

Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*

adottate il 23 luglio 2020

Il presente documento intende offrire una risposta ad alcune delle domande più frequenti ricevute dalle autorità di controllo e sarà elaborato e integrato insieme a un'ulteriore analisi man mano che il comitato europeo per la protezione dei dati (EDPB) proseguirà nell'esame e nella valutazione della sentenza della Corte di giustizia dell'Unione europea (la "Corte").

La sentenza C-311/18 è consultabile [qui](#), mentre il comunicato stampa della Corte è disponibile [qui](#)

1) Che cosa ha stabilito la Corte nella sentenza?

- ➔ Nella sentenza la Corte ha esaminato la validità della decisione 2010/87/UE della Commissione europea, relativa alle clausole contrattuali tipo, e ha ritenuto la decisione valida. La validità di tale decisione non è infatti rimessa in discussione dal solo fatto che le clausole tipo di protezione dei dati di cui alla suddetta decisione, avendo natura contrattuale, non vincolano le autorità del paese terzo verso i quali i dati potrebbero essere trasferiti.

Per contro, la Corte ha precisato che tale validità dipende dall'esistenza all'interno della decisione 2010/87/UE di meccanismi efficaci che consentano, in pratica, di garantire il rispetto di un livello di protezione essenzialmente equivalente a quello garantito all'interno dell'UE dal RGPD e che prevedano la sospensione o il divieto dei trasferimenti di dati personali, fondati su tali clausole, in caso di violazione delle clausole stesse o in caso risulti impossibile garantirne l'osservanza.

A tale riguardo la Corte sottolinea, in particolare, che la decisione 2010/87/UE stabilisce l'obbligo per l'esportatore dei dati e il destinatario di tali dati (l'"importatore dei dati") di verificare, preliminarmente al trasferimento, e tenendo conto delle circostanze di quest'ultimo, se tale livello di protezione sia rispettato nel paese terzo considerato. Inoltre, la Corte rileva che la decisione 2010/87/UE impone all'importatore dei dati di informare l'esportatore di qualsiasi impossibilità di conformarsi alle clausole tipo di protezione nonché, ove necessario, a eventuali

misure supplementari a quelle offerte dalle clausole, con l'onere, in tal caso, per l'esportatore dei dati di sospendere il trasferimento di dati e/o di risolvere il contratto concluso con l'importatore.

- ➔ La Corte ha altresì esaminato la validità della decisione relativa allo «scudo per la privacy» (Decisione 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy), poiché i trasferimenti in questione nel contesto della controversia nazionale sfociata nella domanda di pronuncia pregiudiziale hanno avuto luogo tra l'UE e gli Stati Uniti («USA»).

Secondo la Corte, i requisiti della normativa interna degli Stati Uniti, e in particolare taluni programmi che consentono l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea verso gli Stati Uniti, comportano limitazioni della protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli richiesti nel diritto dell'Unione ⁽¹⁾; inoltre, tale normativa non conferisce agli interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.

Alla luce di tale grado di ingerenza nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy.

2) La sentenza della Corte ha implicazioni su strumenti di trasferimento diversi dallo scudo per la privacy?

- ➔ In generale, per i paesi terzi, la soglia fissata dalla Corte si applica anche a tutte le garanzie adeguate di cui all'articolo 46 del RGPD, utilizzate per il trasferimento dei dati dal SEE a qualsiasi paese terzo. La normativa statunitense richiamata dalla Corte [l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) e l'Executive Order (EO) 12333] si applica a qualsiasi trasferimento verso gli Stati Uniti eseguito con mezzi elettronici che rientri nell'ambito di applicazione della suddetta normativa, a prescindere dallo strumento utilizzato per il trasferimento ⁽²⁾.

3) E' previsto un periodo di tolleranza durante il quale si può continuare a trasferire i dati verso gli Stati Uniti senza valutare la base giuridica per il trasferimento?

- ➔ No, la Corte ha invalidato la decisione sullo scudo per la privacy senza preservarne gli effetti, poiché la normativa statunitense oggetto della valutazione della Corte non fornisce un livello di protezione sostanzialmente equivalente a quello dell'Unione. Di questa valutazione si deve tenere conto con riguardo a qualsiasi trasferimento verso gli Stati Uniti.

4) Trasferivo i dati a un importatore di dati statunitense aderente allo scudo per la privacy, che cosa devo fare ora?

⁽¹⁾ La Corte rileva che taluni programmi di sorveglianza che consentono l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati personali trasferiti dall'Unione europea verso gli Stati Uniti non prevedono limitazioni al potere conferito alle autorità statunitensi, e neppure garanzie per gli stranieri potenzialmente oggetto di tale sorveglianza.

⁽²⁾ L'articolo 702 del FISA si applica a tutti i «fornitori di servizi di comunicazione elettronica» [si veda la definizione al 50 USC § 1881(b)(4)], mentre l'EO 12 333 disciplina la sorveglianza elettronica, definita come «l'acquisizione di una comunicazione non pubblica con mezzi elettronici senza il consenso di una persona che è parte di una comunicazione elettronica o, in caso di comunicazione non elettronica, senza il consenso di una persona visibilmente presente nel luogo della comunicazione, ad esclusione dell'uso di apparecchiature radiogoniometriche al solo scopo di determinare la posizione di un trasmettitore» [3.4; b)].

- ➔ I trasferimenti sulla base di questo quadro giuridico sono illegali. Qualora si desideri continuare a trasferire i dati verso gli Stati Uniti, è necessario verificare se ciò sia possibile alle condizioni stabilite in appresso.

5) Sto utilizzando clausole contrattuali tipo con un importatore di dati negli Stati Uniti, che cosa devo fare?

- ➔ La Corte ha rilevato che la legislazione statunitense (ossia l'articolo 702 del FISA e l'EO 12333) non garantisce un livello di protezione sostanzialmente equivalente.

La possibilità di trasferire dati personali sulla base delle clausole contrattuali tipo dipenderà dall'esito della valutazione condotta, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili. Le misure supplementari unitamente alle clausole contrattuali tipo, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito.

Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende tuttavia proseguire col trasferimento dei dati malgrado la suddetta conclusione, è obbligatorio informarne l'autorità di controllo competente ⁽³⁾.

6) Sto utilizzando norme d'impresa vincolanti (BCR) con un soggetto stabilito negli Stati Uniti, che cosa devo fare?

- ➔ In considerazione della sentenza della Corte, che ha invalidato lo scudo per la privacy a causa del grado di ingerenza creato dalla normativa statunitense nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, e alla luce della circostanza per cui lo scudo per la privacy è stato concepito anche per fornire garanzie ai dati trasferiti con altri strumenti, quali le norme vincolanti d'impresa, la valutazione della Corte si applica anche nel contesto delle norme vincolanti d'impresa, poiché la normativa statunitense prevarrà anche su quest'ultimo strumento.

La possibilità di trasferire i dati personali sulla base delle norme vincolanti d'impresa dipenderà dal risultato della valutazione effettuata, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili. Tali misure supplementari unitamente alle norme vincolanti d'impresa, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito.

Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali. Se si intende ciononostante proseguire col trasferimento dei dati, è obbligatorio informare l'autorità di controllo competente ⁽⁴⁾.

⁽³⁾ Si vedano in particolare il considerando 145 della sentenza della Corte e la clausola 4, lettera g), della decisione della Commissione 2010/87/UE, nonché la clausola 5, lettera a) della decisione della Commissione 2001/497/CE e l'insieme II, lettera c), dell'allegato della decisione della Commissione 2004/915/CE.

⁽⁴⁾ Si vedano in particolare il considerando 145 della sentenza della Corte e la clausola 4, lettera g), della decisione della Commissione 2010/87/UE. Si vedano anche la sezione 6.3, WP256 rev.01 (Gruppo di lavoro «articolo 29», documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, adottato dall'EDPB, <http://ec.europa.eu/newsroom/article29/item->

7) Che cosa è previsto per gli altri strumenti di trasferimento ai sensi dell'articolo 46 del RGPD?

- L'EDPB valuterà le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle clausole contrattuali tipo e dalle norme vincolanti d'impresa. La sentenza chiarisce che lo standard per l'adeguatezza delle garanzie ai sensi dell'articolo 46 del RGPD è costituito dalla «equivalenza sostanziale».

Come evidenziato dalla Corte, l'articolo 46 figura nel capo V del RGPD e, di conseguenza, deve essere letto alla luce dell'articolo 44 del regolamento stesso, in base al quale *«tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato»*.

8) Posso utilizzare le deroghe previste dall'articolo 49 del RGPD per il trasferimento di dati verso gli Stati Uniti?

- Il trasferimento dei dati dal SEE agli Stati Uniti sulla base delle deroghe previste dall'articolo 49 del RGPD è ancora possibile, purché siano soddisfatte le condizioni stabilite in tale articolo. L'EDPB rimanda alle proprie linee guida sul punto ⁽⁵⁾.

Va ricordato, in particolare, che quando i trasferimenti si basano sul consenso dell'interessato, tale consenso deve essere:

-) esplicito,
-) specifico con riguardo al trasferimento o al complesso di trasferimenti di dati in questione (ciò significa che l'esportatore deve assicurarsi di ricevere un consenso specifico prima di mettere in atto il trasferimento, anche se ciò avviene dopo la raccolta dei dati) e
-) informato, soprattutto rispetto ai possibili rischi del trasferimento (ciò significa che l'interessato deve essere informato anche dei rischi specifici derivanti dal trasferimento verso un paese terzo che non offre una protezione adeguata, e dell'assenza di adeguate garanzie per la protezione dei dati).

Per quanto concerne i trasferimenti necessari all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento, va ricordato che i dati personali possono essere trasferiti soltanto su base occasionale. Il carattere «occasionale» o «non occasionale» dei trasferimenti deve essere stabilito caso per caso. Questa deroga può comunque essere applicata soltanto se il trasferimento è oggettivamente necessario per l'esecuzione del contratto.

In relazione ai trasferimenti necessari per importanti motivi di interesse pubblico [che devono essere riconosciuti dal diritto dell'Unione o dal diritto degli Stati membri ⁽⁶⁾], l'EDPB ricorda che il requisito essenziale per l'applicabilità di questa deroga risiede nella constatazione della sussistenza di un motivo di interesse pubblico rilevante e non nella natura del soggetto coinvolto nel trasferimento, e che, sebbene la deroga non si limiti ai trasferimenti di dati «occasionalmente», ciò non significa che, in base alla deroga per importanti motivi di interesse pubblico, possano avere luogo trasferimenti di dati sistematici e su larga scala. Occorre semmai rispettare il principio generale secondo cui le deroghe stabilite nell'articolo 49 del RGPD non dovrebbero trasformarsi

[detail.cfm?item_id=614109](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109)) e la sezione 6.3, WP257 rev.01 (Gruppo di lavoro «articolo 29», documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per i responsabili del trattamento, adottato dall'EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

⁽⁵⁾ Si vedano le Linee-guida 2/2018 del comitato europeo per la protezione dei dati sulle deroghe di cui all'articolo 49 del regolamento 2016/679, adottate il 25 maggio 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf, pag. 3.

⁽⁶⁾ Con il termine «Stati membri» si intendono gli «Stati membri del SEE».

di fatto in una regola, essendo necessario limitarne l'applicazione a situazioni specifiche e purché ogni esportatore di dati garantisca che il trasferimento soddisfa un rigoroso test di necessità.

9) Posso continuare a utilizzare le clausole contrattuali tipo o le norme vincolanti d'impresa per il trasferimento dei dati verso un paese terzo diverso dagli Stati Uniti?

- La Corte ha indicato che, di norma, le clausole contrattuali tipo possono ancora essere utilizzate per il trasferimento di dati verso un paese terzo; tuttavia, la soglia fissata dalla Corte per i trasferimenti verso gli Stati Uniti si applica a qualsiasi paese terzo. Lo stesso vale per le norme vincolanti d'impresa.

La Corte ha sottolineato che spetta all'esportatore e all'importatore dei dati verificare il rispetto, nel paese terzo, del livello di protezione richiesto dal diritto dell'Unione, al fine di determinare se le garanzie previste dalle clausole contrattuali tipo o dalle norme vincolanti d'impresa possano essere rispettate nella pratica. In caso contrario, occorre accertare se sia possibile prevedere misure supplementari atte a garantire un livello di protezione sostanzialmente equivalente a quello vigente nel SEE, e se il diritto del paese terzo non consenta ingerenze nei riguardi delle suddette misure supplementari tali da comprometterne di fatto l'efficacia.

È possibile contattare l'importatore dei dati per verificare la legislazione del rispettivo paese e collaborare alla necessaria valutazione. Qualora si stabilisca, da parte dell'esportatore o dell'importatore nel paese terzo, che il livello di protezione previsto per i dati trasferiti ai sensi delle clausole contrattuali tipo o delle norme vincolanti d'impresa non è sostanzialmente equivalente a quello garantito all'interno del SEE, i trasferimenti devono essere immediatamente sospesi. In caso contrario, occorre informarne l'autorità di controllo competente (7).

- Sebbene, come sottolineato dalla Corte, sia responsabilità primaria degli esportatori e degli importatori accertarsi che la legislazione del paese terzo di destinazione consenta all'importatore di rispettare le clausole tipo di protezione dei dati o le norme vincolanti d'impresa, prima di procedere al trasferimento dei dati personali verso tale paese terzo, anche le autorità di controllo avranno da svolgere un ruolo fondamentale nell'attuazione del RGPD e nell'adozione di ulteriori decisioni in merito ai trasferimenti verso paesi terzi.

Come sollecitato dalla Corte, al fine di evitare decisioni divergenti, le autorità di controllo sono chiamate a proseguire la collaborazione in seno all'EDPB per garantire approcci coerenti, in particolare qualora debbano essere vietati determinati trasferimenti verso paesi terzi.

10) Quali misure supplementari posso introdurre se utilizzo clausole contrattuali tipo o norme vincolanti d'impresa per il trasferimento di dati verso paesi terzi?

- Le misure supplementari eventualmente da introdurre, ove necessario, dovrebbero essere stabilite caso per caso, tenendo conto di tutte le circostanze del trasferimento e previa valutazione della legislazione del paese terzo, al fine di verificare se essa assicuri un livello di protezione adeguato.

La Corte ha sottolineato che è responsabilità primaria dell'esportatore e dell'importatore effettuare tale valutazione e fornire le misure supplementari necessarie.

(7) Si veda in particolare il punto 145 della sentenza della Corte. In relazione alle clausole contrattuali tipo, si vedano la clausola 4, lettera g), della decisione della Commissione 2010/87/UE, nonché la clausola 5, lettera a) della decisione della Commissione 2001/497/CE e l'allegato II, lettera c), della decisione della Commissione 2004/915/CE. In relazione alle norme vincolanti d'impresa, si vedano la sezione 6.3 WP256 rev.01 (approvato dall'EDPB) e la sezione 6.3 WP257 rev.01 (approvato dall'EDPB).

L'EDPB sta analizzando la sentenza della Corte per stabilire quali misure supplementari, di natura giuridica, tecnica o organizzativa, potrebbero essere previste in aggiunta alle clausole contrattuali tipo o alle norme vincolanti d'impresa per il trasferimento dei dati verso paesi terzi in cui dette clausole o norme non offrono isolatamente un livello sufficiente di garanzie.

→ L'EDPB intende approfondire l'analisi relativa alla tipologia delle misure supplementari e fornirà ulteriori indicazioni in merito.

11) Mi avvalgo di un responsabile del trattamento per dati di cui io sono il titolare, come posso sapere se tale responsabile trasferisce i dati verso gli Stati Uniti o un altro paese terzo?

→ Il contratto concluso con un responsabile del trattamento a norma dell'articolo 28, paragrafo 3, del RGPD, deve stabilire se i trasferimenti siano autorizzati o meno (si tenga presente che anche fornire accesso ai dati da un paese terzo, ad esempio per finalità amministrative, costituisce un trasferimento).

→ Occorre un'autorizzazione anche per consentire a responsabili del trattamento di affidare a sub-responsabili il trasferimento dei dati verso paesi terzi. È necessario prestare attenzione e usare cautela poiché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio, per scopi di conservazione o manutenzione).

12) Cosa posso fare per continuare ad avvalermi dei servizi del responsabile del trattamento se il contratto firmato in conformità dell'articolo 28.3 del RGPD indica la possibilità di trasferire i dati verso gli Stati Uniti o un altro paese terzo?

→ Qualora sia previsto che i dati siano trasferiti verso gli Stati Uniti e non siano ipotizzabili misure supplementari atte a garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello garantito nel SEE assicurato dagli strumenti di trasferimento, né si applichino le deroghe di cui all'articolo 49 del RGPD, l'unica soluzione è negoziare un emendamento o una clausola supplementare al contratto al fine di vietare i trasferimenti verso gli Stati Uniti. Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in un luogo diverso dagli Stati Uniti.

→ Nel caso in cui i dati possano essere trasferiti verso un altro paese terzo, è necessario verificare anche la legislazione di tale paese terzo per accertarne la conformità ai requisiti della Corte e al livello di protezione dei dati personali atteso. Qualora sia impossibile individuare un'adeguata base giuridica per il trasferimento verso un paese terzo, non si dovrebbe procedere ad alcun trasferimento di dati personali al di fuori del territorio del SEE e tutte le attività di trattamento dovrebbero avere luogo all'interno del SEE.

Per il comitato europeo per la protezione dei dati

La presidente

Andrea Jelinek