Il Sole 24 ORE

Interventi

Perché sul privacy shield serve una soluzione urgente

di Andrea Fedi e Lucio Scudiero

23 luglio 2020

L'invalidazione del Privacy Shield da parte della Corte di Giustizia (CJEU) (vd. Sole24Ore di Venerdì 17 luglio) **cancella uno dei principali strumenti che legittimavano il trasferimento di dati personali verso gli Usa** e mette a rischio i flussi tra l'Unione e il resto del mondo.

Ai giudici lussemburghesi non sono bastate le migliorie – rispetto al precedente Safe Harbor – che il Privacy Shield aveva incorporato, tra cui l'istituzione di un Ombudsperson competente a garantire tutela legale imparziale agli europei i cui dati fossero stati trasferiti in Usa. Troppo poco – secondo i giudici del Lussemburgo – per garantire quel livello di protezione "sostanzialmente equivalente" richiesto dalle norme privacy europee. Tale equivalenza, infatti, secondo i giudici comunitari e il Comitato Europeo per la Protezione dei Dati (EDPB), va valutata alla luce dei criteri previsti dall'articolo 46(2) del GDPR e la persistenza di programmi di sorveglianza governativi su cittadini non americani, combinati a un controllo giurisdizionale ritenuto troppo debole per rispettare i canoni europei, non garantiscono a sufficienza il diritto alla protezione dei dati come inteso in Europa.

È legittimo adesso interrogarsi sugli effetti che la sentenza demolitoria della Corte potrà avere: se la stessa sarà applicata retroattivamente a tutti i trasferimenti sino a ieri completati sulla base del Privacy Shield (oramai dichiarato invalido); se sarà previsto un periodo di grazia per consentire alle imprese di riorganizzarsi; se EDPB e Garanti Privacy nazionali attiveranno i loro poteri per trovare una soluzione rapida, efficiente e non dogmatica.

Peraltro il giudizio della CJEU, oltre a provocare l'annullamento del Privacy Shield, di fatto ha posto una seria ipoteca sulle *standard contractual clauses* (SCCs) adottate dalla Commissione Europea con decisione 2010/87, che costituiscono di gran lunga lo strumento più utilizzato dalle imprese per esportare i dati personali fuori dall'Unione. Finora la firma delle SCCs, da parte dell'impresa europea esportatrice e di quella extraeuropea importatrice, aveva garantito la legalità del trasferimento; adesso invece, alla luce della decisione della Corte, le parti devono, prima e durante tutta la loro relazione, monitorare la conformità dell'ordinamento straniero di destinazione con gli standard europei. I giudici, sostenuti dall'EDPB, scrivono infatti che i soggetti importatori dovranno informare l'impresa europea qualora non fossero in grado di rispettare i principi europei di protezione dei dati personali (ad esempio perché hanno ricevuto un ordine di comunicazione dei dati personali ad un'autorità del loro ordinamento) e, in tali casi, l'impresa europea dovrà sospendere il trasferimento.

Il problema, enorme, è che di questo complesso sindacato giuridico vengono gravate le imprese che intraprendono il trasferimento di dati personali.

Inoltre, alla luce del giudizio negativo della CJEU sui poteri intrusivi delle autorità americane, sembra logico dedurre che il test di compatibilità non possa più essere superato nei rapporti transatlantici. Non si capisce, infatti, dopo la sentenza della scorsa settimana, come due imprese possano rovesciare le conclusioni negative della Corte sulle carenze dell'ordinamento americano.

L'impatto sarà dirompente in molti settori, a cominciare dal cloud computing, i cui principali fornitori sono statunitensi e incorporano nella propria contrattualistica standard proprio le SCCs; ma si pensi anche a quella amplissima fetta di ricerca clinica finanziata e/o monitorata da imprese d'oltreoceano e condotta in centri di sperimentazione europei, che sulle SCCs ha sempre fondato la liceità dei trasferimenti dei dati dei pazienti dall'Ue; o, ancora, si ponga mente ai trasferimenti dei dati del personali interni ai gruppi multinazionali.

Che fare, dunque?

Per i gruppi multinazionali la strada principale è quella di ricorrere alle norme vincolanti d'impresa, passando per l'approvazione delle autorità garanti, il cui vaglio dovrà essere veloce ed efficiente.

Ma una spinta maggiore va a questo punto impressa anche agli schemi di certificazione e ai codici di

Il Sole 24 ORE

condotta, che, secondo il GDPR, possono costituire strumenti per il trasferimento lecito di dati personali fuori dall'Ue; al momento non ve ne sono di approvati a livello europeo con il bollino di garanzia delle autorità garanti. Un vulnus che mercato e istituzioni dovranno sanare al più presto.

Nel frattempo, almeno per le imprese che si servono di servizi cloud forniti da *providers* extraeuropei, un'opzione è quella di rivolgersi a quei fornitori che abbiano aderito a uno degli schemi di certificazione elencati dall'agenzia europea per la sicurezza delle reti (ENISA) nel proprio Cloud Certification Schemes List: questi schemi non hanno il valore legale previsto dal GDPR (articolo 46, paragrafo 2, lett. e ed f), ma sono comunque pubblicamente sostenuti da un'agenzia europea, e alcuni di essi sono stati elaborati in seno ad iniziative patrocinate dalla Commissione Europea.

Altre strade possono essere tracciate se si interpretano, prudentemente ma evolutivamente, le eccezioni tracciate nell'art. 49 GDPR.

Resta in ogni caso cruciale l'intervento delle autorità di controllo privacy europee, perché dopo la pronuncia della scorsa settimana la tenuta dal sistema dei flussi internazionali di dati personali dipende da ciò che decideranno.

Legance – Avvocati Associati