CYBERSECURITY360

22/10/2020 11:39
Sito Web

cybersecurity360.it

Trasferimento dati oltreoceano dopo Schrems II: un libro bianco a supporto degli operatori

LINK: https://www.cybersecurity360.it/legal/privacy-dati-personali/trasferimento-dati-oltreoceano-dopo-schrems-ii-un-libro-bianco-a-supporto-degli...

Trasferimento dati oltreoceano dopo Schrems II: un libro bianco a supporto degli operatori Home Norme e adeguamenti Privacy e Dati personali In seguito alla sentenza "Schrems II" emessa dalla Corte di Giustizia dell'Unione Europea, il Dipartimento di Commercio USA ha pubblicato un Libro Bianco a supporto degli operatori interessati al trasferimento dati oltreoceano. Ecco tutti i dettagli e alcune utili considerazioni 1 ora fa S Nicola Sandon Associate, Tonucci & Partners V Alessandro Vasta Partner, Tonucci & Partners Il Dipartimento di Commercio degli Stati Uniti d'America ha pubblicato sul proprio sito web un Libro Bianco sulle garanzie per il trasferimento di dati personali verso gli USA[1] per fornire supporto agli operatori travolti dagli effetti della recente pronuncia della Corte di Giustizia dell'Unione europea ("CGUE") nel caso Data Protection Commissioner v. Facebook Ireland e Maximillian Schrems, causa C-311/18 ("sentenza Schrems II"), la quale ha da un lato invalidato il c.d. "Privacy Shield", ritenendolo inidoneo a garantire un adeguato livello di protezione dei dati personali dei cittadini europei, e dall'altro ha minato le fondamenta dei trasferimenti effettuati sulla base di meccanismi di origine contrattuale, quali le clausole contrattuali standard o le norme vincolanti d'impresa. Indice degli argomenti Trasferimento dati oltreoceano dopo Schrems II: l'antefatto Trasferimento dati oltreoceano: il contenuto del Libro Bianco Conclusioni Trasferimento dati oltreoceano dopo Schrems II: l'antefatto Con pronuncia del 16 luglio scorso, la CGUE ha (nuovamente) accolto le rimostranze dell'attivista austriaco Maximilian Schrems, il quale dal 2013 ad oggi è riuscito ad ottenere la sistematica invalidazione in sede giurisdizionale di entrambi i meccanismi di trasferimento dei dati oltreoceano messi a punto dalla Commissione e dal Governo americano per garantire la riservatezza dei dati dei cittadini europei (e non solo), nell'ordine il c.d. "Safe Harbour", adottato con decisione della Commissione (CE) 2000/520, ed il suo successore, denominato "Privacy Shield", adottato con decisione di esecuzione della Commissione (UE) 2016/1250. Ma l'impatto dell'eliminazione dalla cornice normativa del Privacy Shield su imprese e organizzazioni che quotidianamente ricorrono al trasferimento di dati al di fuori del territorio europeo appare dopotutto contenuto se paragonato al colpo (mortale?) inferto dalla Corte allo strumento delle clausole contrattuali standard. Pur riconoscendone la piena validità, tale strumento è stato di fatto reso di difficile, e talvolta impossibile, implementazione da parte della CGUE: non essendo le clausole idonee, per loro natura, a vincolare le Autorità di un paese terzo, le parti coinvolte nel trasferimento dati sono tenute a verificare attentamente, caso per caso (e Paese per Paese) ed in via preliminare, se tale meccanismo di trasferimento sia concretamente applicabile, ovverosia se la legislazione del Paese di destinazione consenta all'importatore di conformarsi pienamente

agli obblighi in esse contenuti, essendo tenuto l'esportatore, in caso contrario, a sospendere o cessare il trasferimento[2]. Il vuoto normativo venutosi a creare a seguito della sentenza Schrems II, in combinazione con la mancata concessione di un grace period[3] e di chiare indicazioni da parte delle autorità competenti, sia a livello nazionale che unionale, ha scaricato su aziende ed organizzazioni pubbliche e private l'ingrato compito di effettuare una complessa valutazione sul grado di tutela per i dati personali offerto dal Paese di destinazione, compito che, se pensiamo agli Stati Uniti, nemmeno la Commissione è riuscita a portare a termine in maniera soddisfacente in ben due distinte occasioni. Trasferimento dati oltreoceano: il contenuto del Libro Bianco In contrapposizione all'incomprensibile silenzio che persiste sul versante europeo dell'Oceano Atlantico, non si è fatta invece attendere una prima risposta da parte degli Stati Uniti, che sono intervenuti rendendo disponibile un Libro Bianco sul trasferimento oltreoceano dei dati dopo il caso Schrems II, frutto di una collaborazione tra il Dipartimento di Commercio, il Dipartimento di Giustizia e l'Ufficio del Direttore Nazionale dell'Intelligence. Il Libro Bianco si apre con un'apprezzabile presa di coscienza da parte statunitense: ogni entità che trasferisce dati extra UE ai sensi delle clausole contrattuali standard (o, parimenti, delle norme vincolanti d'impresa) è tenuta a svolgere un assessment sulla legislazione vigente nel Paese di destinazione, ivi inclusa quella che disciplini l'accesso ai dati da parte di agenzie di intelligence, nonché - nei limiti di quanto necessario sulla base della precedente analisi - a individuare ed adottare idonee misure supplementari a tutela dei dati trasferiti. In caso contrario, ci si espone all'applicazione di sanzioni, quanto meno per violazione del principio cardine di responsabilizzazione, descritto all'art. 5 del Regolamento (UE) 2016/679 ("GDPR"). Il documento dismette poi i panni della guida pratica ed assume le marcate sembianze di un saggio apologetico nei confronti della normativa americana. Sebbene la sentenza Schrems non venga mai apertamente criticata, molteplici sono i punti in cui si lascia intendere che il massimo giudice europeo abbia emesso il suo giudizio in assenza di piena cognizione sulla materia, vuoi perché costretto ad esprimersi sulle limitate indicazioni sulla normativa statunitense contenute nella decisione di esecuzione della Commissione (UE) 2016/1250, vuoi perché non del tutto aggiornato su alcune rilevanti novità introdotte nel panorama legislativo americano negli anni successivi all'adozione del Privacy Shield. Il primo argomento proposto non appare tuttavia particolarmente solido, in quanto confinato ad una dimensione puramente pratica. Il Libro Bianco afferma infatti che è improbabile che i rischi per la privacy individuati dalla CGUE abbiano modo di concretizzarsi, in quanto "la maggior parte delle società operanti in UE. non si trova a trattare dati che possano destare l'interesse delle agenzie di intelligence americane". Appare abbastanza evidente come una simile statuizione (sfornita peraltro di qualsiasi elemento a sostegno) non sia in grado di incidere in maniera rilevante sulla valutazione che è richiesta agli enti che procedano al trasferimento dati verso gli USA, valutazione che deve tenere in considerazione la

potenziale capacità dell'importatore di adempiere agli obblighi posti a suo carico dalle clausole standard. Il documento tenta poi di fondare la legittimità di eventuali trasferimenti posti in essere in ossequio a ordini di accesso ai dati da parte delle Autorità americane, sottolineando come un simile trattamento potrebbe risultare giustificato in quanto "necessario per importanti motivi di interesse pubblico"[4] ai sensi della legge comunitaria o del singolo Stato membro: esistendo un rapporto di reciproca cooperazione tra agenzie di intelligence americane ed europee, nell'ambito del quale è prevista la condivisione delle informazioni rilevanti, sarebbe infatti lecito derogare alle stringenti previsioni di cui agli artt. 45 e 46 del GDPR. Ebbene, l'argomentazione offerta dal Libro Bianco non convince: considerato che l'art. 702 del FISA consente alle agenzie di intelligence di ordinare alle società americane di condividere i propri dati a valle dell'importazione degli stessi su suolo americano, è evidente come la deroga dell'interesse pubblico di cui all'art. 49 del GDPR non sarebbe in alcun modo idonea a giustificare e rendere illegittimo l'originario trasferimento dei dati dall'UE agli US. da parte della singola società interessata. Il Libro Bianco approfondisce quindi il tema centrale dei trasferimenti di dati posti in essere sulla base delle clausole contrattuali standard, ricordando che è ad oggi liberamente accessibile sul web una pletora di documentazione idonea a supportare le imprese nel loro assessment del grado di protezione per i dati personali offerto dagli USA. Assessment che gli States sembrano ritenere del tutto superfluo, già garantendo i presidi normativi posti a tutela della privacy dall'ordinamento americano che l'accesso ai dati da parte delle agenzie di intelligence si basi su norme di legge chiare e accessibili, avvenga in maniera proporzionata e per scopi legittimi, sotto la supervisione di organi indipendenti e fornendo rimedi efficaci per le eventuali violazioni dei diritti. Nello specifico il documento offre una notevole quantità di informazioni aggiuntive in merito all'art. 702 del FISA[5] e all'E.O. 12333[6], le disposizioni di diritto statunitense a fondamento delle attività di intelligence (quali i programmi PRISM e UPSTREAM) che hanno determinato l'invalidazione del Privacy Shield da parte della CGUE, non essendo state ritenute in grado di garantire una protezione per i dati personali sostanzialmente equivalente a quella offerta dal GDPR. Le principali critiche mosse dalla sentenza Schrems II a tali normative sono state la non proporzionalità rispetto alle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia richiamate dalla succitata normativa e l'assenza di un'efficace tutela giurisdizionale nei confronti delle ingerenze da parte delle autorità pubbliche nell'ambito del perseguimento di tali finalità. Ed è proprio da tali rimostranze che il Libro Bianco prende le mosse per disinnescare il potenziale esplosivo della sentenza Schrems II. Quattro sono i principali argomenti offerti dal documento con il dichiarato obiettivo di confutare le risultanze della sentenza con riferimento all'art. 702 del FISA: in primo luogo, viene con forza sostenuto l'effettivo ed indipendente ruolo di supervisione e controllo della Corte FISA, escluso dalla CGUE sulla base dell'assunto che la stessa non sarebbe stata nel concreto in grado di verificare l'operato delle agenzie quali NSA ed FBI non avendo il potere di autorizzare singole misure

di sorveglianza, bensì solo "programmi di sorveglianza, basandosi sulle certificazioni annuali predisposte dal Procuratore Generale e dal Direttore dell'Intelligence Nazionale"[7]. Il supremo giudice europeo non avrebbe infatti tenuto in debita considerazione i seguenti elementi: al momento dell'approvazione delle suddette certificazioni annuali, la Corte FISA approva anche le c.d. "targeting procedures", ovverosia quei protocolli di ingaggio, vincolanti per l'autorità governativa, che stabiliscono i criteri per l'attivazione delle singole attività di sorveglianza e ormai da tempo richiedono la formalizzazione delle ragioni che hanno spinto gli analisti all'attivazione delle misure; ogni "targeting assessment" formulato dagli analisti delle agenzie di intelligence viene sottoposto a scrutinio di legittimità da una sezione dedicata del Dipartimento di Giustizia, tenuta a segnalare qualsiasi violazione dei protocolli alla Corte FISA. La Corte FISA, dal canto suo, è dotata di poteri idonei a garantire il rispetto delle targeting procedures, potendo, nei casi più gravi, imporre la chiusura dell'attività di sorveglianza; ogni sei mesi il Dipartimento di Giustizia e l'Ufficio del Direttore Nazionale dell'Intelligence sono tenuti a fornire alla Corte FISA un report congiunto dedicato a verificare la conformità delle attività di sorveglianza in essere con i protocolli di ingaggio; Nemmeno questa tesi del Governo americano appare convincente: la possibilità per la Corte FISA di esercitare il proprio ruolo di supervisore nei confronti delle singole attività di sorveglianza sarebbe infatti meramente incidentale e relegata all'applicazione di rimedi ex post; in secondo luogo, il documento contesta il dictum della Corte in merito all'assenza di diritti di ricorso effettivi a favore degli interessati cui le Autorità statunitensi avrebbero potuto accedere sulla base dei succitati programmi di intelligence. Il Libro Bianco, infatti, fa presente che gli interessati, a prescindere dalla propria nazionalità, avrebbero la possibilità di formulare ricorsi individuali all'Autorità giurisdizionale per violazione delle attività di sorveglianza autorizzate nell'ambito del programma FISA ai sensi di almeno 3 diverse normative: il FISA stesso, il Communications Privacy Act ed infine l'Administrative Procedure Act. Bisogna in questo caso riconoscere che tutte e tre le normative in questione vengono effettivamente citate nella decisione di approvazione dei Privacy Shield quali rimedi esperibili "contro agenti del governo in caso di accesso o uso illecito dei dati personali da parte del governo, anche per asserite finalità di sicurezza nazionale"[8]; in terzo luogo, il Dipartimento di Commercio rinvia a una serie di novità legislative introdotte a seguito del 2016, anno di approvazione del Privacy Shield, che la CGUE avrebbe omesso di considerare ai fini della propria valutazione complessiva dell'impianto normativo statunitense in termini di tutela del diritto alla riservatezza. Tra queste la più significativa è l'emissione nel 2017 da parte della Corte FISA di un'ordinanza avente ad oggetto la definitiva cancellazione delle attività di c.d. "about collection", o raccolte per "referenza", grazie alla quale ad una società poteva essere chiesto di consegnare tutte le documentazioni contenenti un determinato "selettore"; infine, il Libro Bianco tenta di legittimare l'operato americano mediante un paragone con le attività di controllo giurisdizionale sulle operazioni di raccolta di informazioni da parte dall'intelligence nei vari stati membri, citando un rapporto ufficiale dell'Agenzia dell'Unione Europea per i Diritti Fondamentali del 2015[9],

da cui emerge come poco più della metà degli Stati membri coinvolgerebbe il proprio sistema giudiziario nei processi di approvazione delle attività di sorveglianza. Argomentazione questa di poco momento e del tutto speculativa in quanto prescinde dall'intero quadro normativo europeo, nell'ambito del quale è stata appena riconosciuta l'applicazione dei principi del GDPR alle ipotesi di trattamenti effettuati ai fini della sicurezza nazionale[10] proprio al fine di evitare che una dilatazione della nozione di sicurezza nazionale finisca di fatto per eludere l'effettività della tutela di un fondamentale diritto di libertà, quale quello alla protezione dei dati personali. Meno sistematiche e rigorose appaiono invece le argomentazioni a supporto in merito alle operazioni di intelligence autorizzate ai sensi dell'E.O. 12333. Questo perché, secondo il Libro Bianco, l'errore della CGUE starebbe all'origine, e dunque nel paragone tra l'art. 702 del FISA e l'ordine esecutivo in questione: l'E.O. 12333, infatti, si limiterebbe ad assegnare alle diverse agenzie di intelligence statunitensi la responsabilità di diversi tipi di attività di raccolta di informazioni e di controspionaggio, senza autorizzare in alcun modo il governo degli Stati Uniti a richiedere a una società o a una persona fisica di fornire i dati in suo possesso, dovendo simili operazioni sempre essere espressamente autorizzate su base legislativa ("by statute"). Inoltre, il diritto statunitense prevederebbe apposite tutele in materia di privacy idonee a rendere le operazioni effettuate ai sensi dell'E.O. 12333 proporzionate rispetto alle finalità della norma, quali l'individuazione delle minacce che giustificano il ricorso all'acquisizione di informazioni in blocco, la presenza di criteri idonei a verificare che le operazioni rispondano alle priorità dell'intelligence stilati da un apposito organo e la presenza di procedure interne che disciplinano le raccolte di dati effettuati in tale ambito. Conclusioni L'inciso più rappresentativo delle ventidue pagine del Libro Bianco è senz'altro il seguente: "la realtà è che i dati trasferiti negli Stati Uniti godono di una protezione paragonabile se non superiore a quella dei dati conservati all'interno dell'U.E.". Pur presentandosi come uno strumento di supporto da parte dell'amministrazione Trump alle decine di migliaia di operatori in attesa di risposte chiare, il reale obiettivo del Libro Bianco, di natura squisitamente politica, è quello di arginare la portata assolutamente dirompente della sentenza della CGUE, difendendo la solidità della cornice normativa americana a tutela della protezione dei dati personali e sostenendo in tal modo la possibilità di proseguire in maniera pressoché inalterata il trasferimento oltreoceano di dati personali sulla base delle clausole contrattuali standard. Le argomentazioni fornite a tal fine dal Dipartimento di Commercio non appaiono nel complesso esaustive né convincenti e meritano senz'altro di essere sottoposte ad un più approfondito scrutinio da parte delle autorità competenti, in particolar modo dalla task force del Comitato Europeo per la Protezione dei Dati dedicata alle misure supplementari che gli esportatori e gli importatori di dati possono essere tenuti ad adottare per garantire una protezione adeguata in caso di trasferimento dei dati, alla luce della sentenza Schrems II. È ad ogni modo indubbio che la copiosa documentazione richiamata nel documento e alcune delle puntualizzazioni effettuate possano offrire importanti spunti di riflessione per le aziende che si troveranno a dover

effettuare le proprie valutazioni sui trasferimenti oltreoceano di dati personali di cittadini europei e non., a maggior ragione in questo periodo di incertezza legato all'inerzia del vecchio continente. In assenza di una linea guida comune, una moltitudine di operatori di ogni settore che oggi basa la propria operatività su servizi digitali (e sul flusso di dati alla base di questi) si trova in bilico tra l'esigenza di porre in essere quella titanica opera di assessment della normativa dei Paesi di destinazione richiesta dalla CGUE - di straordinaria complessità per competenze e risorse da impiegare - e la totale assenza di garanzie in merito al valore di tale valutazione o di indicazioni in merito alle misure di sicurezza supplementari da implementare per procedere in conformità alla normativa. Tema quest'ultimo ancor più spinoso se si considera che alcune delle soluzioni proposte dalle Autorità nazionali (quali ad esempio la cifratura dei dati con chiave di decrittazione assegnata al solo esportatore), non sono solo economicamente onerose e tecnicamente difficoltose da implementare, ma risultano applicabili ad una limitata gamma di servizi, quali il semplice cloud storage. A tutto ciò bisogna poi aggiungere la pressione derivante dal concreto rischio di vedersi elevare sanzioni in grado di raggiungere i 20 milioni di euro o il 4% del fatturato annuo globale. A distanza di quasi tre mesi dalla pubblicazione della sentenza Schrems II, dunque, non ci si può esimere dall'invocare a gran voce un concreto intervento chiarificatore da parte delle istituzioni europee, che giunga ben prima della versione rinnovata delle clausole standard che dovrebbe vedere la luce entro la fine dell'anno. NOTE "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II", disponibile qui. Sentenza del 16 luglio 2020, Data Protection Commissioner v. Facebook Ireland e Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, punto 134. Come espressamente confermato dal Comitato Europeo per la Protezione dei Dati con le proprie FAQ ("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"). Art. 49, c. 1, lett. d) del GDPR. Foreign Intelligence Surveillance Act. Executive Order 12333. Decisione di esecuzione della Commissione (UE) 2016/1250, punto 109. Decisione di esecuzione della Commissione (UE) 2016/1250, punto 113. Agenzia dell'Unione Europea per i Diritti Fondamentali, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume I: Member States' legal frameworks" (2015). Sentenza del 6 ottobre Privacy International, C-623/17, ECLI:EU:C:2020:790.