini e le imprese europei;

12. sottolinea che, a differenza di tutti gli altri paesi terzi che si sono dotati di una decisione di adeguatezza a norma del Tribunale, gli Stati Uniti ancora non dispongono di una legge federale sulla protezione dei dati; sottolinea che l'applicazione dell'ordinanza esecutiva n. 14086 non è chiara, precisa né prevedibile, in quanto può essere modificata o revocata in qualsiasi momento dal Presidente degli Stati Uniti, che ha anche il potere di emettere ordinanze esecutive segrete; osserva che il riesame dell'accertamento di adeguatezza dovrebbe aver luogo decorso un anno dalla data di notifica della decisione di adeguatezza agli Stati membri e successivamente almeno ogni quattro anni; invita la Commissione, nel caso in cui sia adottata una futura decisione di adeguatezza, a effettuare riesami successivi almeno ogni tre anni, come richiesto dal parere del comitato europeo per la protezione dei dati; esprime preoccupazione in merito all'assenza di una clausola di decadenza tale che la decisione giunga automaticamente a scadenza quattro anni dopo la sua entrata in vigore, e decorso tale periodo la Commissione dovrebbe adottare una nuova decisione; esprime preoccupazione per il fatto che questa mancanza di una clausola di decadenza in merito alla presente decisione di adeguatezza rappresenti un approccio più indulgente nei confronti degli Stati Uniti, nonostante il quadro statunitense in materia di privacy si basi su un'ordinanza esecutiva che consente modifiche segrete e possa essere modificato senza consultare il Congresso, né informare le controparti dell'UE; invita pertanto la Commissione a introdurre tale clausola;

13. condivide le preoccupazioni del comitato europeo per la protezione dei dati per quanto riguarda i diritti degli interessati, l'assenza di definizioni chiave e di norme specifiche sul processo decisionale automatizzato e la profilazione, la mancanza di chiarezza in merito all'applicazione dei principi del quadro in materia di privacy dei dati ai responsabili del trattamento e la necessità di evitare i trasferimenti successivi che compromettono il livello di protezione;

14. sottolinea che le decisioni di adeguatezza devono includere meccanismi chiari e rigorosi

di monitoraggio e riesame, al fine di garantire che le decisioni siano adeguate alle esigenze future o abrogate o modificate, se necessario, e che sia sempre garantito il diritto fondamentale dei cittadini dell'UE alla protezione dei dati; sottolinea che la futura decisione di adeguatezza dovrebbe essere soggetta a riesame continuo, tenendo conto degli sviluppi giuridici e pratici negli Stati Uniti;

Conclusioni

15. ricorda che, nella sua risoluzione del 20 maggio 2021, il Parlamento ha invitato la Commissione a non adottare alcuna nuova decisione di adeguatezza in relazione agli Stati Uniti, a meno che non siano state introdotte riforme significative, in particolare a fini di sicurezza nazionale e intelligence; non ritiene che l'ordinanza esecutiva n. 14086 sia sufficientemente significativa; ribadisce che la Commissione non dovrebbe lasciare il compito di proteggere i diritti fondamentali dei cittadini dell'UE alla Corte di giustizia dell'Unione europea in conseguenza di denunce presentate dagli stessi singoli cittadini;

16. ricorda che la Commissione deve valutare l'adeguatezza di un paese terzo basandosi sulla legislazione e sulle pratiche in vigore, non solo nella sostanza ma anche nella pratica, come stabilito nelle sentenze Schrems I, Schrems II e nel RGPD (considerando 104);

17. osserva che i principi del quadro in materia di privacy dei dati del Dipartimento del commercio degli Stati Uniti non hanno subito modifiche sufficienti, rispetto a quelle previste dallo scudo per la privacy, al fine di fornire una protezione sostanzialmente equivalente a quella prevista dal RGPD;

18. osserva che, mentre gli Stati Uniti stanno assumendo un impegno importante per migliorare l'accesso ai mezzi di ricorso e alle norme sul trattamento dei dati da parte delle autorità pubbliche, la comunità dell'intelligence statunitense ha tempo fino a ottobre 2023 per aggiornare le proprie politiche e pratiche in linea con l'impegno dell'ordinanza esecutiva n. 14086, e che l'Advocate General degli Stati Uniti non ha ancora definito l'UE e i suoi Stati membri come paesi che soddisfano i requisiti per poter accedere ai mezzi di ricorso disponibili dinanzi al Tribunale; sottolinea che ciò significa che la Commissione non è stata in grado di valutare "in pratica" l'efficacia dei mezzi di ricorso delle misure proposti in materia di accesso ai dati; conclude, pertanto, che la Commissione può solamente procedere con la fase successiva di una decisione di adeguatezza una volta che tali scadenze e obiettivi fondamentali siano soddisfatti dagli Stati Uniti per garantire che gli impegni siano rispettati nella pratica;

19. conclude che il quadro UE-USA in materia di privacy dei dati non crea un'equivalenza essenziale del livello di protezione; invita la Commissione a proseguire i negoziati con le sue controparti statunitensi al fine di creare un meccanismo che garantisca tale equivalenza, nonché l'adeguato livello di protezione richiesto dal diritto dell'Unione in materia di protezione dei dati e dalla Carta secondo l'interpretazione della CGUE; invita la Commissione a non adottare la decisione di adeguatezza fino a quando non saranno pienamente attuate tutte le raccomandazioni formulate nella presente risoluzione e nel parere del comitato europeo per la protezione dei dati;

20. invita la Commissione ad agire nell'interesse delle imprese e dei cittadini dell'UE garantendo che il quadro proposto fornisca una base giuridica solida, sufficiente e orientata al futuro per i trasferimenti di dati UE-USA; si attende che qualsiasi decisione

di adeguatezza, se adottata, sia di nuovo impugnata dinanzi alla CGUE; sottolinea la responsabilità della Commissione nella mancata tutela dei diritti dei cittadini dell'UE nel caso in cui la decisione di adeguatezza sia nuovamente invalidata dalla CGUE;

°

° °

21. incarica la sua Presidente di trasmettere la presente risoluzione al Consiglio, alla Commissione, nonché al Presidente e al Congresso degli Stati Uniti d'America.