[Traduzione a cura dell'Ufficio del Garante]

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI - EDPB

Domande frequenti sulla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 — *Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems*

Adottate il 23 luglio 2020

Il presente documento mira a fornire risposte ad alcune domande frequenti ricevute dalle autorità di controllo e sarà sviluppato e integrato con ulteriori analisi man mano che il comitato europeo per la protezione dei dati prosegue nell'esame e nella valutazione della sentenza della Corte di giustizia dell'Unione europea ("la Corte").
La sentenza C-311/18 è disponibile qui e il comunicato stampa della Corte è disponibile qui.

1) Che cosa ha stabilito la Corte nella sua sentenza?

- → Nella sua sentenza, la Corte ha esaminato la validità della decisione n. 2010/87/CE della Commissione europea sulle clausole contrattuali tipo ("SCC") e ne ha ritenuto la validità. Infatti, la validità di tale decisione non è in dubbio per il semplice motivo che le clausole tipo di protezione dei dati di cui alla suddetta decisione non sono vincolanti per le autorità del paese terzo verso il quale i dati possono essere trasferiti, avendo esse natura contrattuale.

Tuttavia, tale validità, ha aggiunto la Corte, dipende dall'esistenza all'interno della decisione 2010/87/CE di meccanismi efficaci che consentano, in pratica, di garantire il rispetto di un livello di protezione sostanzialmente equivalente a quello garantito dal RGPD all'interno dell'Unione europea, e che prevedano la sospensione o il divieto dei trasferimenti di dati personali ai sensi di tali clausole in caso di violazione delle clausole stesse o in caso risulti impossibile garantirne l'osservanza.

A tale riguardo, la Corte rileva, in particolare, che la decisione 2010/87/CE impone all'esportatore di dati e al destinatario dei dati ("l'importatore dei dati") l'obbligo di verificare, prima di qualsiasi trasferimento, alla luce delle circostanze del trasferimento stesso, se tale livello di protezione sia rispettato nel paese terzo in questione. Inoltre, la Corte rileva che la decisione 2010/87/CE impone all'importatore di informare l'esportatore di qualsiasi impossibilità di rispettare le clausole tipo di protezione dei dati nonché, ove necessario, eventuali misure supplementari a quelle offerte da tali clausole, nel qual caso l'esportatore di dati è tenuto a sospendere, a sua volta, il trasferimento dei dati e/o a risolvere il contratto con l'importatore.

- ➔ La Corte ha inoltre esaminato la validità della decisione relativa allo scudo per la privacy (*Privacy Shield*) (Decisione 2016/1250 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy), poiché i trasferimenti in esame nell'ambito della controversia nazionale che ha portato alla domanda di pronuncia pregiudiziale si sono svolti tra l'UE e gli Stati Uniti ("USA").

La Corte ha ritenuto che i requisiti del diritto interno degli Stati Uniti, e in particolare determinati programmi che consentono alle autorità pubbliche degli Stati Uniti di accedere ai dati personali trasferiti dall'UE agli Stati Uniti ai fini della sicurezza nazionale, comportino limitazioni alla protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli previsti dal diritto dell'UE[1] e che tale legislazione non accordi ai soggetti 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 il suddetto paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy (Privacy Shield).

2) La sentenza della Corte ha implicazioni sugli 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 ai sensi dell'articolo 46 del RGPD delle quali ci si avvalga per trasferire dati dal SEE a qualsiasi paese terzo. La normativa statunitense cui fa riferimento la Corte (vale a dire l'articolo 702 della FISA e l'Executive Order (EO) 12333) si applica a qualsiasi trasferimento verso gli Stati Uniti per via elettronica che rientra nell'ambito di applicazione della suddetta normativa, indipendentemente dallo strumento utilizzato per il trasferimento[2].

3) È previsto un periodo di grazia durante il quale continuare a trasferire i dati verso gli USA senza valutare la base giuridica per il trasferimento?

→ No, la Corte ha annullato la decisione relativa allo scudo per la privacy senza preservarne gli effetti, in quanto la normativa americana che è oggetto di valutazione da parte della Corte non fornisce un livello di protezione sostanzialmente equivalente a quello dell'UE. Tale valutazione deve essere tenuta presente con riguardo a ogni trasferimento verso gli Stati Uniti.

4) Trasferisco dati a un importatore di dati statunitense aderente allo scudo per la privacy, cosa devo fare adesso?

→ I trasferimenti sulla base di tale quadro giuridico sono illegali. Qualora desideri continuare a trasferire i dati verso gli Stati Uniti, occorre verificare se ciò sia possibile alle condizioni di seguito indicate.

5) Mi avvalgo di SCC con un importatore di dati negli Stati Uniti, cosa devo fare?

[1] La Corte sottolinea che taluni programmi di sorveglianza che consentono alle autorità pubbliche statunitensi di accedere ai dati personali trasferiti dall'UE agli Stati Uniti per motivi di sicurezza nazionale non prevedono limitazioni al potere conferito alle autorità statunitensi né garanzie per soggetti non statunitensi potenzialmente sottoposti a tale sorveglianza.

[2] L'articolo 702 della FISA si applica a ogni "fornitore di servizi di comunicazione elettronica" (cfr. la definizione di cui all'articolo 1881 dell'USC 50, lettera b) (4)), mentre l'Executive Order 12 333 disciplina la sorveglianza elettronica, definita come "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, con l'esclusione dell'impiego di dispositivi radio di direzionamento al solo scopo di stabilire la posizione di un apparato trasmittente" (3.4;b)).

→ La Corte ha rilevato che la normativa degli Stati Uniti (Art. 702 della FISA ed EO 12333) non garantisce un livello di protezione sostanzialmente equivalente.

La possibilità o meno di trasferire dati personali sulla base di SCC dipende dall'esito della valutazione che dovrà compiere, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle SCC, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi sarebbero adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente[3].

6) Utilizzo le norme vincolanti d'impresa ("BCR") con un soggetto stabilito negli Stati Uniti, cosa devo fare?

→ Tenuto conto della sentenza della Corte, che ha annullato lo scudo per la privacy a causa del grado di interferenza creato dalla normativa degli Stati Uniti con i 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 era stato concepito anche al fine di apportare garanzie ai dati trasferiti utilizzando altri strumenti, come le norme vincolanti d'impresa, la valutazione della Corte si applica anche con riguardo alle norme vincolanti d'impresa, in quanto la normativa statunitense prevarrà anche sull'applicazione di quest'ultimo strumento.

La possibilità di trasferire o meno dati personali sulla base delle BCR dipenderà dall'esito della valutazione, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle BCR, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle BCR e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi sarebbero adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente[4].

[3] V., in particolare, il punto 145 della sentenza della Corte e la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione, nonché la clausola 5 (a) della decisione n. 2001/497/CE della Commissione e l'allegato II (c) della decisione n. 2004/915/CE della Commissione.

[4] V., in particolare, il punto 145 della sentenza della Corte e la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione. Cfr. anche sezione 6.3 WP256 rev.01 (Gruppo di lavoro articolo 29, documento di lavoro che stabilisce una tabella con gli elementi e i principi contenuti nelle BCR per titolari del trattamento, approvato dal comitato europeo per la protezione dei dati, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), e sezione 6.3 WP257 rev.01 (Gruppo di lavoro articolo 29, documento di lavoro che stabilisce una tabella con gli elementi e i principi contenuti nelle BCR per responsabili del trattamento, approvato dal comitato europeo per la protezione dei dati, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

7) E che succede rispetto agli altri strumenti di trasferimento previsti dall'articolo 46 del RGPD?

→ Il Comitato europeo per la protezione dei dati valuterà le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle SCC e dalle BCR. La sentenza chiarisce che il parametro per l'adeguatezza delle garanzie di cui all'Art. 46 RGPD è costituito dalla "equivalenza sostanziale".

Come sottolineato dalla Corte, occorre rilevare che 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 di detto capo devono essere applicate al fine di garantire che non sia compromesso il livello di protezione delle persone fisiche garantito da tale regolamento*".

8) Posso utilizzare una delle deroghe di cui all'articolo 49 del regolamento generale sulla protezione dei dati al fine di trasferire i dati negli Stati Uniti?

→ È ancora possibile trasferire dati dal SEE agli Stati Uniti sulla base delle deroghe previste dall'articolo 49 del regolamento generale sulla protezione dei dati, purché siano soddisfatte le condizioni di cui a tale articolo. Il Comitato europeo per la protezione dei dati rinvia alle proprie linee-guida in merito[5].

In particolare, è opportuno ricordare che, quando i trasferimenti sono basati sul consenso dell'interessato, esso dovrebbe essere:

- esplicito,
- specifico con riguardo al particolare trasferimento o insieme di trasferimenti (il che significa che l'esportatore deve assicurarsi di ottenere un consenso specifico prima che il trasferimento sia messo in atto anche se ciò avviene dopo la raccolta dei dati), e
- informato, in particolare sui possibili rischi del trasferimento (il che significa che l'interessato dovrebbe essere informato anche dei rischi specifici derivanti dal trasferimento dei dati verso un paese che non fornisce una protezione adeguata, e dell'assenza di misure di salvaguardia adeguate volte a proteggere i dati).

Per quanto riguarda i trasferimenti necessari all'esecuzione di un contratto tra l'interessato e il titolare del trattamento, occorre tenere presente che i dati personali possono essere trasferiti solo su base occasionale. Dovrebbe essere stabilito caso per caso se i trasferimenti di dati in questione abbiano natura "occasionale" ovvero "non occasionale". In ogni caso, tale deroga può essere invocata solo quando il trasferimento è oggettivamente necessario all'esecuzione del contratto.

In relazione ai trasferimenti necessari per importanti motivi di interesse pubblico (che devono essere riconosciuti nella legislazione dell'UE o degli Stati membri[6]), il Comitato europeo per la protezione dei dati ricorda che il requisito essenziale per l'applicabilità di tale deroga è la constatazione della sussistenza di importanti motivi di interesse pubblico, e non già la natura del soggetto coinvolto nel trasferimento, e che, sebbene tale deroga non sia limitata ai trasferimenti di

[5] Cfr. le linee-guida del comitato europeo per la protezione dei dati 2/2018 sulle deroghe di cui all'articolo 49 del regolamento (CE) n. 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] I riferimenti agli "Stati membri" vanno intesi come riferimenti agli "Stati membri del SEE".

dati aventi natura "occasionale", ciò non significa che i trasferimenti di dati sulla base della deroga relativa alla sussistenza di importanti motivi di interesse pubblico possano configurarsi su larga scala e in modo sistematico. Occorre semmai rispettare il principio generale per cui le deroghe previste all'articolo 49 del regolamento generale sulla protezione dei dati non dovrebbero trasformarsi 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 SCC o le BCR per il trasferimento dei dati verso un paese terzo diverso dagli Stati Uniti?

→ La Corte ha indicato che è ancora possibile utilizzare le SCC per trasferire dati in 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 (BCR).

La Corte ha sottolineato che spetta all'esportatore e all'importatore di dati valutare se il livello di protezione richiesto dal diritto dell'UE sia rispettato nel paese terzo in questione al fine di determinare se le garanzie fornite dalle SCC o dalle BCR possano essere rispettate nella pratica. In caso contrario, occorre valutare se sia possibile prevedere misure supplementari per garantire un livello di protezione sostanzialmente equivalente a quello previsto nel SEE, e se la legislazione del paese terzo non consenta ingerenze nei riguardi delle suddette misure supplementari tali da comprometterne di fatto l'efficacia.

È possibile rivolgersi all'importatore di dati per verificare la legislazione del rispettivo paese ed effettuarne una valutazione congiunta. Qualora l'esportatore o l'importatore dei dati nel paese terzo constati che i dati trasferiti ai sensi delle SCC o delle BCR non godono di un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE, occorre sospendere immediatamente i trasferimenti. In caso contrario, occorre informarne la competente SA[7].

- ➔ Sebbene, come sottolineato dalla Corte, spetti in via primaria agli esportatori e agli importatori di dati valutare direttamente che la legislazione del paese terzo di destinazione consente all'importatore di dati di rispettare le clausole tipo di protezione dei dati o le BCR, prima di trasferire i dati personali a tale paese terzo, anche le autorità di controllo avranno un ruolo fondamentale da svolgere in sede di applicazione del regolamento generale sulla protezione dei dati e al momento di adottare ulteriori decisioni in materia di trasferimenti verso paesi terzi.

Come sollecitato dalla Corte, al fine di evitare decisioni divergenti, le autorità di controllo proseguiranno i lavori in seno al comitato europeo al fine di garantire approcci coerenti, in particolare qualora debbano essere vietati determinati trasferimenti verso paesi terzi.

[7] V., in particolare, il punto 145 della sentenza della Corte. In relazione alle SCC, cfr. la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione, nonché la clausola 5 (a) della decisione n. 2001/497/CE della Commissione e l'allegato II (c) della decisione n. 2004/915/CE della Commissione. Per le norme vincolanti d'impresa, cfr. sezione 6.3 WP256 rev.01 (approvato dal comitato europeo per la protezione dei dati), e sezione 6.3 WP257 rev.01 (approvato dal comitato europeo per la protezione dei dati).

10) Quali misure supplementari posso introdurre in caso di utilizzo di SCC o BCR per il trasferimento dei 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 a seguito della valutazione della legislazione del paese terzo, al fine di verificare se essa garantisca un livello di protezione adeguato.

La Corte ha sottolineato che spetta in primo luogo all'esportatore e all'importatore di dati effettuare tale valutazione e fornire le necessarie misure supplementari.

Al momento il Comitato europeo per la protezione dei dati sta analizzando la sentenza della Corte per stabilire quali misure supplementari potrebbero essere fornite in aggiunta alle SCC o alle BCR, siano esse misure giuridiche, tecniche o organizzative, per trasferire dati verso paesi terzi in cui le SCC o le BCR non potranno assicurare isolatamente un livello sufficiente di garanzie.

→ Il Comitato europeo per la protezione dei dati intende approfondire l'analisi relativa alla tipologia delle misure supplementari e fornire ulteriori orientamenti in merito.

11) Mi avvalgo di un responsabile del trattamento che tratta dati per mio conto, essendo io il titolare del trattamento. Come posso sapere se il mio responsabile del trattamento trasferisce i dati verso gli Stati Uniti o un altro paese terzo?

→ Il contratto stipulato con il responsabile in conformità dell'articolo 28, paragrafo 3, del RGPD deve stabilire se i trasferimenti siano o meno autorizzati (occorre tenere presente che costituisce un trasferimento anche l'accesso ai dati effettuato a partire da un paese terzo, ad esempio a fini amministrativi).

→Occorre un'autorizzazione anche per consentire a un responsabile di affidare a sub-responsabili del trattamento il trasferimento di dati verso paesi terzi. È necessaria particolare attenzione perché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio, a fini di conservazione o manutenzione).

12) Che cosa posso fare per continuare a utilizzare i servizi del mio responsabile del trattamento se il contratto firmato a norma dell'articolo 28, paragrafo 3, RGPD indica che i dati possono essere trasferiti verso gli USA o verso un altro paese terzo?

→ Se è previsto che i dati siano trasferiti verso gli Stati Uniti e non possono essere introdotte misure supplementari per garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello offerto nel SEE assicurato dagli strumenti di trasferimento, né si applicano le deroghe di cui all'articolo 49 del RGPD, l'unica soluzione è negoziare un emendamento o una clausola aggiuntiva al contratto per vietare il trasferimento di dati verso gli USA. Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in paesi diversi dagli USA.

- ➔ Se è previsto che i dati siano trasferiti verso un altro paese terzo, occorre analizzare anche la legislazione di tale paese terzo per verificarne la conformità ai requisiti della Corte e al livello di protezione dei dati personali atteso. Se non è possibile individuare un'idonea base

giuridica per il trasferimento verso un paese terzo, non dovrebbe aver luogo alcun trasferimento di dati personali al di fuori del SEE e tutte le attività di trattamento dovrebbero aver luogo all'interno del SEE.

Per il comitato europeo per la protezione dei dati

La presidente
Andrea Jelinek