

Il nuovo EU-USA Data Privacy Framework: quale tutela per la privacy dei cittadini europei?

di Maria Bianca Armiento - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 6 dicembre 2023

Il 10 luglio 2023, la Commissione europea ha adottato, ai sensi dell'art. 45 § 3 del Regolamento sulla Protezione dei Dati Personali (GDPR), la decisione di adeguatezza dello EU-USA Data Privacy Framework. L'accordo è stato annunciato il 25 marzo 2022 con un comunicato congiunto da parte del Presidente americano Joe Biden e dalla Presidente della Commissione europea Ursula Von Der Leyen. Esso recepisce le previsioni contenute nell'Executive Order statunitense del Presidente Joe Biden del 7 ottobre 2022 "Enhancing Safeguards for United States Signals Intelligence Activities".

Al pari di quanto avvenuto con i precedenti Safe Harbor del 2000 e Privacy Shield del 2016, la decisione esprime un giudizio di adeguatezza sulla disciplina statunitense del trasferimento di dati personali dall'Unione Europea alle imprese USA partecipanti al Framework. In altre parole, si riconosce che i trasferimenti di dati verso gli Stati Uniti sono improntati a un livello adeguato di protezione dei diritti e delle libertà dei soggetti interessati. Ne consegue che, alla luce del nuovo accordo, siffatti trasferimenti non necessitano di ulteriori misure aggiuntive a garanzia dei dati personali.

L'intervento della Commissione si inserisce in un quadro di incertezza normativa, verificatasi a seguito delle due note pronunce Schrems che avevano portato all'annullamento dei precedenti accordi.

Volendo riassumere, la vicenda (in questo Osservatorio, ne abbiamo parlato QUI e QUI) trae origine dal reclamo presentato da Max Schrems, cittadino austriaco, al Garante privacy irlandese per chiedere la sospensione del trasferimento dei propri dati immessi su Facebook verso gli Stati Uniti, Paese in cui la società è ubicata. Il reclamo era proposto da Schrems anche a seguito delle rivelazioni di Edward Snowden sull'utilizzo che le agenzie americane di intelligence facevano dei dati personali, compresi quelli conservati da Facebook (ne abbiamo parlato in questo Osservatorio QUI).

La Corte di Giustizia dell'Unione Europea, adita dalla High Court irlandese, considerava invalido l'accordo Safe Harbor, dal momento che la possibilità di accesso generalizzato e indiscriminato da parte delle autorità pubbliche a dati personali, in assenza di alcun rimedio esperibile da parte degli interessati, costituiva una violazione del diritto europeo. Successivamente, Schrems chiedeva l'annullamento anche del successivo accordo Privacy Shields, contestando, oltre alle modalità di utilizzo dei dati personali, il ricorso alle clausole contrattuali standard (vale a dire, clausole standardizzate, preventivamente approvate dalla Commissione, che consentono il trasferimento di dati personali dall'Europa agli Stati Uniti). Nel 2020, la Corte di Giustizia dichiarava invalida la decisione di esecuzione del Privacy Shield del 2016: pur ritenendo valide le clausole contrattuali standard, rilevava come l'impianto normativo statunitense sulla privacy, unito all'assenza di un meccanismo di reclamo esperibile dai cittadini europei, non garantisse una protezione adeguata dei dati personali.

Ciò premesso, cosa prevede il nuovo Framework?

Anche alla luce degli interventi della Corte di Giustizia, vi sono alcuni profili di interesse.

Innanzitutto, è previsto un sistema di certificazione delle imprese, soggetto a revisione annuale. Pertanto, le società statunitensi che vogliano aderire al Framework, devono rispettare i principi in materia di protezione dei dati personali elaborati dallo U.S. Department of Commerce. Il relativo accertamento, così come il monitoraggio sul rispetto dei principi, è condotto dalla Federal Trade Commission.

Il Framework pone poi limiti all'accesso ai dati da parte delle agenzie di intelligence statunitensi: ciò potrà avvenire solo ai fini di quanto sia necessario e proporzionato per proteggere la sicurezza nazionale.

Da ultimo, cogliendo una delle criticità emerse grazie alla sentenza Schrems II, viene introdotto un meccanismo di reclamo su due livelli. È infatti istituito il Civil Liberties Protection Officer, nella persona di un funzionario dell'intelligence statunitense, incaricato di far rispettare la riservatezza e la tutela dei diritti fondamentali dei cittadini europei. Questi ultimi potranno inoltre accedere gratuitamente alla Data Protection Review Court: si tratta di un tribunale del riesame indipendente, che, in caso di trattamento scorretto dei dati personali dei cittadini europei da parte di imprese e agenzie di intelligence americane, può imporre misure vincolanti (come, ad esempio, ordinare la cancellazione dei dati raccolti in violazione delle garanzie predisposte).

Questo, dunque, il nuovo quadro normativo. All'alba della sua adozione, l'associazione None Of Your Business (NOYB), presieduta proprio da Max Schrems, nel commentare il nuovo accordo, ha aspramente criticato la nuova decisione, annunciando che procederà ad impugnarla, come già fatto in passato. Infatti, il Privacy Framework riprodurrebbe le stesse criticità dei precedenti.

Il nuovo accordo, dunque, potrebbe non avere vita facile. Emergono alcuni dubbi sulla sua capacità di contrastare o quantomeno limitare le criticità che avevano portato all'annullamento di Safe Harbor e Privacy Shield.

Se ne possono evidenziare tre.

In primo luogo, emerge un problema di “disallineamento” tra le legislazioni europea e americana. Negli Stati Uniti, infatti, non esiste una legge federale sulla protezione dei dati personali. Questo profilo è stato messo in luce, ad esempio, dal Comitato europeo per la Protezione dei Dati, che pur rilevando i miglioramenti del nuovo accordo, ha espresso non poche perplessità su quest'ultimo. In particolare, il Comitato, proprio alla luce delle differenze normative in materia di privacy tra Stati Uniti ed Unione Europea (differenze, in alcuni casi, di natura non unicamente terminologica), si è interrogato sulla possibilità che i cittadini europei fossero concretamente in grado di esercitare nei confronti dei titolari del trattamento statunitensi i diritti riconosciuti dal GDPR (come il diritto d'accesso o il diritto a non essere sottoposti a una decisione completamente automatizzata). Una questione collegata alla precedente riguarda il principio di proporzionalità/necessità che deve informare l'utilizzo dei dati da parte delle agenzie di intelligence. Il principio potrebbe essere infatti interpretato dalle amministrazioni statunitensi in modo molto diverso da quanto avviene nell'Unione Europea.

In secondo luogo, viene da chiedersi se il nuovo meccanismo di reclamo su due livelli possa considerarsi effettivo nel tutelare i dati personali dei cittadini europei. Sul punto, non può non menzionarsi la risoluzione dell'11 maggio 2023, con cui il Parlamento europeo ha espresso in modo netto la propria contrarietà al testo dell'accordo. Nello specifico, il Parlamento ha sottolineato l'inadeguatezza del meccanismo di reclamo, dal momento che le decisioni della Data Protection Review Court non sono pubbliche e che i giudici sono soggetti al controllo del Presidente degli Stati Uniti, con la conseguenza che il Tribunale non godrebbe di piena indipendenza.

Da ultimo, si può rilevare come la nuova decisione venga adottata in un periodo storico particolarmente “delicato” per la protezione dei dati personali. Si pensi, ad esempio, alla comparsa di tecnologie avanzate come l'intelligenza artificiale generativa (in questo Osservatorio, con riferimento all'ormai famoso ChatGPT e alle sue implicazioni in termini di tutela della riservatezza, ne abbiamo parlato QUI, QUI e QUI). Per questi sistemi, le tutele tradizionali sembrano non essere più sufficienti, imponendo un generale rafforzamento delle garanzie per gli interessati.

Vi è dunque il rischio che la nuova decisione si riveli già obsoleta ben prima di cominciare a sortire i suoi effetti.

**Le opinioni espresse nel presente contributo sono attribuibili esclusivamente all'autrice e non impegnano l'Istituzione di appartenenza.*