Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie

Adottate il 2 febbraio 2021

Indice

Il Comitato europeo per la protezione dei dati

visto l'articolo 51, paragrafo 1, lettera b), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI RACCOMANDAZIONI

1. INTRODUZIONE

1. Il gruppo di lavoro Articolo 29 ha pubblicato un documento di lavoro[2] sui criteri di riferimento per l'adeguatezza ai sensi del regolamento generale della protezione dei dati[3]. Tale documento di lavoro è stato approvato dal comitato europeo per la protezione dei dati (il "comitato") in occasione della sua prima sessione plenaria.

2. Come affermato nella dichiarazione n. 21 allegata al trattato di Lisbona, potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE).

3. Su questa base, il legislatore dell'UE ha adottato la direttiva (UE) 2016/680 (la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, di seguito "LED") che stabilisce le norme specifiche in materia di trattamento dei dati personali da parte delle autorità competenti a fini di **prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica**.

4. Tale direttiva stabilisce i presupposti che consentono il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale in tale contesto. Uno dei presupposti ai fini di tale trasferimento è la decisione della Commissione europea attestante che il paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato.

5. Mentre il documento di lavoro WP254 rev.01 sui criteri di riferimento per l'adeguatezza mira a fornire orientamenti alla Commissione europea in merito al livello di protezione dei dati nei paesi

[1] GU L 119 del 4.5.2016, pag. 89.
[2] WP254 rev.01, adottato dal gruppo di lavoro Articolo 29 il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, che aggiorna il capitolo I del documento di lavoro "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati", WP12, adottato dal gruppo di lavoro Articolo 29 il 24 luglio 1998.
[3] 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 (GU L 119 del 4.5.2016, pag. 1).

terzi e nelle organizzazioni internazionali ai sensi del regolamento generale sulla protezione dei dati, il presente documento mira a fornire orientamenti analoghi nel quadro della LED. In tale contesto stabilisce i principi fondamentali in materia di protezione dei dati che devono essere presenti nel quadro giuridico di un paese terzo o di un'organizzazione internazionale per garantire un'equivalenza essenziale rispetto al quadro dell'UE nell'ambito di applicazione della LED (ossia per il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali). Inoltre, può fornire orientamenti ai paesi terzi e alle organizzazioni internazionali interessati a ottenere l'adeguatezza.

6. Il presente documento si concentra esclusivamente sulle decisioni di adeguatezza. Si tratta di atti di esecuzione della Commissione europea a norma dell'articolo 36, paragrafo 3, della LED.

2. CONCETTO DI ADEGUATEZZA

7. La LED stabilisce le norme per il trasferimento di dati personali verso paesi terzi e organizzazioni internazionali nella misura in cui tali trasferimenti rientrano nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati personali sono contenute nel capo V di tale direttiva, in particolare negli articoli da 35 a 39.

8. Ai sensi dell'articolo 36 della LED, il trasferimento di dati verso un paese terzo o un'organizzazione internazionale può avvenire se un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Dalla giurisprudenza della Corte di giustizia dell'Unione europea[4] si evince che tale disposizione deve essere letta alla luce dell'articolo 35 della LED, intitolato "Principi generali per il trasferimento di dati personali", il quale stabilisce che "[t]utte le disposizioni del [capo V di tale direttiva] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche assicurato dalla presente direttiva non sia pregiudicato".

9. Se la Commissione europea ha deciso che è garantito un tale livello di protezione adeguato, i trasferimenti di dati personali verso tale paese terzo, territorio, settore od organizzazione internazionale possono avere luogo senza specifiche autorizzazioni, tranne nel caso in cui un altro Stato membro presso cui sono stati ottenuti i dati debba autorizzare il trasferimento, come previsto dagli articoli 35 e 36 e dal considerando 66 della LED. Ciò non pregiudica la necessità che il trattamento dei dati da parte delle autorità degli Stati membri interessati debba essere conforme alle disposizioni nazionali adottate a norma della direttiva (UE) 2016/680.

10. Il concetto di "livello di protezione adeguato", che già esisteva ai sensi della direttiva 95/46[5] e della decisione quadro 2008/977/GAI del Consiglio[6], è stato ulteriormente sviluppato dalla Corte di giustizia dell'Unione europea in questo contesto e, di recente, nel quadro del regolamento generale sulla protezione dei dati.

[4] Causa C-311/18, Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems, 16 luglio 2020, ECLI:EU:C:2020:559, punto 92 (Schrems II).
[5] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).
[6] Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60).

11. Come specificato dalla Corte di giustizia dell'Unione europea, sebbene il livello di protezione nel paese terzo debba essere sostanzialmente equivalente a quello garantito nell'UE, "gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione" ma "tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi"[7]. Il livello di adeguatezza non richiede pertanto di riprodurre punto per punto la legislazione dell'UE, bensì di stabilire i requisiti sostanziali - di base - di tale legislazione.

12. In tale contesto la Corte ha altresì chiarito che una decisione di adeguatezza della Commissione dovrebbe contenere una dichiarazione quanto all'esistenza, nel paese terzo, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso tale paese terzo, ingerenze che entità statali di tale paese sarebbero *autorizzate* a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale[8].

13. Lo scopo delle decisioni di adeguatezza emesse dalla Commissione europea è confermare formalmente con effetto vincolante per gli Stati membri[9], comprese le autorità competenti per la protezione dei dati personali[10], che il livello di protezione dei dati in un paese terzo o in un'organizzazione internazionale è sostanzialmente equivalente al livello di protezione dei dati all'interno dell'Unione europea. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un adeguato livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione, in particolare qualora i dati siano trattati in uno o più settori specifici[11].

14. L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti riconosciuti agli interessati e obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, uniti al controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo o un'organizzazione internazionale, ma anche il sistema vigente per garantirne l'efficacia. La presenza di meccanismi efficienti di applicazione delle norme è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[12].

[7] Causa C−362/14, Maximillian Schrems/Data Protection Commissioner, 6 ottobre 2015, ECLI:EU:C:2015:650, punti 73 e 74 (Schrems I).
[8] *Schrems I*, punto 88.
[9] Articolo 288, paragrafo 2, TFUE.
[10] *Schrems I*, punto 52.
[11] Considerando 67 della LED.
[12] *Schrems I*, punti da 72 a 74 e parere 1/15 della Corte di giustizia dell'Unione europea del 26 luglio 2017 sul progetto di accordo tra il Canada e l'Unione europea, ECLI:EU:C:2017:592 (parere 1/15), punto 134: "[t]ale diritto alla protezione dei dati di carattere personale richiede, in particolare, che la continuità del livello elevato di protezione delle libertà e dei diritti fondamentali riconosciuti dal diritto dell'Unione sia garantita in caso di trasferimento di dati personali dall'Unione a un paese terzo. Anche se le misure dirette ad assicurare un siffatto livello di protezione possono essere diverse da quelle attuate all'interno dell'Unione al fine di garantire il rispetto degli obblighi risultanti dal diritto dell'Unione, tali misure devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione".

3. ASPETTI PROCEDURALI PER I RISCONTRI RELATIVI ALL'ADEGUATEZZA A NORMA DELLA LED

15. Al fine di adempiere il proprio compito di fornire consulenza alla Commissione europea a norma dell'articolo 51, paragrafo 1, lettera g), della LED, il comitato deve ricevere tutta la documentazione necessaria, compresa la corrispondenza pertinente e le conclusioni tratte dalla Commissione europea. È assolutamente necessario che tutti i documenti pertinenti siano trasmessi al comitato con sufficiente anticipo, e tradotti in inglese, per consentire discussioni informate e utili prima dell'adozione definitiva delle decisioni di adeguatezza. Se il quadro giuridico è complesso, dovrebbero essere fornite anche eventuali relazioni sul livello di protezione dei dati nel paese terzo o nell'organizzazione internazionale. In ogni caso, le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e consentire al comitato di valutare l'analisi condotta dalla Commissione in merito al livello di protezione dei dati nel paese terzo o presso l'organizzazione internazionale.

16. Il comitato fornirà in tempo utile un parere sui riscontri della Commissione europea, individuando eventuali carenze nel quadro giuridico in materia di adeguatezza e formulando eventuali raccomandazioni ove necessario.

17. A norma dell'articolo 36, paragrafo 4, della LED, spetta alla Commissione europea controllare su base continuativa gli sviluppi che potrebbero incidere sul funzionamento delle decisioni di adeguatezza.

18. L'articolo 36, paragrafo 3, della LED stabilisce che deve essere effettuato un riesame periodico almeno ogni quattro anni. Si tratta di un'indicazione temporale generica, che deve essere adattata a ciascun paese terzo o a ciascuna organizzazione internazionale tramite la decisione di adeguatezza. A seconda delle circostanze particolari del caso, potrebbe essere giustificata una frequenza più breve. Inoltre, un incidente o nuove informazioni sul quadro giuridico del paese terzo o dell'organizzazione internazionale o una modifica dello stesso potrebbero rendere necessario anticipare il riesame rispetto al previsto. Sarebbe inoltre opportuno procedere tempestivamente a un primo riesame di una decisione di adeguatezza interamente nuova e adattare progressivamente il ciclo di riesame in base all'esito di tale attività.

19. Alla luce del compito del comitato di fornire alla Commissione un parere per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione, il comitato deve ricevere a tempo debito dalla Commissione europea informazioni significative sul monitoraggio degli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale in questione. Il comitato dovrebbe quindi essere tenuto informato su eventuali processi di riesame e missioni di valutazione in corso nel paese terzo o con riferimento all'organizzazione internazionale. Il comitato raccomanda di essere invitato a partecipare a tali processi di riesame e missioni, come previsto nella decisione sullo scudo per la privacy e nella decisione di adeguatezza relativa al Giappone.

20. Va inoltre rilevato che, a norma dell'articolo 36, paragrafo 5, della LED, la Commissione europea ha la facoltà di revocare, modificare o sospendere le decisioni di adeguatezza in vigore nel caso in cui il paese terzo o l'organizzazione internazionale non garantisca più un livello di protezione adeguato. La procedura di revoca, modifica o sospensione coinvolge il comitato, chiamato a esprimere il suo parere in merito conformemente all'articolo 51, paragrafo 1, lettera g), della LED.

21. Inoltre, fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale, le autorità di controllo dovrebbero avere la facoltà di agire in sede giudiziale o stragiudiziale in caso di violazione della LED[13]. Dalla sentenza *Schrems I* della Corte di giustizia dell'Unione europea si desume in particolare che le autorità di protezione dei dati devono essere in grado di avviare procedimenti giudiziari dinanzi gli organi giurisdizionali nazionali qualora ritengano che un reclamo promosso da una persona nei confronti di una decisione di adeguatezza sia ben fondato[14]. La sentenza *Schrems II* ha confermato tale valutazione[15].

4. NORME UE CONCERNENTI L'ADEGUATEZZA NELLA COOPERAZIONE DI POLIZIA E NELLA COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE

22. Nel merito, le decisioni di adeguatezza dovrebbero concentrarsi sulla valutazione della legislazione vigente nel paese terzo interessato nel suo complesso, a livello teorico e pratico, alla luce dei criteri di valutazione di cui all'articolo 36 della LED. Il sistema di un paese terzo o di un'organizzazione internazionale deve prevedere i meccanismi e i principi generali fondamentali di cui in appresso in termini di disposizioni procedurali e di applicazione della legislazione in materia di protezione dei dati.

23. L'articolo 36, paragrafo 2, della LED stabilisce gli elementi che la Commissione europea deve prendere in considerazione nel valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale.

24. In particolare, la Commissione deve prendere in considerazione lo Stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali[16], la legislazione pertinente, l'attuazione di tale legislazione, l'esistenza di diritti effettivi ed azionabili degli interessati e di un mezzo di ricorso effettivo in sede amministrativa e giudiziale per gli interessati i cui dati personali vengono trasferiti, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti e gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale.

---

[13] Cfr. articolo 47, paragrafo 5 e considerando 82 della LED.

[14] Cfr. *Schrems I*, punto 65: "[...] incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione".

[15] Cfr. *Schrems II*, punto 120: "anche in presenza di una decisione di adeguatezza della Commissione, l'autorità nazionale di controllo competente, investita da una persona di un reclamo relativo alla protezione dei suoi diritti e delle sue libertà rispetto ad un trattamento di dati personali che la riguardano, deve poter esaminare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti posti dal RGPD e, se del caso, proporre un ricorso dinanzi ai giudici nazionali affinché questi ultimi procedano, se condividono i dubbi di tale autorità quanto alla validità della decisione di adeguatezza, ad un rinvio pregiudiziale diretto all'esame della suddetta validità".

[16] Nel valutare il quadro giuridico del paese terzo, occorre tenere conto della possibilità che si possa giungere all'imposizione della pena di morte o di qualsiasi forma di trattamento crudele e inumano sulla base dei dati trasferiti dall'UE. In effetti, qualora tale pena o trattamento sia previsto nel diritto del paese terzo, occorre trovare misure di salvaguardia ulteriori nel quadro giuridico del paese terzo atte a garantire che i dati trasferiti dall'UE non vengano utilizzati per richiedere, pronunciare o eseguire una pena di morte o qualsiasi forma di trattamento crudele e inumano (ad esempio un accordo internazionale che impone condizioni sul trasferimento, un impegno da parte del paese terzo a non imporre una pena di morte o qualsiasi forma di trattamento crudele e inumano sulla base di dati trasferiti dall'UE oppure una moratoria in merito alla pena di morte).

25. È chiaro dunque che qualsiasi analisi significativa dell'adeguatezza della protezione deve comprendere due elementi fondamentali: il contenuto delle norme applicabili e i mezzi per garantirne l'effettiva attuazione nella pratica. Spetta alla Commissione europea verificare sistematicamente che le norme in vigore siano efficaci nella pratica.

26. Il "nucleo" dei principi generali in materia di protezione dei dati e delle prescrizioni "procedurali e attuative", la cui osservanza potrebbe essere considerata una condizione minima per l'adeguatezza della protezione, è tratto dalla Carta dei diritti fondamentali dell'Unione europea (la Carta) e dalla LED. Le disposizioni generali sulla protezione dei dati e la vita privata nel paese terzo non sono sufficienti. Nel quadro giuridico del paese terzo o dell'organizzazione internazionale devono figurare anche disposizioni specifiche che assicurino concretamente il diritto alla protezione dei dati nel settore delle attività giudiziarie e di polizia. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un livello di protezione adeguato, sostanzialmente equivalente a quello garantito all'interno dell'Unione. Tali disposizioni devono essere azionabili.

27. Inoltre, per quanto concerne il principio di proporzionalità[17], in relazione alle leggi degli Stati membri, la Corte di giustizia dell'Unione europea ha ritenuto che la questione relativa all'eventuale giustificazione di una limitazione dei diritti alla vita privata e alla protezione dei dati deve essere valutata, da un lato, misurando la **gravità dell'ingerenza** che tale limitazione comporta[18] e, dall'altro, verificando che **l'importanza dell'obiettivo di interesse pubblico** perseguito da tale limitazione sia proporzionato a tale gravità[19].

28. Secondo la giurisprudenza della Corte di giustizia dell'Unione europea, per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura[20]. Deroghe alla protezione dei dati personali devono operare nei limiti dello stretto necessario[21]. Al fine di soddisfare tale prescrizione, oltre a stabilire norme chiare e precise che regolino la portata e l'applicazione della misura in questione, la normativa interessata deve imporre misure di salvaguardia, in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di 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"[22].

29. Il comitato ha adottato raccomandazioni che individuano garanzie essenziali, modellate sulla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo (Corte EDU) nel settore della sorveglianza, che devono essere riscontrate nel diritto del paese terzo quando si valutano le ingerenze di tali misure di sorveglianza del paese terzo in questione rispetto ai diritti degli interessati nel caso in cui i dati siano trasferiti in tale paese ai

[17] Articolo 52, paragrafo 1, della Carta.
[18] La Corte 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 [...]" (cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, ECLI:EU:C:2020:791, punto 187, compresa la giurisprudenza ivi citata).
[19] *La Quadrature du Net e a.*, punto 131.
[20] *Schrems II*, punto 180.
[21] *Schrems II*, punto 176, compresa la giurisprudenza citata.
[22] *Schrems II*, punto 176, compresa la giurisprudenza citata.

sensi del regolamento generale sulla protezione dei dati[23]. Ai fini della valutazione del rispetto delle condizioni di cui all'articolo 36, paragrafo 2, lettera a), della LED, il comitato ritiene che si debbano prendere in considerazione le garanzie stabilite nelle presenti raccomandazioni all'atto di valutare l'adeguatezza di un paese terzo alla luce della LED nel settore della sorveglianza, tenendo presenti ulteriori condizioni specifiche applicabili in questo ambito al settore suddetto.

30. In relazione alla prescrizione di cui all'articolo 36, paragrafo 2, lettera b), il paese terzo dovrebbe assicurare non soltanto un controllo indipendente ed efficace della protezione dei dati, ma prevedere anche meccanismi di cooperazione con le autorità di protezione dei dati degli Stati membri[24].

31. In relazione alla prescrizione di cui all'articolo 36, paragrafo 2, lettera c), al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale ha assunto, si dovrebbero tenere altresì in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, in particolare rispetto alla protezione dei dati personali, nonché l'attuazione di tali obblighi, in particolare l'adesione del paese terzo ad altri accordi internazionali in materia di protezione dei dati, ad esempio la convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale (convenzione 108[25] e la sua versione modernizzata, convenzione 108+). Si può tenere conto anche del rispetto da parte del paese terzo dei principi sanciti in documenti internazionali quali il documento del Consiglio d'Europa *Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime*.

32. Una decisione di adeguatezza dovrebbe garantire che, attraverso il contenuto dei diritti in materia di vita privata e protezione dei dati e in virtù dell'attuazione, della vigilanza e di un'applicazione efficaci di tali diritti, il sistema del paese terzo nel suo complesso garantisca il livello di protezione richiesto, anche per i dati in transito verso tale paese terzo. Come sottolineato dalla Corte di giustizia dell'Unione europea nella sentenza *Schrems II*, il livello elevato di protezione offerto dovrebbe essere garantito altresì durante il trasferimento dei dati verso un paese terzo[26].

33. Infine, nell'adottare una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo, la Commissione europea dovrebbe prendere in considerazione criteri chiari e obiettivi quali specifiche attività di trattamento o l'ambito di applicazione delle pertinenti norme giuridiche e degli strumenti legislativi in vigore nel paese terzo[27].

A. Principi generali e garanzie

a) Nozioni

34. Dovrebbero essere fissate alcune nozioni basilari in materia di protezione dei dati. Tali nozioni non devono necessariamente riprendere la terminologia della LED, ma dovrebbero rispecchiare ed essere coerenti con le nozioni sancite nel diritto europeo in materia di protezione dei dati. A titolo esemplificativo, la LED contiene le seguenti nozioni fondamentali: "dati personali",

[23] Comitato europeo per la protezione dei dati, Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020.
[24] Considerando 67 della LED.
[25] Considerando 68 della LED.
[26] Cfr. punto 93.
[27] Considerando 67 della LED.

"trattamento dei dati personali", "autorità competente", "titolare del trattamento", "responsabile del trattamento", "destinatario", "dati sensibili", "esattezza", "profilazione", "protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", "autorità di controllo" e "pseudonimizzazione".

b) Liceità e correttezza del trattamento dei dati personali (articolo 4 - considerando 26)

35. Ai sensi dell'articolo 8, paragrafo 2, della Carta, i dati personali dovrebbero tra l'altro essere trattati "per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge"[28]. Tuttavia, nel contesto delle attività di contrasto, occorre rilevare che l'adempimento dei compiti di prevenzione, indagine, accertamento e perseguimento di reati, affidato istituzionalmente dalla legge alle autorità competenti, consente a queste ultime di richiedere od ordinare alle persone fisiche di dare seguito alle richieste formulate. In tal caso il consenso dell'interessato non dovrebbe costituire la base giuridica per il trattamento dei dati personali da parte delle autorità competenti[29].

36. La base giuridica dovrebbe stabilire norme chiare e precise che disciplinano la portata e l'applicazione delle attività di trattamento dei dati pertinenti e imporre misure di salvaguardia minime[30]. Inoltre la Corte di giustizia dell'Unione europea ha ricordato che tale "normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale"[31].

37. Per essere lecito, il trattamento dei dati[32] dovrebbe essere necessario per l'esecuzione di un compito svolto da un'autorità competente ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, comprese le misure di salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica[33]. Tali finalità dovrebbero essere previste dal diritto nazionale.

38. I dati personali devono essere trattati correttamente. Il principio di correttezza del trattamento proprio della protezione dei dati è una nozione distinta dal diritto a un giudice imparziale sancito dall'articolo 47 della Carta e nell'articolo 6 della convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)[34].

c) Il principio della limitazione delle finalità (articolo 4)

[28] Cfr. *Schrems II*, punto 173.

[29] Il considerando 35 della LED afferma inoltre che "[q]ualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali".

[30] Cfr. *Schrems II*, punti 175 e 180 e parere 1/15, punto 139 e la giurisprudenza citata.

[31] Cfr. causa C-623/17, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e a.*, 6 ottobre 2020, ECLI:EU:C:2020:790, punto 68 - Dovrebbe inoltre essere chiaro che nella versione francese della sentenza, la Corte utilizza la parola "*réglementation*" che è più ampia rispetto ai soli atti del Parlamento.

[32] Il trattamento interamente o parzialmente automatizzato di dati personali e il trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

[33] Le autorità competenti sono un'autorità pubblica competente per tali finalità o qualsiasi altro organismo o entità incaricato/a dalla legge ad esercitare poteri pubblici a tali fini.

[34] Considerando 26 della LED.

39. Le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta[35].
40. I dati dovrebbero essere trattati per una finalità determinata, esplicita e legittima a scopi di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[36], incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica nel paese terzo, e successivamente utilizzati per uno qualsiasi di tali scopi nella misura in cui ciò non sia incompatibile con la finalità originale del trattamento (ad esempio per procedimenti paralleli di natura attuativa o a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici) e sia soggetto a garanzie adeguate per i diritti e le libertà degli interessati. Se i dati personali sono trattati dallo stesso o da un altro titolare del trattamento (autorità competente[37]) per una finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali diversa da quella per la quale sono stati raccolti, tale trattamento dovrebbe essere consentito purché sia autorizzato conformemente alle disposizioni giuridiche applicabili e sia necessario e proporzionato a tale diversa finalità[38]. Dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti degli Stati membri pertinenti in merito a tale ulteriore trattamento dei dati[39]. Inoltre, in ogni caso, il livello di protezione delle persone fisiche previsto nell'Unione dalla LED non dovrebbe essere compromesso, anche nei casi di trasferimenti dei dati personali dal paese terzo verso titolari del trattamento o responsabili del trattamento nello stesso paese terzo[40].

d) Condizioni specifiche per l'ulteriore trattamento per finalità diverse (articolo 9)

41. Per quanto riguarda l'ulteriore trattamento o la divulgazione di dati trasferiti dall'UE per finalità diverse da quelle connesse all'attuazione della normativa pertinente, quali quelle relative alla sicurezza nazionale, la legge dovrebbe altresì prevedere che esse siano necessarie e proporzionate. Dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti degli Stati membri pertinenti in merito a tale ulteriore trattamento dei dati[41]. Anche in questo caso, una volta ulteriormente trattati o divulgati, i dati dovrebbero beneficiare del medesimo livello di protezione di cui godevano nel momento in cui sono stati trattati inizialmente dall'autorità competente ricevente.

e) Il principio della minimizzazione dei dati

42. I dati dovrebbero essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite. In particolare occorre prendere in considerazione l'applicazione dei requisiti relativi alla protezione

[35] Considerando 26 della LED.
[36] Comprese "le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse. Esse comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati" (considerando 12 della LED). Occorre operare una distinzione rispetto alla finalità della sicurezza nazionale o alle attività rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea (TUE) (considerando 14 della LED).
[37] Cfr. nota 33.
[38] Considerando 29 della LED.
[39] Tale meccanismo potrebbe essere ad esempio il ricorso a codici di gestione concordati di comune accordo, un obbligo di notifica nel quadro di uno strumento internazionale, comprese possibili notifiche automatizzate o altre misure di trasparenza analoghe.
[40] Considerando 64 della LED.
[41] Cfr. nota 39.

dei dati fin dalla progettazione e alla protezione per impostazione predefinita, quali l'impiego di campi a inserimento limitato (comunicazioni strutturate) o controlli della qualità automatizzati e non automatizzati.

f) Il principio dell'esattezza dei dati

43. I dati dovrebbero essere esatti e, se necessario, aggiornati. Tuttavia il principio dell'esattezza dei dati dovrebbe essere applicato tenendo conto della natura e della finalità del trattamento in questione. In particolare nei procedimenti giudiziari, le dichiarazioni contenenti dati personali sono basate sulla percezione soggettiva delle persone e non sempre sono verificabili. Il requisito dell'esattezza non dovrebbe pertanto riferirsi all'esattezza di una dichiarazione ma al semplice fatto che è stata rilasciata[42].

44. Si dovrebbe garantire che i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili[43] e che siano previste procedure per rettificare o eliminare dati inesatti. In particolare si dovrebbe tenere conto di eventuali sistemi per la classificazione delle informazioni trattate, in termini di affidabilità delle fonti e livello di verifica dei fatti[44].

g) Il principio della conservazione dei dati

45. I dati dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Occorre istituire meccanismi adeguati per la cancellazione dei dati personali; può trattarsi di un periodo fisso o di un riesame periodico della necessità di conservazione dei dati personali (oppure una combinazione di entrambi: periodo massimo fisso e riesame periodico a determinati intervalli)[45]. I dati personali conservati per periodi più lunghi per fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici dovrebbero essere soggetti a garanzie adeguate (ad esempio in relazione all'accesso)[46].

h) Il principio della sicurezza e della riservatezza (articolo 29, considerando 28 e 71)

46. Qualsiasi soggetto che tratti dati personali dovrebbe assicurare che essi siano trattati in modo da garantirne un'adeguata sicurezza per impedire l'accesso o l'utilizzo non autorizzati dei dati personali e delle attrezzature impiegate per il trattamento. Ciò comprende la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti illeciti e dalla perdita, dalla distruzione o dal danno accidentali, e la disponibilità di misure adeguate per farvi fronte. Nel determinare il livello di sicurezza, occorre tenere conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

47. Occorre garantire canali sicuri di comunicazione tra le autorità degli Stati membri che trasferiscono i dati personali e le autorità riceventi dei paesi terzi.

[42] Considerando 30 della LED.
[43] Considerando 32 della LED.
[44] Ad esempio griglie 4x4 per valutazioni dell'affidabilità e codici di gestione.
[45] Articolo 5 della LED.
[46] Considerando 26 della LED.

i) Il principio della trasparenza (articolo 13; considerando 26, 39, 42, 43, 44, 46)

48. È opportuno che le persone fisiche siano sensibilizzate rispetto ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento dei loro dati personali, nonché alle modalità di esercizio dei diritti di cui godono in relazione al trattamento[47].

49. Dovrebbero essere messe a disposizione delle persone fisiche informazioni su tutti i principali elementi del trattamento dei loro dati personali. Tali informazioni dovrebbero essere facilmente accessibili e comprensibili ed essere scritte in un linguaggio semplice e chiaro. Le informazioni dovrebbero comprendere la finalità del trattamento, l'identità del titolare del trattamento, i diritti di cui gode l'interessato[48] e altre informazioni nella misura in cui ciò sia necessario a garantire la correttezza del trattamento.

50. Possono aversi alcune eccezioni a tale diritto di informazione. Tale limitazione dovrebbe tuttavia essere prevista da una misura legislativa ed essere necessaria e proporzionata per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui, per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata. Tali limitazioni dovrebbero altresì essere prese in considerazione e valutate tenendo conto della possibilità di proporre reclamo a un'autorità di controllo o di proporre ricorso giurisdizionale. In ogni caso, qualsiasi eventuale limitazione dovrebbe essere temporanea e non generalizzata e dovrebbe essere accompagnata da condizioni, garanzie e limitazioni analoghe a quelle previste dalla Carta e dalla CEDU, come interpretate rispettivamente nella giurisprudenza della Corte di giustizia dell'Unione europea e dalla Corte EDU, e rispettare in particolare la sostanza di tali diritti e libertà.

j) Il diritto di accesso, rettifica e cancellazione (articoli 14 e 16)

51. L'interessato dovrebbe avere il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso ai propri dati. Tale diritto dovrebbe comprendere quanto meno determinate informazioni in merito al trattamento, quali le finalità e la base giuridica per il trattamento, il diritto di proporre reclamo presso l'autorità di controllo o le categorie di dati personali in questione[49]. Ciò è particolarmente importante nel caso in cui la trasparenza sia conseguita mediante una notifica di carattere generale (ad esempio informazioni sul sito web dell'autorità).

52. L'interessato dovrebbe avere il diritto di ottenere la rettifica dei propri dati per motivi specifici, ad esempio qualora risultino essere inesatti o incompleti. L'interessato dovrebbe inoltre avere il diritto di ottenere la cancellazione dei propri dati quando, ad esempio, il loro trattamento non è più necessario o è illecito.

53. L'esercizio di tali diritti non dovrebbe essere eccessivamente oneroso per l'interessato.

[47] Considerando 26 della LED.
[48] Tanto i diritti sostanziali (diritto di accesso, di rettifica, ecc.) quanto il diritto di ricorso.
[49] Articolo 14 della LED.

k) Limitazioni dei diritti degli interessati

54. Potrebbero sussistere limitazioni a tali diritti per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui, per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata. Tali limitazioni dovrebbero altresì essere prese in considerazione e valutate tenendo conto della possibilità di proporre reclamo a un'autorità di controllo o di proporre ricorso giurisdizionale.

l) Limitazione relativa ai trasferimenti successivi (articolo 35, considerando 64 e 65)

55. I trasferimenti successivi di dati personali da parte del destinatario iniziale verso un altro paese terzo o un'altra organizzazione internazionale non devono compromettere il livello di protezione, previsto nell'Unione, delle persone fisiche i cui dati vengono trasferiti. Di conseguenza tali trasferimenti successivi di dati dovrebbero essere consentiti soltanto laddove sia garantita la continuità del livello di protezione offerto dal diritto dell'Unione[50]. In particolare il destinatario successivo (ossia il destinatario del trasferimento successivo) dovrebbe essere un'autorità competente per fini di contrasto[51] e tali trasferimenti successivi possono avvenire soltanto per finalità limitate e determinate e purché vi sia una base giuridica per tale trattamento.

56. Dovrebbe essere presa in considerazione anche l'esistenza di un meccanismo che consenta alle autorità competenti dello Stato membro interessato di essere informate e di autorizzare un tale trasferimento successivo dei dati. Il destinatario iniziale dei dati trasferiti dall'UE dovrebbe essere chiamato a, e in grado di, dimostrare che l'autorità competente dello Stato membro ha autorizzato il trasferimento successivo[52] e che sono previste garanzie adeguate per i trasferimenti successivi in assenza di una decisione di adeguatezza relativa al paese terzo verso il quale i dati verrebbero ulteriormente trasferiti[53].

m) Principio di responsabilizzazione (articolo 4, paragrafo 4)

57. Il titolare del trattamento dovrebbe essere competente per e in grado di dimostrare il rispetto dei principi di protezione dei dati di cui all'articolo 4 della LED.

[50] Cfr. anche parere 1/15.
[51] Cfr. nota 33.
[52] In tale contesto è opportuno prendere in considerazione l'esistenza di un obbligo o un impegno ad attuare codici di gestione pertinenti definiti dalle autorità dello Stato membro che effettua il trasferimento.
[53] I requisiti di cui sopra non pregiudicano le condizioni specifiche per i trasferimenti successivi verso un paese adeguato stabilite nel quadro della LED (articolo 35, paragrafo 1, lettere c) ed e)).

B. Esempi di principi supplementari da applicare a tipi specifici di trattamento

a) Categorie particolari di dati (articolo 10 e considerando 37)

58. Nel caso in cui siano interessate "categorie particolari di dati"[54] dovrebbero esistere garanzie specifiche destinate a far fronte ai rischi specifici in questione[55]. Tali categorie dovrebbero rispecchiare quelle previste all'articolo 10 della LED. Pertanto, il trattamento di categorie particolari di dati dovrebbe essere soggetto a garanzie specifiche ed essere consentito soltanto se strettamente necessario a determinate condizioni, ad esempio per tutelare gli interessi vitali di una persona.

b) Processo decisionale automatizzato e profilazione (articolo 11 e considerando 38)

59. Le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione, che producono effetti giuridici negativi che riguardano l'interessato o incidono significativamente sulla sua persona dovrebbero aver luogo soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo[56].

60. Nel contesto dell'Unione europea, tali condizioni comprendono ad esempio la fornitura di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano presso il titolare del trattamento, in particolare il diritto di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione.

61. Il diritto del paese terzo dovrebbe, in ogni caso, prevedere le garanzie necessarie per i diritti e le libertà dell'interessato. A tale riguardo dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti dello Stato membro pertinente in merito a qualsiasi ulteriore trattamento, come l'uso dei dati trasferiti per la profilazione su larga scala.

c) Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (articolo 20)

62. Nel valutare l'adeguatezza, l'attenzione dovrebbe essere rivolta all'esistenza di un obbligo in capo ai titolari del trattamento di adottare politiche interne e attuare misure che aderiscono ai principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, al fine di adottare misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie.

[54] Tali categorie particolari sono anche qualificate dati "sensibili" al considerando 37 della LED.
[55] Tali garanzie aggiuntive potrebbero essere ad esempio misure specifiche di sicurezza, diritti di accesso limitato per il personale, limitazioni relative all'ulteriore trattamento, processo decisionale automatizzato, condivisione successiva o trasferimenti successivi.
[56] Parere 1/15, punto 173.

C. Meccanismi procedurali e attuativi

63. Anche se gli strumenti dei quali il paese terzo si avvale per assicurare un livello di protezione adeguato possono essere diversi da quelli utilizzati all'interno dell'Unione europea[57], un sistema coerente con quello europeo deve essere caratterizzato dalla presenza degli elementi di cui in appresso.

a) Autorità di controllo indipendente competente (articolo 36, paragrafo 2, lettera b), articolo 36, paragrafo 3 e considerando 67)

64. Dovrebbero essere presenti una o più autorità di controllo indipendenti, aventi il compito di garantire e far rispettare le disposizioni in materia di protezione dei dati e della vita privata. L'autorità di controllo agisce in piena indipendenza e imparzialità nell'adempimento dei suoi compiti e nell'esercizio dei suoi poteri, senza richiedere né accettare istruzioni. In tale contesto, l'autorità di controllo dovrebbe disporre di tutti i poteri di esecuzione per garantire in maniera efficace la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo. Dovrebbero inoltre essere presi in considerazione il personale e il bilancio dell'autorità di controllo. L'autorità di controllo dovrebbe essere in grado, infine, di condurre indagini di propria iniziativa. Dovrebbe inoltre essere incaricata di assistere e consigliare gli interessati nell'esercizio dei loro diritti (cfr. anche la seguente lettera c)). Le decisioni di adeguatezza dovrebbero individuare, se del caso, la o le autorità di controllo e i meccanismi di cooperazione con le autorità di controllo degli Stati membri finalizzati ad assicurare il rispetto delle norme in materia di protezione dei dati.

b) Attuazione efficace delle norme in materia di protezione dei dati

65. Il paese terzo dovrebbe garantire che i titolari del trattamento e chi tratta i dati personali per loro conto abbiano un buon livello di consapevolezza dei propri obblighi, compiti e responsabilità, e che gli interessati siano consapevoli dei propri diritti e dei mezzi a disposizione per esercitarli. L'esistenza di sanzioni effettive e dissuasive può svolgere un ruolo importante nel garantire il rispetto delle norme, così come la presenza di sistemi di verifica diretta da parte di autorità, ispettori o incaricati della protezione dei dati indipendenti.

66. Il sistema di protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento o i soggetti che trattano i dati personali per loro conto a rispettarne le disposizioni e a dimostrare tale conformità, in particolare all'autorità di controllo competente. Tali misure dovrebbero comprendere la conservazione di documentazione o registrazioni delle attività di trattamento dei dati per un periodo di tempo adeguato. Possono comprendere anche, ad esempio, valutazioni d'impatto sulla protezione dei dati, la designazione di un responsabile della protezione dei dati o la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita.

c) il sistema di protezione dei dati deve facilitare l'esercizio dei diritti dell'interessato (articoli 12, 17 e 46 della LED)

67. Il sistema di protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento a facilitare l'esercizio dei diritti degli interessati di cui alla precedente sezione A, lettera j) e prevedere che l'autorità di controllo, su richiesta, informi qualsiasi interessato in merito all'esercizio dei suoi diritti[58].

[57] *Schrems I*, punto 74.
[58] L'esercizio dei diritti degli interessati potrebbe essere diretto o indiretto.

d) Il sistema di protezione dei dati deve prevedere meccanismi di ricorso adeguati

68. Sebbene attualmente non esista giurisprudenza relativa all'adeguatezza dell'ordinamento giuridico di un paese terzo ai sensi della LED, la Corte di giustizia dell'Unione europea ha interpretato il diritto fondamentale a una tutela giurisdizionale effettiva sancito dall'articolo 47 della Carta. L'articolo 47, primo comma, della Carta stabilisce che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice[59], nel rispetto delle condizioni previste da tale articolo.

69. Secondo una giurisprudenza costante della Corte di giustizia dell'Unione europea, l'esistenza stessa di un controllo giurisdizionale effettivo volto a garantire il rispetto delle disposizioni del diritto dell'Unione è inerente all'esistenza dello Stato di diritto. Di conseguenza una legislazione che non preveda alcuna possibilità per una persona fisica di disporre di mezzi di ricorso per avere accesso ai dati personali che la riguardano, o di ottenere la rettifica o la cancellazione di tali dati, non rispetta l'essenza del diritto fondamentale a una tutela giurisdizionale effettiva, come sancito all'articolo 47 della Carta[60].

70. L'interessato dovrebbe essere in grado di avvalersi di mezzi di ricorso per far valere i propri diritti con rapidità ed efficacia, e senza costi proibitivi, nonché per ottenere l'osservanza delle norme.

71. A tal fine devono essere disponibili meccanismi di controllo che consentano un'indagine indipendente in caso di reclami e che permettano di individuare e sanzionare nella pratica eventuali violazioni del diritto alla protezione dei dati e al rispetto della vita privata.

72. In caso di inosservanza delle norme, all'interessato i cui dati sono stati trasferiti verso il paese terzo dovrebbe inoltre essere riconosciuto un mezzo di ricorso effettivo in sede amministrativa e giudiziale nel paese terzo, anche ai fini del risarcimento per i danni subiti a causa di un trattamento illecito dei dati personali che lo riguardano. Si tratta di un elemento fondamentale che deve prevedere un sistema di conciliazione indipendente o di arbitrato che permetta l'eventuale pagamento di indennizzi o l'imposizione di sanzioni.

[59] La Corte di giustizia dell'Unione europea ritiene che una tutela giurisdizionale effettiva possa essere garantita non soltanto da un organo giurisdizionale, ma anche da un organo che offre garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta (cfr. *Schrems II*, punto 197). Ciò potrebbe interessare in particolare le organizzazioni internazionali.
[60] *Schrems II*, punti 187 e 194, compresa la giurisprudenza citata.