Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza

Adottate il 10 novembre 2020

Indice

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE 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 (in appresso: il «RGPD»)[1],

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

visto l'articolo 12 e l'articolo 22 del regolamento interno,

visto il documento di lavoro del Gruppo "Articolo 29" sulla giustificazione delle ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati mediante misure di sorveglianza nel contesto del trasferimento di dati personali (garanzie essenziali europee), WP237,

HA ADOTTATO LE SEGUENTI RACCOMANDAZIONI

1. INTRODUZIONE

1. A seguito della sentenza Schrems I, le autorità competenti per la protezione dei dati personali dell'UE riunite nel gruppo "Articolo 29" hanno fatto riferimento alla giurisprudenza per individuare le garanzie essenziali europee che devono essere rispettate al fine di garantire che, in rapporto al trasferimento di dati personali, le ingerenze nei diritti al rispetto della vita privata e alla protezione dei dati personali mediante misure di sorveglianza non eccedano quanto è necessario e proporzionato in una società democratica.

2. L'EDPB desidera sottolineare che le garanzie essenziali europee si basano sulla giurisprudenza della Corte di giustizia dell'Unione europea (in appresso: CGUE) relativa agli articoli 7, 8, 47 e 52 della Carta dei diritti fondamentali dell'UE (in appresso: la Carta) e, se del caso, sulla giurisprudenza della Corte europea dei diritti dell'uomo (in appresso: CEDH) relativa all'articolo 8 della Convenzione europea dei diritti dell'uomo (in appresso: CEDU) che riguarda le questioni relative alle attività di sorveglianza negli Stati firmatari della CEDU[3].

[1] Il presente documento non riguarda i trasferimenti o le condivisioni successive che ricadano nell'ambito della direttiva "polizia e giustizia" [direttiva (UE) 2016/680].

[2] Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».

[3] Nelle presenti raccomandazioni, il termine «diritti fondamentali» deriva dalla Carta dei diritti fondamentali dell'UE. Tuttavia, esso è utilizzato anche per ricomprendere i «diritti umani» inclusi nella Convenzione europea dei diritti dell'uomo.

3. L'aggiornamento del presente documento, originariamente redatto in risposta alla sentenza Schrems I[4], intende sviluppare ulteriormente le garanzie essenziali europee per tenere conto dei chiarimenti forniti dalla CGUE (e dalla CEDH) successivamente alla sua prima pubblicazione, in particolare nella fondamentale sentenza Schrems II[5].

4. Nella sentenza Schrems II, la CGUE ha dichiarato che l'esame della decisione 2010/87/UE della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi, alla luce degli articoli 7, 8 e 47 della Carta, non ha evidenziato alcun elemento idoneo a inficiarne la validità, ma ha condotto ad annullare la decisione relativa allo «scudo per la privacy» (*Privacy Shield)*. La CGUE ha dichiarato che la decisione relativa allo «scudo per la privacy» è incompatibile con l'articolo 45, paragrafo 1, RGPD, alla luce degli articoli 7, 8 e 47 della Carta. La sentenza può quindi servire da esempio nel caso in cui le misure di sorveglianza in un paese terzo [in questo caso gli Stati Uniti con l'articolo 702 della Foreign Intelligence Surveillance Act (FISA) e il decreto presidenziale (Executive Order) 12333] non siano né sufficientemente limitate né soggette a un ricorso effettivo a disposizione degli interessati per far valere i loro diritti, come richiesto dal diritto dell'UE al fine di considerare il livello di protezione in un paese terzo come «sostanzialmente equivalente» a quello garantito all'interno dell'Unione europea ai sensi dell'articolo 45, paragrafo 1, del RGPD.

5. Le motivazioni che hanno condotto all'invalidazione della decisione relativa allo «scudo per la privacy» comportano conseguenze anche su altri strumenti di trasferimento[6]. Benché la Corte abbia interpretato l'articolo 46, paragrafo 1, del RGPD nel contesto della validità delle clausole contrattuali tipo, la sua interpretazione si applica a qualsiasi trasferimento verso paesi terzi che si fondi su uno qualsiasi degli strumenti di cui all'articolo 46 RGPD[7].

6. In ultima analisi, spetta alla CGUE giudicare se le ingerenze in un diritto fondamentale possano essere giustificate. Tuttavia, in assenza di un tale giudizio e in applicazione della giurisprudenza consolidata, le autorità competenti per la protezione dei dati personali sono tenute a valutare i singoli casi, d'ufficio o a seguito di un reclamo, e a deferire il caso a un tribunale nazionale se sospettano che il trasferimento non sia conforme all'articolo 45 in presenza di una decisione di adeguatezza, oppure a sospendere o vietare il trasferimento se ritengono che l'articolo 46 RGPD non possa essere rispettato e che non sia possibile garantire con altri mezzi la protezione richiesta dal diritto dell'UE per i dati trasferiti.

7. Le garanzie essenziali europee come aggiornate in questo documento intendono fornire elementi utili a valutare se misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possano configurare un'ingerenza giustificabile o meno.

[4] Sentenza della CGUE del 6 ottobre 2015, Maximillian Schrems contro Data Protection Commissioner, causa C-362/14, EU:C:2015:650 (in appresso: Schrems I).

[5] Sentenza della CGUE del 16 luglio 2020, Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems, causa C-311/18, ECLI:EU:C:2020:559 (in appresso: Schrems II).

[6] Cfr. § 105 di Schrems II.

[7] Cfr. § 92 di Schrems II.

8. Infatti, le garanzie essenziali europee fanno parte della valutazione da effettuare per stabilire se un paese terzo fornisca un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE, ma non mirano a definire di per sé tutti gli elementi necessari a ritenere che un paese terzo fornisce tale livello di protezione in conformità dell'articolo 45 del RGPD. Analogamente, esse non mirano a definire di per sé tutti gli elementi che potrebbero essere tenuti presenti nel valutare se il regime giuridico di un paese terzo impedisca all'esportatore e all'importatore di dati di assicurare le adeguate garanzie di cui all'articolo 46 del RGPD.

9. Pertanto, gli elementi forniti nel presente documento dovrebbero essere considerati come le garanzie essenziali da individuare in un paese terzo nel valutare l'ingerenza nei diritti al rispetto della vita privata e alla protezione dei dati derivante dalle misure di sorveglianza applicate in tale paese terzo, e non già un elenco di elementi atti a dimostrare che il regime giuridico di un paese terzo nel suo insieme fornisce un livello di protezione sostanzialmente equivalente.

10. L'articolo 6, paragrafo 3, del trattato sull'Unione europea stabilisce che i diritti fondamentali sanciti dalla CEDU fanno parte del diritto dell'UE in quanto principi generali. Tuttavia, come ricorda la CGUE nella sua giurisprudenza, la CEDU non costituisce, finché l'Unione europea non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'UE[8]. Pertanto, il livello di tutela dei diritti fondamentali richiesto dall'articolo 46, paragrafo 1, del RGPD deve essere determinato sulla base delle disposizioni di tale regolamento, lette alla luce dei diritti fondamentali sanciti dalla Carta. Ciò detto, ai sensi dell'articolo 52, paragrafo 3, della Carta, i diritti in essa contenuti che corrispondono ai diritti garantiti dalla CEDU hanno lo stesso significato e la stessa portata di quelli previsti da tale Convenzione e, di conseguenza, come ricordato dalla CGUE, occorre tener conto della giurisprudenza della CEDH in materia di diritti previsti anche dalla Carta dei diritti fondamentali dell'UE, in quanto livello minimo di protezione per interpretare i corrispondenti diritti della Carta[9]. Secondo l'ultimo comma dell'articolo 52, paragrafo 3, della Carta, tuttavia, «[l]a presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa».

11. Pertanto, la sostanza delle garanzie essenziali continuerà a essere in parte basata sulla giurisprudenza della CEDH, nella misura in cui la Carta, come interpretata dalla CGUE, non preveda un livello di protezione più elevato che prescriva requisiti diversi dalla giurisprudenza della CEDH.

12. Il presente documento illustra il contesto e approfondisce ulteriormente le quattro garanzie essenziali europee.

2. INGERENZE NEI DIRITTI FONDAMENTALI

13. I diritti fondamentali al rispetto della vita privata e familiare, comprese le comunicazioni, e alla protezione dei dati personali sono stabiliti dagli articoli 7 e 8 della Carta e si applicano a tutti. L'articolo 8 stabilisce inoltre le condizioni per la liceità del trattamento dei dati personali e riconosce il diritto di accesso e di rettifica, oltre a imporre che tali norme siano soggette al controllo di un'autorità indipendente.

[8] Cfr. § 98 di Schrems II.

[9] Cfr. § 124 delle cause riunite C-511/18, C-512/18 e C-520/18, La Quadrature du Net et al. (in appresso: La Quadrature du Net et al.).

14. «[L]'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, in quanto tale, un trattamento di dati personali»[10]. Pertanto, gli articoli 7 e 8 della Carta si applicano a questa specifica operazione e la loro protezione si estende ai dati trasferiti, motivo per cui gli interessati i cui dati personali sono trasferiti verso un paese terzo devono poter beneficiare di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione europea[11].

15. Secondo la CGUE, quando il diritto fondamentale al rispetto della vita privata sancito dall'articolo 7 della Carta è pregiudicato, mediante il trattamento di dati personali di una persona, anche il diritto alla protezione dei dati è pregiudicato, in quanto tale trattamento rientra nell'ambito di applicazione dell'articolo 8 della Carta e, di conseguenza, deve necessariamente soddisfare il requisito di protezione dei dati previsto da tale articolo[12].

16. Pertanto, per quanto riguarda l'eventuale ingerenza nei diritti fondamentali ai sensi del diritto dell'UE, l'obbligo imposto ai fornitori di servizi di comunicazione elettronica [...] di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto degli articoli 7 e 8 della Carta[13]. Le stesse questioni si pongono anche per altre tipologie di trattamento di dati, come la loro trasmissione a soggetti diversi dagli utenti o l'accesso ai dati ai fini del loro utilizzo[14], che pertanto comportano un'ingerenza in tali diritti fondamentali. Inoltre, l'accesso di un'autorità pubblica ai dati costituisce un'ingerenza ulteriore, secondo una giurisprudenza consolidata[15].

17. Al fine di individuare un'ingerenza, non importa «che le informazioni relative alla vita privata di cui trattasi abbiano o meno natura sensibile, o che gli interessati abbiano o meno subito eventuali inconvenienti per effetto di tale ingerenza[16]». La CGUE ha inoltre sottolineato che è irrilevante[17] il fatto che i dati conservati siano stati o meno utilizzati successivamente.

18. Tuttavia, i diritti sanciti agli articoli 7 e 8 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale[18].

19. La Carta prevede un test di necessità e proporzionalità per configurare le limitazioni ai diritti che tutela. L'articolo 52, paragrafo 1, della Carta specifica la portata delle possibili limitazioni ai diritti di cui agli articoli 7 e 8, affermando che «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

[10] CGUE, Schrems II, § 83.
[11] CGUE, Schrems II, § 96.
[12] CGUE, Schrems II, §§ 170-171.
[13] CGUE, causa C-623/17, Privacy International (in appresso: Privacy International), § 60.
[14] CGUE, Privacy International, § 61.
[15] CEDH, Leander, § 48; CEDH, Rotaru, § 46; CGUE, Digital Rights Ireland, § 35.
[16] CGUE, Schrems II, § 171, compresa la giurisprudenza citata.
[17] CGUE, Schrems II, § 171, compresa la giurisprudenza citata.
[18] CGUE, Privacy International, § 63.

20. La CGUE ha ribadito che la legislazione dell'UE che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta «deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi», in particolare quando i dati personali sono sottoposti a trattamento automatico e «qualora esista un rischio considerevole di accesso illecito ai dati stessi»[19].

21. Secondo la CGUE, la tutela del diritto al rispetto della vita privata richiede che le deroghe e le restrizioni al diritto alla protezione dei dati «debbano operare entro i limiti dello stretto necessario». Inoltre, un obiettivo di interesse generale deve essere conciliato con i diritti fondamentali interessati dalla misura, «effettuando un equilibrato contemperamento» tra l'obiettivo e i diritti in questione[20].

22. Ne consegue che l'accesso, la conservazione e il successivo utilizzo di dati personali da parte delle autorità pubbliche nell'ambito delle misure di sorveglianza non devono superare i limiti dello stretto necessario, valutato alla luce della Carta, altrimenti «non [possono] essere [considerati giustificati] in una società democratica»[21].

23. Le quattro garanzie essenziali europee, così come sono sviluppate nel capitolo successivo, intendono specificare ulteriormente come valutare il livello di ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati nel contesto delle misure di sorveglianza applicate da autorità pubbliche di un paese terzo, in presenza di un trasferimento di dati personali, e quali requisiti giuridici devono essere conseguentemente in vigore per valutare se tali ingerenze siano accettabili ai sensi della Carta.

3. LE GARANZIE ESSENZIALI EUROPEE

24. In seguito all'analisi della giurisprudenza, l'EDPB ritiene che i requisiti giuridici applicabili per rendere giustificabili le limitazioni ai diritti alla protezione dei dati e al rispetto della vita privata riconosciuti dalla Carta possano essere riassunti in quattro garanzie essenziali europee:

A. Il trattamento deve basarsi su regole chiare, precise e accessibili
B. Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti
C. Dovrebbe esistere un meccanismo di controllo indipendente
D. La persona deve poter accedere a mezzi di ricorso efficaci

25. Le garanzie si basano sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati che si applicano a tutti, indipendentemente dalla nazionalità.

[19] CGUE, Privacy International, § 68 e giurisprudenza ivi menzionata.
[20] CGUE, Privacy International, § 67 e giurisprudenza ivi menzionata.
[21] CGUE, Privacy International, § 81.

Garanzia A - Il trattamento deve basarsi su regole chiare, precise e accessibili

26. Ai sensi dell'articolo 8, paragrafo 2, della Carta, i dati personali devono, in particolare, essere trattati «per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge»[22], come la CGUE ha ricordato nella sentenza Schrems II. Inoltre, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta all'interno dell'UE devono essere previste dalla legge. Pertanto, un'ingerenza giustificabile deve essere conforme alla legge.

27. Questa base giuridica dovrebbe definire regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano alcune salvaguardie minime[23]. Inoltre, la Corte ha ricordato che «[la] normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale»[24]. A questo proposito, la CGUE ha chiarito che la valutazione del diritto applicabile dei paesi terzi dovrebbe concentrarsi sulla possibilità riconosciuta alle persone di invocarlo e azionarlo dinanzi ai giudici[25]. La Corte indica pertanto che i diritti riconosciuti agli interessati devono essere azionabili; qualora alle persone non siano concessi diritti opponibili alle autorità pubbliche, il livello di protezione non può essere considerato sostanzialmente equivalente a quello derivante dalla Carta, contrariamente al requisito di cui all'articolo 45, paragrafo 2, lettera a), del RGPD[26].

28. Inoltre, la Corte ha sottolineato che il diritto applicabile deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che preveda il trattamento dei dati in questione[27] (cfr. *infra* alla garanzia B il rapporto fra tali requisiti e i principi di necessità e proporzionalità).

29. Inoltre, la CGUE ha indicato che «il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato»[28].

30. Infine, la Corte europea dei diritti dell'uomo «non ritiene che sussistano fondati motivi per giustificare l'applicazione di principi differenti alla questione dell'accessibilità e della chiarezza delle regole che governano, da un lato, l'intercettazione di comunicazioni individuali, e, dall'altro, i più generali programmi di sorveglianza»[29]. La CEDH ha inoltre chiarito che la base giuridica dovrebbe comprendere almeno una definizione delle categorie di persone che potrebbero essere soggette a sorveglianza, un limite alla durata della misura, la procedura da seguire per l'esame, l'utilizzo e la

[22] Cfr. § 173 di Schrems II.

[23] Cfr. § 175 e § 180 di Schrems II e il parere 1/15 [accordo UE-Canada sul codice di prenotazione (Passenger Name Record, PNR)] del 26 luglio 2017, § 139 e la giurisprudenza citata.

[24] Cfr. § 68 di Privacy International – Si fa notare che nella versione francese della sentenza la Corte usa la parola «réglementation», che è più ampia rispetto ai soli atti del Parlamento.

[25] Cfr. § 181 di Schrems II; in tale paragrafo la CGUE si riferisce alla direttiva presidenziale 28 (Presidential Policy directive 28) degli Stati Uniti.

[26] Cfr. § 181 di Schrems II.

[27] Cfr. § 68 di Privacy International, in relazione al diritto degli Stati membri.

[28] Cfr. Schrems II, § 175 e la giurisprudenza citata, nonché Privacy International, § 65.

[29] CEDH, Liberty, § 63.

conservazione dei dati ottenuti e le precauzioni da adottare nella comunicazione dei dati ad altre parti[30].

31. Infine, l'ingerenza deve essere prevedibile nei suoi effetti sulla persona, al fine di garantire una protezione adeguata ed efficace contro le ingerenze arbitrarie e il rischio di abusi. Di conseguenza, il trattamento deve fondarsi su una base giuridica precisa, chiara ma anche accessibile (cioè pubblica)[31]. La CEDH, in merito a tale questione, ha ricordato nel caso Zakharov che «la nozione di "prevedibilità" nel contesto dell'intercettazione delle comunicazioni non può essere interpretata secondo gli stessi parametri utilizzati in molti altri campi». Ha precisato che nel contesto delle misure segrete di sorveglianza, quali l'intercettazione delle comunicazioni, «la prevedibilità non può significare che una persona debba essere in grado di prevedere quando le autorità potrebbero intercettare le sue comunicazioni in modo da poter adattare il suo comportamento di conseguenza». Tuttavia, considerando che in questo tipo di situazione i rischi di arbitrarietà sono evidenti, «è essenziale avere regole chiare e dettagliate sull'intercettazione delle conversazioni telefoniche, tanto più che la tecnologia disponibile per tale scopo diventa sempre più sofisticata. Il diritto nazionale deve essere sufficientemente chiaro da fornire ai cittadini un'indicazione adeguata in merito alle circostanze in cui e alle condizioni alle quali le autorità pubbliche possono ricorrere a tali misure»[32].

Garanzia B - Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti

32. In conformità del primo comma dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta devono rispettare il contenuto essenziale di detti diritti e libertà. Ai sensi del secondo comma dell'articolo 52, paragrafo 1, della Carta, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[33].

33. Per quanto riguarda il **principio di proporzionalità**, la Corte ha dichiarato, in relazione alle legislazioni degli Stati membri, che la giustificabilità di una limitazione dei diritti al rispetto della vita privata e alla protezione dei dati deve essere valutata, da un lato, misurando la **gravità dell'ingerenza** che tale limitazione comporta[34] e, dall'altro, verificando che l'**importanza dell'obiettivo di interesse generale** perseguito attraverso tale limitazione sia proporzionata alla suddetta gravità[35].

34. In La Quadrature du Net et al., si può osservare che la CGUE ha stabilito, in relazione al diritto di uno Stato membro e non al diritto di un paese terzo, che l'obiettivo di salvaguardia della sicurezza nazionale è, per la sua importanza, idoneo a giustificare misure che comportino ingerenze nei diritti

[30] CEDH, Weber e Saravia, § 95.

[31] CEDH, Malone, §§ 65 e 66.

[32] CEDH, Zakharov, § 229.

[33] Schrems II, § 174.

[34] In tale contesto, il giudice ha rilevato, ad esempio, che «l'ingerenza derivante dalla raccolta in tempo reale dei dati che consentono di localizzare un'apparecchiatura terminale risulta particolarmente grave, dato che tali dati forniscono alle autorità nazionali competenti uno strumento di controllo preciso e permanente degli spostamenti degli utenti dei telefoni mobili [...]» (La Quadrature du Net et al., § 187, compresa la giurisprudenza citata).

[35] La Quadrature du Net et al., § 131.

fondamentali più gravi di quelle che potrebbero essere giustificate da altri obiettivi, come la lotta alla criminalità. Essa ha tuttavia constatato che ciò vale fintantoché ricorrano circostanze sufficientemente concrete tali da consentire di ritenere che lo Stato interessato si trovi dinanzi a una minaccia grave alla sicurezza nazionale, che si dimostri reale e attuale o prevedibile, e a condizione che siano soddisfatti gli altri requisiti di cui all'articolo 52, paragrafo 1, della Carta[36].

35. A tal proposito, secondo la giurisprudenza consolidata della Corte, le deroghe e le limitazioni alla protezione dei dati personali devono essere applicate solo nella misura strettamente necessaria[37]. Per soddisfare tale requisito, oltre a stabilire regole chiare e precise che disciplinano la portata e l'applicazione della misura in questione, la legislazione deve imporre alcune salvaguardie minime in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti a proteggere efficacemente i loro dati personali contro il rischio di abusi. «In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato»[38].

36. In Schrems II, la CGUE ha sottolineato che la legislazione di un paese terzo che non indica alcuna limitazione al potere da essa conferito di attuare programmi di sorveglianza ai fini dell'intelligence esterna non può assicurare un livello di protezione sostanzialmente equivalente a quello garantito dalla Carta. Infatti, secondo la giurisprudenza, una base giuridica che consente ingerenze nei diritti fondamentali, al fine di soddisfare i requisiti del principio di proporzionalità, deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi[39].

37. Per quanto riguarda il **principio di necessità**, la CGUE ha chiarito che le legislazioni «che autorizzano, su base generalizzata, la conservazione dei dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione Europea [...] senza che sia fatta alcuna distinzione, limitazione o eccezione alla luce dell'obiettivo perseguito e senza che sia stabilito un criterio oggettivo per determinare i limiti dell'accesso delle autorità pubbliche ai dati e del loro successivo utilizzo, per finalità specifiche, strettamente limitate e atte a giustificare l'ingerenza che l'accesso ai dati e il loro utilizzo comportano», non rispettano tale principio[40]. In particolare, le leggi che consentono alle autorità pubbliche di

[36] §§ 136 e 137. Cfr. anche Privacy International: come precisato dalla Corte, tali minacce possono essere distinte, per la loro natura e la loro particolare gravità, dal rischio generale che si verifichino tensioni o perturbazioni, anche gravi, della pubblica sicurezza. § 75. Ad esempio, nella causa La Quadrature du Net et al., la Corte ha rilevato che l'analisi automatizzata dei dati relativi al traffico e all'ubicazione appare come un'ingerenza particolarmente grave in quanto riguarda in modo generalizzato e indifferenziato i dati delle persone che si avvalgono dei mezzi di comunicazione elettronica; una tale misura può soddisfare il requisito di proporzionalità solo in situazioni nelle quali lo Stato membro interessato si trovi di fronte ad una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile e, in particolare, a condizione che la durata di tale conservazione sia limitata allo stretto necessario (§§ 174-177).

[37] Schrems II, § 176, compresa la giurisprudenza citata.

[38] Schrems II, § 175.

[39] Schrems II, § 180.

[40] Schrems I, § 93 e ulteriori riferimenti. Cfr., ma in relazione al diritto di uno Stato membro e non a quello di un paese terzo, Privacy International, § 71, inclusa la giurisprudenza citata. In questo caso, la Corte ha affermato che la legislazione di uno Stato membro che impone ai fornitori di servizi di comunicazione elettronica di comunicare i dati relativi al traffico e all'ubicazione alle agenzie di sicurezza e di intelligence mediante una trasmissione

accedere in maniera generalizzata al contenuto di comunicazioni elettroniche devono essere ritenute pregiudizievoli del contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta[41].

38. Analogamente, ma nel valutare il diritto di uno Stato membro e non quello di un paese terzo, la CGUE ha affermato, nella sentenza La Quadrature du Net et al., che «una normativa che preveda una conservazione dei dati personali deve sempre rispondere a criteri oggettivi, che pongano un rapporto tra i dati personali da conservare e l'obiettivo perseguito»[42]. Nello stesso contesto, nella sentenza Privacy International, ha affermato inoltre che il legislatore «deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in cui dev'essere concesso alle autorità nazionali competenti l'accesso ai dati di cui trattasi»[43].

Garanzia C - Meccanismo di controllo indipendente

39. L'EDPB ricorda che un'ingerenza avviene al momento della raccolta dei dati, ma anche al momento dell'accesso ai dati da parte di un'autorità pubblica in vista di un trattamento ulteriore. La CEDH ha specificato più volte che qualsiasi ingerenza nel diritto al rispetto della vita privata e alla protezione dei dati deve essere soggetta a un sistema di controllo efficace, indipendente e imparziale che deve essere previsto da un giudice o da un altro organo indipendente[44] (ad esempio un'autorità amministrativa o un organo parlamentare). Il controllo indipendente dell'attuazione delle misure di sorveglianza è stato preso in considerazione anche dalla CGUE nella sentenza Schrems II[45].

40. La CEDH precisa che, se da un lato l'autorizzazione preventiva (giudiziaria) delle misure di sorveglianza costituisce un requisito importante contro l'arbitrarietà, dall'altro occorre anche tener conto del funzionamento concreto del sistema di intercettazione, compresi i meccanismi tesi ad assicurare l'esercizio equilibrato del potere, nonché dell'esistenza o meno di un effettivo abuso[46]. Nel

generale e indifferenziata supera i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, come richiesto dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, letta alla luce della Carta (§ 81).

[41] Schrems I, § 94.

[42] La Quadrature du Net et al., § 133. In tale contesto, la Corte ha confermato che le misure legislative che prevedono, in via preventiva, la conservazione generale e indifferenziata dei dati relativi al traffico e all'ubicazione sono vietate dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, letta alla luce della Carta. Per contro, la Corte ha stabilito che, in situazioni di grave minaccia alla sicurezza nazionale che si dimostri reale e presente o prevedibile, il legislatore può consentire, per la salvaguardia della sicurezza nazionale, il ricorso a un'istruzione che imponga ai fornitori di servizi di comunicazione elettronica di conservare, in modo generale e indifferenziato, i dati relativi al traffico e all'ubicazione. Tale misura deve tuttavia soddisfare condizioni specifiche. In particolare, l'istruzione può essere impartita solo per un periodo di tempo limitato allo stretto necessario, che può essere prorogato se tale minaccia persiste (§ 168).

[43] Privacy International, § 78, compresa la giurisprudenza citata. Nella causa Privacy International, per quanto riguarda l'accesso di un'autorità ai dati personali forniti ai sensi della legge di uno Stato membro, la Corte ha stabilito che «un accesso generale a tutti i dati conservati, in mancanza di qualunque nesso, anche indiretto, con la finalità perseguita, non può essere considerato limitato allo stretto necessario» (§ 77-78).

[44] CEDH, Klass, §§ 17, 51.

[45] Schrems II, §§ 179, 183.

[46] CEDH, Big Brother Watch in appello, §§ 319-320.

caso Schrems II, la CGUE ha tenuto conto anche dell'ambito della vigilanza affidata al meccanismo di controllo, che non comprendeva le singole misure di sorveglianza[47].

41. Per quanto riguarda il diritto degli Stati membri, la CGUE ha individuato una serie di misure che sono conformi al diritto dell'UE solo qualora siano soggette a un controllo effettivo da parte di un tribunale o di un'autorità amministrativa indipendente la cui decisione sia vincolante. Lo scopo di tale controllo è verificare l'esistenza di una situazione che giustifichi la misura in questione, e il rispetto delle condizioni e delle garanzie che devono essere previste[48]. Per quanto riguarda la raccolta in tempo reale dei dati relativi al traffico e all'ubicazione, l'esame dovrebbe consentire di verificare ex ante, tra l'altro, se essa sia autorizzata solo nei limiti dello stretto necessario. In caso di emergenza debitamente giustificata, le misure possono essere applicate senza tale controllo preventivo; tuttavia, la Corte richiede comunque che il controllo successivo intervenga tempestivamente[49].

42. Per quanto riguarda l'indipendenza dei meccanismi di controllo in relazione alle misure di sorveglianza, si può tener conto delle conclusioni della CGUE in merito all'indipendenza di un organismo nell'esercizio di mezzi di ricorso (cfr. *infra* alla garanzia D). Inoltre, la giurisprudenza della CEDH può offrire ulteriori elementi. Quest'ultima, infatti, si è espressa nel senso di preferire che il controllo sia affidato a un giudice. Tuttavia, non è escluso che un altro organismo possa essere incaricato di tale controllo, «purché sia sufficientemente indipendente dall'esecutivo»[50] e «dalle autorità che effettuano la sorveglianza, e [sia] dotato di poteri e competenze sufficienti per esercitare un controllo efficace e continuo»[51]. La CEDH ha aggiunto che occorre tenere in considerazione «le modalità di nomina e lo status giuridico dei membri dell'organismo di controllo»[52] nel valutarne l'indipendenza. Ciò include «persone qualificate a ricoprire una funzione giurisdizionale, nominate dal parlamento o dal Primo ministro. Al contrario, un ministro dell'Interno, che non solo era di nomina politica e membro dell'esecutivo, ma era direttamente coinvolto nella messa in funzione di misure speciali di sorveglianza, è stato giudicato non sufficientemente indipendente»[53]. La CEDH «osserva inoltre che è essenziale che l'organo di vigilanza abbia accesso a tutti i documenti pertinenti, compreso il materiale riservato»[54]. Infine, la CEDH prende in considerazione «se le attività dell'organo di controllo siano soggette al controllo pubblico»[55].

Garanzia D - La persona deve poter accedere a mezzi di ricorso efficaci

43. L'ultima garanzia essenziale europea è legata ai diritti di ricorso della persona, che deve poter disporre di un mezzo di ricorso efficace per soddisfare i suoi diritti quando ritiene che essi non siano o non siano stati rispettati. Nella sentenza Schrems I la CGUE ha spiegato che «una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati non rispetta il contenuto

[47] Schrems II, § 179.
[48] CGUE, La Quadrature du Net et al., §§ 168, 189.
[49] CGUE, La Quadrature du Net et al., § 189.
[50] CEDH, Zakharov, § 258, Iordachi et al. C. Moldavia, §§ 40 e 51, e Dumitru Popescu c. Romania, §§ 70-73.
[51] CDEH, Klass § 56 e Big Brother Watch in appello, § 318.
[52] CEDH, Zakharov, § 278.
[53] CEDH, Zakharov, § 278.
[54] CEDH, Zakharov, § 281.
[55] CEDH, Zakharov, § 283.

essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo»[56].

44. Nel valutare il diritto di uno Stato membro che consente la raccolta in tempo reale dei dati relativi al traffico e all'ubicazione, la Corte ha ritenuto che la comunicazione alla persona interessata sia necessaria «per consentire a dette persone di esercitare i loro diritti, derivanti dagli articoli 7 e 8 della Carta, di chiedere l'accesso ai propri dati personali costituenti l'oggetto di tali misure e, se del caso, la rettifica o la cancellazione degli stessi, nonché di proporre, conformemente all'articolo 47, primo comma, della Carta, un ricorso effettivo dinanzi a un giudice»[57]. Tuttavia, ha anche riconosciuto che la comunicazione alle persone i cui dati sono stati raccolti o analizzati deve avvenire soltanto nella misura e a partire dal momento in cui essa non può più compromettere lo svolgimento dei compiti che sono di pertinenza delle specifiche autorità[58].

45. Anche per la CEDH la questione dell'esistenza di un mezzo di ricorso efficace è indissolubilmente legata alla comunicazione alla persona dell'applicazione di una misura di sorveglianza una volta terminata la sorveglianza stessa. In particolare, la Corte ha ritenuto che «in linea di principio vi sono scarse possibilità di ricorso al giudice da parte della persona interessata, a meno che quest'ultima non sia informata delle misure adottate a sua insaputa e possa quindi contestarne la legalità a posteriori o, in alternativa, a meno che chiunque sospetti che le sue comunicazioni siano o siano state intercettate possa rivolgersi al giudice, di modo che la competenza del giudice non dipenda dalla comunicazione al soggetto intercettato dell'avvenuta intercettazione delle sue comunicazioni»[59]. La CEDH ha quindi riconosciuto che in alcuni casi potrebbe non esserci alcuna comunicazione, ma è necessario prevedere sempre un mezzo di ricorso efficace. In questo caso, la Corte ha chiarito, ad esempio nella causa Kennedy, che un tribunale offre sufficienti possibilità di ricorso qualora soddisfi una serie di criteri, vale a dire sia un organo indipendente e imparziale, che abbia adottato un proprio regolamento interno, sia composto da membri che devono ricoprire o aver ricoperto alte cariche giudiziarie o essere avvocati esperti, e non vi sia alcuna soglia di ordine probatorio da superare per poterlo adire[60]. Nell'esaminare le denunce dei singoli, il tribunale deve avere accesso a tutte le informazioni pertinenti[61], compreso il materiale riservato. Infine, dovrebbe avere il potere di disporre rimedi in caso di inosservanza[62].

[56] CGUE, Schrems I, § 95.
[57] Cfr. § 190 di La Quadrature du Net et al. E CGUE, parere 1/15, § 220.
[58] Cfr. § 191 di La Quadrature du Net et al..
[59] CEDH, Zakharov, § 234.
[60] CEDH, Kennedy, § 190.
[61] L'EDPB osserva che il Commissario per i diritti umani del Consiglio d'Europa ritiene che la cosiddetta regola dei «terzi», in base alla quale le agenzie di intelligence di un paese che forniscono dati alle agenzie di intelligence di un altro paese possono imporre agli organismi riceventi l'obbligo di non divulgare i dati trasferiti a terzi, non dovrebbe applicarsi agli organismi di controllo per non compromettere la possibilità di un ricorso efficace (Issue Paper on Democratic and effective oversight of national security services).
[62] CEDH, Kennedy, § 167.

46. L'articolo 47 della Carta fa riferimento a un tribunale, anche se nelle versioni linguistiche diverse dall'inglese la preferenza è data alla parola «giudice»[63], mentre la CEDU si limita a prevedere l'obbligo per gli Stati membri di garantire che «ogni persona i cui diritti e le cui libertà siano stati violati, [abbia] diritto a un ricorso effettivo davanti a un'istanza nazionale»[64], che non deve necessariamente essere un'autorità giudiziaria[65].

47. La CGUE, nel contesto della sentenza Schrems II, nel valutare l'adeguatezza del livello di protezione di un paese terzo, ha ribadito che «i singoli devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati»[66]. Nello stesso contesto, la CGUE ritiene che un'efficace protezione giudiziaria contro tali interferenze possa essere assicurata non solo da un tribunale, ma anche da un organo[67] che offra garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta. Nella sentenza Schrems II, la CGUE ha sottolineato che l'indipendenza del giudice o dell'organo deve essere assicurata, in particolare nei confronti del potere esecutivo, con tutte le garanzie necessarie, anche per quanto riguarda le condizioni di revoca o annullamento della nomina[68], e che i poteri che dovrebbero essere concessi a un giudice devono essere conformi ai requisiti dell'articolo 47 della Carta. A tale riguardo, all'organo[69] deve essere conferito il potere di adottare decisioni vincolanti per i servizi di intelligence, nel rispetto di garanzie giuridiche che gli interessati possano invocare[70].

4. OSSERVAZIONI CONCLUSIVE

48. Le quattro garanzie essenziali europee sono da considerarsi elementi fondamentali per valutare il livello di ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati. Esse non dovrebbero essere valutate in modo indipendente, essendo in realtà strettamente interconnesse, bensì complessivamente, esaminando la legislazione pertinente in relazione alle misure di sorveglianza, al livello minimo di garanzie per la protezione dei diritti degli interessati e ai mezzi di ricorso previsti dalla legislazione nazionale del paese terzo.

49. Tali garanzie richiedono un certo grado di interpretazione, soprattutto perché la legislazione del paese terzo non deve necessariamente essere identica al quadro giuridico dell'UE.

50. Come ha affermato la Corte europea dei diritti dell'uomo nel caso Kennedy, «la valutazione dipende da tutte le circostanze del caso, come la natura, la portata e la durata delle possibili misure, i requisiti necessari per disporne l'adozione, le autorità competenti ad autorizzarle, applicarle e controllarle e la tipologia dei mezzi di ricorso previsti dal diritto nazionale»[71].

---

[63] La parola «tribunale» è ad esempio tradotta come «Gericht» in tedesco e «gerecht» in olandese.

[64] Articolo 13 della CEDU

[65] CEDH, Klass § 67.

[66] Cfr. § 194 di Schrems II.

[67] Cfr. § 197 di Schrems II, in cui la Corte usa espressamente tale termine.

[68] Cfr. § 195 di Schrems II.

[69] Cfr. § 197 di Schrems II, in cui la Corte usa espressamente tale termine.

[70] Cfr. § 196 di Schrems II.

[71] CEDH, Kennedy, § 153.

51. Di conseguenza, la valutazione delle misure di sorveglianza dei paesi terzi rispetto alle garanzie essenziali europee può portare a due conclusioni:

- la legislazione del paese terzo in questione non soddisfa i requisiti delle garanzie essenziali europee: in questo caso, la legislazione del paese terzo non offrirebbe un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE;

- la legislazione del paese terzo in questione soddisfa le garanzie essenziali europee.

52. Nel valutare l'adeguatezza del livello di protezione, ai sensi dell'articolo 45 del RGPD, la Commissione dovrà valutare se le garanzie essenziali europee siano soddisfatte nel quadro degli elementi da considerare per garantire che la legislazione del paese terzo nel suo insieme offra un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.

53. Quando gli esportatori di dati si affidano, insieme agli importatori di dati, ad adeguate garanzie ai sensi dell'articolo 46 del RGPD, tenuto conto dei requisiti della legislazione dei paesi terzi specificamente applicabili ai dati trasferiti, essi dovrebbero garantire che sia effettivamente raggiunto un livello di protezione sostanzialmente equivalente. In particolare, qualora la legislazione del paese terzo non sia conforme ai requisiti delle garanzie essenziali europee, ciò comporterebbe garantire che la legislazione in questione non pregiudichi le garanzie e le salvaguardie relative al trasferimento affinché sia comunque assicurato un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.

54. L'EDPB ha pubblicato ulteriori linee-guida e raccomandazioni da prendere in considerazione nel procedere alla valutazione, a seconda dello strumento di trasferimento da utilizzare e della necessità di fornire garanzie adeguate, comprese, se del caso, misure supplementari[72].

55. Inoltre, va osservato che le garanzie essenziali europee si basano su quanto previsto dalla legge. L'EDPB sottolinea che le garanzie essenziali europee sono fondate sui diritti fondamentali, i quali si applicano a tutti, indipendentemente dalla nazionalità.

56. L'EDPB ribadisce che le garanzie essenziali europee sono uno standard di riferimento per valutare l'ingerenza che le misure di sorveglianza di paesi terzi comportano nel contesto dei trasferimenti internazionali di dati. Tali standard derivano dal diritto dell'UE e dalla giurisprudenza della CGUE e della CEDH, che è vincolante per gli Stati membri.

[72] Adequacy Referential WP 254 rev.01, riveduto e adottato il 6 febbraio 2018; raccomandazioni 01/2020 dell'EDPB relative alle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE, 10 novembre 2020.