DATA PROTECTION TRANSFER ASSESSMENT: IL PUNTO DI VISTA DELL'EDPB.

di GABRIELE BORGHI

Nella recente (e famosa) sentenza C-311/2018 (cd. Schrems II), la Corte di Giustizia dell'Unione Europea (CGUE) ha ricordato, da un lato, che la protezione concessa, ad opera del Regolamento UE n. 2016/679 (GDPR), ai dati personali all'interno dello Spazio Economico Europeo (SEE) deve sussistere e permanere a prescindere da qualsiasi trasferimento a cui tali informazioni sono sottoposte, dato che il livello di protezione, sussistente all'interno del paese extra SEE ("paese terzo") o dell'organizzazione internazionale, deve essere "sostanzialmente equivalente" a quello prescritto dal GDPR; dall'altro lato, la CGUE ha precisato, altresì, che colui che intende trasferire i dati personali ("esportatore") è tenuto a verificare – caso per caso, e, ove possibile, in collaborazione con colui che riceve i dati oggetto di trasferimento ("importatore") – che la legislazione (e la prassi) del paese cd. terzo dell'importatore non interferisca sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento previsti negli artt. 46 e 47 del GDPR (es. SCC; BCR; codici di condotta; meccanismi di certificazione)[1], prescrivendo, in tale ipotesi, la possibilità (o meglio, l'onere) di attuare misure supplementari, idonee a colmare le lacune riscontrate e, dunque, ad elevare il livello (di tutele) imposto dalla normativa euro unitaria, composta, in primis, dalla Carta dei diritti fondamentali dell'UE.

[1] Sul punto, la CGUE ha chiarito che le SCC, adottate dalla Commissione UE, sono intese esclusivamente a fornire garanzie contrattuali che si applicano uniformemente in tutti i paesi terzi: dunque, a causa della loro natura contrattuale, le SCC non possono vincolare le autorità pubbliche dei paesi terzi (o delle organizzazioni internazionali), giacché esse non fanno parte del relativo rapporto contrattuale.

Al fine di supportare (e aiutare) l'esportatore nell'esecuzione di tale gravoso, delicato e complesso compito (di valutazione del paese cd. terzo (o organizzazione internazionale), e di individuazione, ove necessario, delle misure integrative adeguate) nonché al fine di incoraggiare un applicazione coerente del GDPR[2] (e della pronunzia in questione a firma della CGUE), l'EDPB ha adottato, nel rispetto dell'art. 70 paragrafo 1) del GDPR, la **Raccomandazione n. 1/2020** (**da leggersi assieme alla Raccomandazione n. 2/2020 dell'EDPB, alle Linee Guida n. 2/2020, alle Linee Guida n. 2/2018, al Parere n. 254/2018, al Documento di Lavoro n. 1/2016 e al Parere n. 4/2014, tutti a firma del WP Art. 29**), onde fornire a quest'ultimo soggetto una serie di step da seguire, potenziali fonti di informazioni[3] da utilizzare e, infine, una casistica esemplificativa di misure supplementari[4] da attuare.

Orbene, gli step preliminari, consigliati all'esportatore dall'EDPB, sono sei, così riassunti:

i. Conoscere e mappare, tramite il Registro delle attività del trattamento ex art. 30 del GDPR, i trasferimenti dei propri dati personali, ivi inclusa la valutazione circa il rispetto dei principi ex art. 5 del GDPR (in primis, quello di "minimizzazione")[5].

[2] A tal riguardo, preme ricordare che il diritto alla protezione dei dati personali non è un diritto assoluto, ma deve essere considerato in relazione alla sua funzione nella società e deve essere bilanciato con gli altri diritti fondamentali, secondo il principio di proporzionalità: cfr. Considerando n. 4) del GDPR, e sentenza della CGUE n. C-507/17 (Google LLC v. CNIL, paragrafo 60).

[3] L'EDPB ha indicato le seguenti fonti di informazioni: giurisprudenza della CGUE e della CEDU; decisioni di adeguatezza della Commissione UE; risoluzioni e rapporti di organizzazioni intergovernative (es. Consiglio d'Europa).

[4] In merito, l'EDPB ha precisato che: "Il GDPR o la Corte [n.d.r.: CGUE] non definiscono né specificano le "garanzie aggiuntive", le "misure aggiuntive" o le "misure integrative" alle garanzie degli strumenti di trasferimento di cui all'articolo 46, paragrafo 2, del GDPR che titolari e responsabili del trattamento possono adottare per garantire il rispetto del livello di protezione richiesto dal diritto dell'UE in un determinato paese terzo" (traduzione non ufficiale).

[5] Quando si mappano i trasferimenti, è fondamentale non dimenticare di prendere in considerazione anche i trasferimenti successivi (es. se il nominato Responsabile del trattamento, stabilito al di fuori del SEE, trasferisce i dati personali ad un sub-Responsabile del trattamento in un altro paese terzo o nello stesso paese terzo). In proposito, è necessario tenere presente che l'accesso remoto da un paese terzo (es. supporto) e/o l'archiviazione in un cloud situato extra SEE

ii. Verificare lo strumento (giuridico) utilizzato per il trasferimento, tra quelli compresi nel Capo V) del GDPR[6].

iii. Valutare eventuali elementi, presenti all'interno della normativa e/o prassi del paese cd. terzo (o della organizzazione internazionale), idonei a pregiudicare, in concreto[7], l'efficacia delle garanzie apportate dagli strumenti di trasferimento di cui si fa affidamento, nel contesto della specifica operazione di trasferimento[8].

Questa analisi deve basarsi, in primo luogo, sulla normativa pubblicamente disponibile[9] che deve contenere

offerto da un cloud service provider è considerato un trasferimento: in particolare, se si utilizza una infrastruttura cloud internazionale, è opportuno valutare se i dati personali saranno trasferiti in un paese terzo (e quale), a meno che il cloud provider dichiari espressamente, all'interno del contratto, che i dati non saranno trattati in alcun paese terzo.

[6] Nel caso in cui la Commissione UE abbia dichiarato adeguato il paese cd. terzo (o una parte o un settore di esso) o l'organizzazione internazionale grazie a una Decisione di adeguatezza ex art. 45 del GDPR (o della precedente Direttiva n. 95/46/CE) non è necessario compiere ulteriori passi, se non quello di monitorare la validità della relativa decisione di adeguatezza (peraltro, la Commissione UE pubblica l'elenco delle proprie decisioni di adeguatezza: ec.europa.eu/info/law-topic/data-protection/international-dimension-dataprotection/adeguacy-decisions_en).

Oltre agli strumenti ex artt. 46 e 47 del GDPR, il medesimo GDPR contiene, all'art. 49, una "terza via", una deroga di natura eccezionale e, dunque, essa non può divenire la regola nella pratica, ma deve essere limitata a situazioni specifiche (cfr. Linee Guida n. 2/2018 dell'EDPB).

[7] Cfr. art. 44 del GDPR, e paragrafi 126), 137) e 148) della sentenza cd. Schrems II della CGUE.

[8] Tale esame può risultare particolarmente rilevante (e problematico) laddove: (i) la legislazione del paese terzo (o della organizzazione internazionale) che soddisfa formalmente gli standard euro comunitari non è, invero, applicata o rispettata nella pratica; (ii) manca una normativa pertinente nel paese terzo (o nella organizzazione internazionale): in tal caso, non si può automaticamente dedurre che lo strumento di trasferimento scelto possa essere effettivamente applicato: infatti, bisogna verificare se vi sono indicazioni pratiche, in vigore nel paese terzo (o nella organizzazione internazionale), incompatibili con il diritto dell'UE e con gli impegni sanciti dallo strumento di trasferimento prescelto; iii) i dati personali oggetto di trasferimento ovvero l'importatore potrebbero rientrare nell'ambito di applicazione di una normativa che non permette al soggetto interessato di godere di un livello di protezione sostanzialmente equivalente, con particolare focus sui diritti fondamentali e sui principi di necessità e di proporzionalità.

[9] In via generale, l'importatore è tenuto a fornire all'esportatore le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito, e le leggi e le pratiche in vigore applicabili al trasferimento. Nello specifico, l'EDPB ha precisato che le fonti e le informazioni devono essere pertinenti (dunque, non

elementi riguardanti l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo, quali: (i) elementi sul fatto che una o più autorità pubbliche del paese terzo dell'importatore possano cercare di accedere ai dati personali, anche senza la consapevolezza o la conoscenza dell'importatore; (ii) elementi sulla possibilità che una o più autorità pubbliche possano accedere ai dati tramite l'importatore o tramite i fornitori (o canali) di telecomunicazione, alla luce della normativa, delle risorse tecniche/finanziarie/umane a disposizione e, infine, dei precedenti verificatesi[10]; in secondo luogo, è necessario valutare, altresì, anche differenti aspetti dell'ordinamento giuridico del paese terzo, tra cui, senz'altro, gli elementi previsti dall'art. 45 paragrafo 2) del GDPR (es. stato di diritto; rispetto dei diritti umani e delle libertà fondamentali; legislazione generale e settoriale (es. sicurezza pubblica/nazionale; difesa; diritto penale); esistenza ed effettivo funzionamento di una o più autorità di controllo indipendenti)[11].

generali ed astratte), obiettive, affidabili, verificabili e disponibili al pubblico (o quantomeno accessibili).

[10] E' possibile prendere in considerazione l'esperienza pratica documentata dell'importatore, unitamente alle relative e precedenti istanze di accesso ricevute dalle autorità pubbliche, ove legalmente consentito.

[11] Cfr. Parere n. 254/2018 del WP 29: "L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e il controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e rispettate nella pratica. E' pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti in un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati […] E' 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 applicazione […] Ulteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal successivo trasferimento".

Sul punto, l'EDPB ha posto l'accento sul fatto che gli artt. 47 e 52 della Carta dei diritti fondamentali dell'UE devono essere utilizzati come (fondamentale) riferimento, al fine di valutare, in particolare, se l'accesso delle autorità pubbliche sia limitato a quanto necessario e proporzionato in una società democratica, e se, infine, è concesso all'interessato un una tutela giudiziaria effettiva.

In merito, l'EDPB ha ulteriormente precisato che il contesto giuridico (e le relative pratiche applicabili) dipendono dalle specifiche circostanze del trattamento, tra cui: (i) finalità per le quali i dati personali vengono trasferiti e trattati; (ii) tipologia dei soggetti coinvolti nel trattamento; (iii) settore in cui avviene il trasferimento; (iv) categoria dei dati personali trasferiti; (v) se i dati personali sono archiviati nel paese terzo, o se esiste un accesso (remoto) ai dati archiviati all'interno del SEE; (vi) formato dei dati personali oggetto di trasferimento (es. semplice; pseudonimizzato; crittografato); (vii) possibilità che i dati personali possono essere oggetto di successivi trasferimenti dal paese terzo a un altro paese terzo[12] (o da una organizzazione internazionale a un'altra organizzazione internazionale).

A tal supporto, l'EDPB ha provveduto ad elencare, all'interno della (connessa) **Raccomandazione n. 2/2020**, le quattro garanzie essenziali europee[13], fondate sull'art. 52 paragrafo 1) della Carta dei diritti fondamentali

[12] Tale valutazione deve prendere in considerazione tutti gli attori che partecipano al trasferimento, così come individuati nell'esercizio di mappatura dei trasferimenti.

[13] L'EDPB ha sottolineato che tali garanzie essenziali si fondano sulla giurisprudenza della CGUE relativa agli artt. 7, 8, 47 e 52 della Carta dei diritti fondamentali dell'UE, e sulla giurisprudenza della CEDU relativa all'art. 8 della Convenzione europea dei diritti dell'uomo. Tali misure essenziali intendono fornire elementi utili a valutare se le misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo (siano esse agenzie di sicurezza o autorità incaricate ex lege) possano configurare un'ingerenza giustificabile o meno; dall'altro lato, esse devono essere valutate e considerate in modo unitario, stante la loro stretta interconnessione (cfr., in merito, anche Documento di Lavoro n. 1/2016 del WP Art. 29).

dell'UE[14], da rispettare al fine di valutare il livello di ingerenza (che non deve eccedere quanto è necessario e proporzionato all'interno di una società democratica) nei diritti fondamentali al rispetto della vita privata ("privacy") e alla protezione dei dati personali ("data protection") nel contesto delle misure di sorveglianza applicate da una (o più) autorità pubbliche di un paese terzo (o di una organizzazione internazionale)[15] in presenza di un trasferimento di dati personali, e, di conseguenza, ha provveduto ad individuare quali requisiti giuridici devono essere conseguentemente in vigore per valutare se tali ingerenze siano accettabili ai sensi della Carta dei diritti fondamentali dell'UE:

1. Il trattamento deve basarsi su regole chiare, precise, accessibili (ossia, pubbliche) ed i cui diritti riconosciuti possono essere effettivamente azionati dall'interessato e da quest'ultimo opposti alle autorità pubbliche[16].

   Nello specifico, la CEDU ha chiarito che la base giuridica deve comprendere almeno: (i) una definizione delle categorie di soggetti interessati che potrebbero essere soggetti alla sorveglianza da parte dell'autorità pubblica; (ii) un limitazione della durata di tale misura; (iii) la procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati personali ottenuti. Oltre a ciò, è stato osservato che l'ingerenza in parola deve essere prevedibile, nei suoi effetti, sulla persona, al fine di

[14] Art. 52 paragrafo 1) della Carta dei diritti fondamentali dell'UE: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

[15] Cfr., sul punto, anche il Parere n. 4/2014 del WP Art. 29.

[16] Sul punto, la CGUE ha precisato – all'interno della sentenza "Schrems II", paragrafo n. 175) – che qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge, e deve definire essa stessa la portata della limitazione dell'esercizio del diritto in esame.

garantire una protezione adeguata ed efficace contro le ingerenze arbitrarie ed abusive[17].

2. Deve sussistere (e deve essere dimostrata) la necessità[18] e la proporzionalità[19] del trattamento rispetto agli obiettivi legittimi e di interesse generale (riconosciuti dall'UE o comunque volti a proteggere i diritti e le libertà altrui) perseguiti.

3. Dovrebbe esistere un meccanismo di controllo efficace, indipendente (dal potere esecutivo ovvero dalle autorità pubbliche deputate a svolgere la videosorveglianza), imparziale, e coordinato da un giudice o da un altro organo indipendente.

4. Il soggetto interessato deve poter accedere ai mezzi di ricorso efficaci ed effettivi, nel rispetto dell'art. 47 della Carta dei diritti fondamentali dell'UE.

iv. Valutare, individuare ed adottare misure di natura contrattuale, tecnica o organizzativa[20] supplementari (agli

[17] La prevedibilità non può, tuttavia, significare che una persona debba essere in grado di prevedere quando un'autorità potrebbe intercettare le sue comunicazioni, in modo da poter adattare il suo comportamento.

[18] Per quanto riguarda il principio di necessità, la CGUE ha chiarito che le legislazioni "che autorizzano, su base generalizzata, la conservazione dei dati personali di tutte le persone i cui dati sono stati trasferiti dall'UE […] senza che sia fatta alcuna distinzione, limitazione o eccezione alla luce dell'obiettivo perseguito e senza che sia stabilito un criterio oggettivo per determinare i limiti dell'accesso delle autorità pubbliche ai dati e al loro successivo utilizzo, per finalità specifiche, strettamente limitate e atte a giustificare l'ingerenza che l'accesso ai dati e il loro utilizzo comportano" non rispettano i principi sanciti nella Carta dei diritti fondamentali dell'UE.

[19] Per quanto riguarda il principio di proporzionalità, la CGUE ha dichiarato che la giustificabilità di una limitazione dei diritti al rispetto della vita privata e alla protezione dei dati personali deve essere valutata, da un lato, misurando la gravità dell'ingerenza che tale limitazione comporta e, dall'altro lato, verificando che l'importanza dell'obiettivo di interesse generale perseguito attraverso tale limitazione sia proporzionato alla suddetta gravità. Al riguardo, si ricorda che la CGUE ha sottolineato, all'interno della sentenza cd. Schrems II, che la legislazione di un paese terzo che non indica alcuna limitazione al potere da essa conferito di attuare programmi di sorveglianza ai fini dell'intelligence esterna non può assicurare un livello di protezione sostanzialmente equivalente a quello garantito dalla Carta dei diritti fondamentali dell'UE.

[20] L'EDPB ha aggiunto, da un lato, che l'eventuale combinazione di misure differenti può migliorare il livello di protezione, e, dunque, può contribuire al

strumenti di trasferimento ex artt. 46 e 47 del GDPR, e alle misure di sicurezza tecniche ed organizzative ex art. 32 del GDPR) ove necessario[21], e documentare, in modo compiuto e dettagliato, la scelta effettuata, nel rispetto del principio di accountability.

v. Intraprendere qualsiasi ed eventuale ulteriore passaggio formale, ivi inclusa la consultazione dell'Authority[22].

vi. Rivalutare, ad intervalli appropriati, il livello di protezione del paese terzo, anche al fine di monitorare la sussistenza di eventuali ed ulteriori sviluppi idonei ad influenzare la relativa operazione di trasferimento.

Da ultimo, in relazione alle misure supplementari, l'EDPB ha tenuto, innanzitutto, a precisare che le stesse – oltre ad essere soltanto esemplificative, giacché fisiologicamente suscettibili della costante evoluzione tecnologica, legale ed organizzativa – sono da considerarsi efficaci, nella misura in cui, da sole ovvero in combinazione tra di loro, risolvono le specifiche carenze risultanti dalla valutazione del paese terzo, effettuata nel rispetto dei criteri di cui al precedente punto iii).

Come anticipato, esse si suddividono nelle seguenti categorie:

i. Misure tecniche: pseudonimizzazione; crittografia; suddivisione dei dati personali trasferiti a due o più importatori situati in differenti giurisdizioni, in modo che

raggiungimento degli standard (di tutela) dell'UE; per altro verso, la medesima EDPB ha rilevato che le sole misure contrattuali ed organizzative non impediscono, in via generale, l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo.

[21] Infatti, la valutazione di cui al precedente punto v) può rivelare che la legislazione pertinente nel paese terzo sia problematica, giacché i dati oggetto di trasferimento ovvero l'importatore rientrano (o potrebbero rientrare) nell'ambito di tale normativa: nel caso, l'esportatore può: (i) sospendere il trasferimento; (ii) adottare le misure supplementari; (iii) procedere al trasferimento senza l'adozione di misure integrative, se l'esportatore ritiene di non aver alcun motivo per ritenere che ai dati personali oggetto di trasferimento verrà applicata, nella pratica, una normativa "problematica" del paese terzo, tenuto anche conto dell'esperienza di altri attori operanti nell'ambito del medesimo settore e/o riguardanti analoghi dati personali oggetto di trasferimento.

[22] Esempio: misure integrative idonee a contraddire, in modo diretto o indiretto, le SCC, anche mediante la limitazione dei diritti e degli obblighi ivi sanciti.

nessuno di essi sia in grado di identificare le informazioni trasferite[23].

ii. Misure contrattuali (unilaterali, bilaterali o multilaterali)[24]: obbligo di adozione di specifiche misure tecniche; obbligo di allegazione, da parte dell'importatore, delle informazioni circa l'accesso ai dati personali oggetto di trasferimento da parte delle autorità pubbliche; impegno con cui l'importatore certifica all'esportatore che (i) non ha creato intenzionalmente una back door (o programmi simili) utilizzabili per accedere al sistema e/o ai dati personali, (ii) non ha creato o modificato intenzionalmente i suoi processi aziendali, in modo da facilitare l'accesso ai dati personali, e (iii) la legislazione nazionale non richiede all'importatore di creare o di mantenere una back door o di facilitare l'accesso ai dati o che quest'ultimo sia in possesso o debba consegnare la chiave di cifratura; audit dell'esportatore presso la struttura dell'importatore, al fine di verificare se i dati personali sono stati comunicati alle autorità pubbliche e a quali condizioni; obbligo dell'importatore di comunicare tempestivamente all'esportatore la sua incapacità di rispettare gli impegni contrattuali; obbligo, in capo all'esportatore e/o all'importatore, di comunicare, in modo tempestivo, all'interessato la richiesta o l'ordine ricevuto dalla pubblica autorità del paese terzo ovvero l'impossibilità dell'importatore di rispettare gli impegni contrattuali, al fine di consentire al soggetto interessato di ottenere maggiori informazioni o di instaurare un ricorso giurisdizionale.

[23] Sul punto, l'EDPB ha evidenziato che, ad oggi, non sussistono misure tecniche supplementari sufficienti ed idonee ad impedire una potenziale lesione dei diritti fondamentali dell'interessato, nel caso in cui l'esportatore deve trasferire i dati personali mediante trasmissione elettronica, mediante la messa a disposizione di un cloud service provider o mediante la messa a disposizione da remoto da parte di un importatore, e tali informazioni personali non possono essere soggette ad una procedura di pseudonimizzazione o di cifratura.

[24] Stante la specifica natura contrattuale, queste misure spesso devono essere combinate con altre misure tecniche ed organizzative, al fine di fornire il livello di protezione richiesto.

iii. Misure organizzative: politiche interne con chiara assegnazione di responsabilità per il trasferimento dei dati personali; canali di segnalazione per la gestione delle richieste formali o informali di accesso ai dati ad opera delle pubbliche autorità; rendicontazione delle richieste di accesso da parte delle autorità pubbliche, ivi inclusa la risposta fornita.