Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

cep**Studio** – Punti chiave

26 Gennaio 2021

Illegittimità del trasferimento dei dati negli USA

La sentenza della CGUE "Schrems II" e le sue conseguenze

Anja Hoffmann

A seguito della sentenza "Schrems II" della Corte di Giustizia UE, i trasferimenti di dati personali verso gli Stati Uniti possono non essere più basati sull'Accordo denominato "Privacy Shield", perché gli Stati Uniti non offrono una adeguata protezione dei dati. Attualmente, i trasferimenti di dati si basano quindi per lo più su clausole contrattuali standard, il cui utilizzo rimane in linea di principio consentito.

- Le clausole contrattuali tipo e le norme interne aziendali sulla protezione dei dati non possono essere utilizzate come base per il trasferimento di dati verso gli Stati Uniti se i destinatari dei dati sono soggetti alle leggi di sorveglianza degli Stati Uniti ed hanno accesso al contenuto dei dati in chiaro.
- In questi casi, anche misure supplementari di protezione dei dati non possono impedire efficacemente l'accesso da parte delle autorità statunitensi.
- In particolare, vanno considerati illegali i trasferimenti a servizi *Cloud* e i trasferimenti all'interno di gruppi aziendali verso gli USA. L'esportatore di dati - o l'autorità di controllo - deve interrompere il trasferimento dei dati.
- Né la riforma del *Privacy Shield* né le modifiche delle clausole contrattuali tipo proposte dalla Commissione UE nel novembre 2020 possono migliorare questo aspetto, fin quando gli Stati Uniti non limiteranno i loro diritti di sorveglianza a quanto consentito dalla normativa UE e non forniranno ai cittadini dell'UE rimedi efficaci.
- Lo stesso vale per i trasferimenti di dati verso altri Paesi terzi, nella misura in cui le loro leggi di sorveglianza sono in conflitto con la protezione dei dati dell'UE. Ogni possibile conflitto deve essere valutato caso per caso.

Punti chiave

Sulla sentenza "Schrems II" della CGUE

- I trasferimenti di dati personali dall'UE verso gli USA non possono più essere basati sull'accordo "*Privacy Shield*" realizzato dalla Commissione UE. La Corte di Giustizia Europea (CGUE) ha giustamente dichiarato invalida questa misura nella sentenza "Schrems II", in quanto il "*Privacy Shield*" non fornisce una protezione dei dati equivalente a quella dell'UE.
- I trasferimenti di dati verso un Paese terzo sulla base di clausole contrattuali tipo - ovvero clausole modello di protezione dei dati rilasciate dalla Commissione UE e concordate tra l'esportatore e il destinatario dei dati - in linea di principio sono ancora consentiti. Gli esportatori e i destinatari dei dati devono tuttavia verificare che il diritto del Paese terzo e le clausole contrattuali tipo nel loro insieme garantiscano una protezione dei dati sostanzialmente equivalente a quella dell'UE, e che le persone interessate i cui dati sono trasferiti dispongano di diritti esigibili e di mezzi di ricorso efficaci.

Gli effetti della sentenza "Schrems II"

- Il Comitato Europeo per la Protezione dei Dati (EDPB) ha pubblicato due proposte di raccomandazione a seguito della sentenza. Secondo queste ultime, nell'esaminare il livello di protezione nel Paese terzo, devono essere prese in considerazione tutte le circostanze del trasferimento specifico dei dati - comprese le categorie e il formato dei dati trasferiti - ma non la valutazione soggettiva della probabilità di accesso da parte delle autorità.
- Inoltre, secondo le clausole contrattuali tipo, l'esportatore ed il destinatario dei dati devono verificare se la legislazione del Paese terzo consente anche al destinatario di rispettare tali clausole. Particolarmente problematici sono i trasferimenti di dati a destinatari ai quali il diritto dello Stato terzo impone obblighi che contraddicono le clausole contrattuali tipo e compromettono le garanzie che queste offrono.
- Secondo l'EDPB, l'obbligo del destinatario dei dati di comunicare o di fornire l'accesso ai dati alle autorità del Paese terzo non impedisce il rispetto delle clausole contrattuali tipo, se il Paese terzo rispetta le "garanzie essenziali europee" nelle sue attività di controllo.
- Le misure di sorveglianza soddisfano le "salvaguardie europee essenziali" dell'EDPB se si basano su regole chiare per il trattamento dei dati, se gli interventi sono necessari e proporzionati e se nel Paese terzo esistono un controllo indipendente e rimedi giurisdizionali efficaci.
- Se le misure di sorveglianza non sono conformi alle misure di salvaguardia - come nel caso della legislazione statunitense sulla sorveglianza - manca un livello di protezione sostanzialmente equivalente. Le clausole contrattuali tipo da sole non sono sufficienti; l'esportatore di dati deve piuttosto prevedere ulteriori misure complementari per la protezione dei dati.
- Vi è incertezza giuridica in merito alle misure supplementari che l'esportatore di dati deve adottare per colmare le lacune di protezione. A tal fine, le autorità di vigilanza propongono misure tecniche come l'anonimizzazione, la cifratura, lo pseudonimo o la suddivisione dei dati, clausole contrattuali supplementari e misure organizzative.
- Obblighi contrattuali più severi, ad esempio l'informazione sull'accesso ai dati o la contestazione sul piano giuridico, e misure organizzative come le politiche interne, aumentano la protezione, ma non sono sufficienti da sole e devono essere integrate da misure tecniche. Questo perché anche obblighi contrattuali più severi non possono né vincolare le autorità del Paese terzo, né creare rimedi efficaci per i cittadini dell'UE.
- Secondo l'EDPB, le misure tecniche possono impedire in modo efficace un accesso ufficiale sproporzionato solo se anche il destinatario dei dati non è in grado di decodificare, de-pseudonimizzare o ricostruire i dati. Questo può avvenire solo in pochi casi, come ad esempio quando i dati vengono memorizzati nel Paese terzo esclusivamente per scopi di sicurezza (backup).
- Se il destinatario dei dati ha accesso o ha bisogno di accedere ai dati in chiaro per la loro elaborazione, anche delle misure tecniche non proteggono efficacemente dal controllo da parte delle autorità. Se il

destinatario è in possesso della chiave, potrebbe essere obbligato a consegnarla alle autorità. Anche le "*backdoor*" attualmente in discussione rispetto al software di cifratura ostacolerebbero la protezione.

- Se l'esportatore di dati non può garantire una protezione dei dati equivalente a quella dell'UE attraverso misure supplementari, egli - o in secondo luogo l'autorità di controllo - deve interrompere il trasferimento dei dati. Nel caso di trasferimenti verso gli Stati Uniti, tuttavia, non si ravvisano misure che possano effettivamente impedire l'accesso da parte delle autorità sulla base delle leggi di sorveglianza di tali Paesi, nella misura in cui al destinatario dei dati non sia interdetto l'accesso ai dati.
- Anche le clausole contrattuali tipo modificate secondo le proposte della Commissione nel novembre 2020, per i motivi suddetti possono fornire una protezione equivalente dei dati solo unitamente a misure tecniche. Per evitare ulteriori ambiguità, le nuove clausole contrattuali tipo dovrebbero essere maggiormente in linea con le raccomandazioni dell'EDPB.

Conseguenze sul trasferimento dei dati personali negli Stati Uniti

- Tutti i trasferimenti di dati verso gli USA a destinatari che sono soggetti alle leggi di sorveglianza degli Stati Uniti e che hanno accesso al contenuto dei dati in chiaro sono pertanto attualmente illegittimi. Sono interessati dalla sentenza, tra gli altri, i trasferimenti a fornitori di servizi *Cloud* e i trasferimenti all'interno di gruppi aziendali per la fornitura di servizi per il personale.
- Le autorità di controllo della protezione dei dati dell'UE dovrebbero fornire indicazioni interpretative su quali destinatari dei dati rientrino nel campo di applicazione delle norme di sorveglianza statunitensi e quali trasferimenti siano quindi essenziali.
- Fintanto che gli Stati Uniti non limitano le loro leggi di sorveglianza a quanto necessario e non forniscono ai cittadini dell'UE rimedi efficaci, nè delle clausole contrattuali tipo ad hoc, né un nuovo e "migliorato" scudo di protezione della privacy saranno utili a risolvere la problematica.

Conseguenze per altri strumenti di trasferimento e trasferimenti di dati verso altri Paesi terzi

- Le osservazioni della CGUE sulle clausole contrattuali tipo sono applicabili ad altri strumenti di trasferimento, come ad esempio le norme vincolanti d'impresa (BCR). Il loro utilizzo comporta quindi rischi simili per il trasferimento di dati verso gli USA, se i destinatari sono soggetti a norme di sorveglianza.
- Le leggi in materia di sorveglianza in conflitto con le clausole contrattuali tipo possono sussistere anche in altri Paesi terzi. Gli esportatori di dati devono quindi verificare anche il livello di protezione per i trasferimenti di dati verso altri Paesi per i quali non esistono misure di adeguatezza e, se necessario, integrare le clausole contrattuali tipo. I trasferimenti di dati verso il Regno Unito rimangono consentiti, almeno per il momento.
- La Commissione UE deve rivedere in modo critico le misure di adeguatezza esistenti per altri Paesi terzi, per determinare se esse (ancora) soddisfano i requisiti stabiliti dalla Corte di Giustizia UE.

Conclusioni

- La soluzione più sicura dal punto di vista giuridico è quella di astenersi dai trasferimenti di dati verso i Paesi terzi sopra descritti, di archiviare i dati in territorio UE in modo tale che le società statunitensi o le loro filiali non abbiano alcun controllo su di essi e di utilizzare solo fornitori europei appropriati.
- Tra gli elevati requisiti di protezione dei dati in territorio UE e le attuali pratiche di trasferimento sussistono delle differenze. Gli esportatori di dati che non ne impediscono il trasferimento illegittimo rischiano di incorrere in sanzioni pecuniarie elevate. Anche le proposte di raccomandazione dell'EDPB e le clausole contrattuali tipo modificate della Commissione UE promettono, nella migliore delle ipotesi, una soluzione giuridicamente sicura e allo stesso tempo pratica solo per un numero limitato di casi.
- La sentenza "Schrems II" offre l'opportunità di rafforzare servizi di alta qualità e sicurezza (ad esempio i *Cloud*) all'interno dell'UE. Solo una volta che sarà fatto ciò, il passaggio a fornitori di servizi appartenenti all'UE può diventare un'alternativa di lungo periodo. La creazione di Gaia-X quale primo *Cloud* europeo può rappresentare un giusto passo in questa direzione.

Il presente documento rappresenta una breve sintesi dello studio integrale pubblicato dal cep in lingua tedesca, disponibile qui

Centrum für Europäische Politik
FREIBURG | BERLIN

Autrice:
Dr. Anja Hoffmann, LL.M. Eur.
hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Strasse 266 | D-79098 Freiburg
Schiffbauerdamm 40 4315 | D-10117 Berlin
Tel. + 49 761 38 69 30

Centro Politiche Europee
ROMA

Traduzione:
Prof. Andrea De Petris

Centro Politiche Europee ROMA
Via G. Vico, 1 | I-00196 Roma
Tel. + 39 0684388433
cepitalia@cep.eu

Il **Centro Politiche Europee** ROMA e i suoi partner
Centrum für Europäische Politik FREIBURG | BERLIN e **Centre de Politique Européenne** PARIS
compongono il **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA

*Gli istituti della rete **cep** sono specializzati nell'analisi e nella valutazione degli atti promossi dalle istituzioni dell'Unione europea nell'ambito delle politiche di loro competenza e nel quadro d'insieme del processo di integrazione. Il lavoro scientifico, riflesso in particolare nelle proprie pubblicazioni, viene portato avanti indipendentemente da qualsiasi interesse di parte e in favore di un'Europa che rispetti lo stato di diritto e i principi dell'economia sociale di mercato.*