Innovation Law Insights

Innovazione e diritto: le novità della settimana

INNOVATION LAW INSIGHTS

17 luglio 2020

Privacy

La Corte di Giustizia UE invalida il Privacy Shield, ma anche le clausole contrattuali standard potrebbero non bastare sul trasferimento dei dati

Nella causa c.d. Schrems II, la Corte di giustizia europea ha stabilito che il Privacy Shield è invalido, ma la possibilità di basarsi su clausole contrattuali standard per il trasferimento dei dati deve essere valutata caso per caso.

In una delle sentenze più attese dell'anno (Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems C-311/18, comunemente nota come "Schrems II"), la CGUE ha invalidato il Privacy Shield come meccanismo per il trasferimento di dati personali negli Stati Uniti. La CGUE ha inoltre ritenuto che le clausole contrattuali standard, il meccanismo più comunemente utilizzato per il trasferimento di dati personali al di fuori dell'UE, rimane valido a condizione che le imprese verifichino se il contesto generale del trasferimento (compreso il paese di destinazione) offre garanzie adeguate ai dati personali delle persone. La sentenza impone alle autorità privacy europee di sospendere o vietare i trasferimenti qualora non sia possibile fornire tali garanzie appropriate.

Qualche informazione di background sul caso Schrems II

Il GDPR regola il trasferimento dei dati personali dall'UE, richiedendo un valido meccanismo di trasferimento. Tali meccanismi includono le decisioni di adeguatezza della Commissione Europea (come il Privacy Shield) e le opportune salvaguardie (come le Standard Contractual Clauses e le Binding Corporate Rules, che riguardano i trasferimenti intragruppo).

Non è la prima volta che la CGUE invalida un meccanismo di trasferimento: nel 2015, la CGUE ha invalidato il c.d. Safe Harbor (il predecessore di Privacy Shield) in un caso comunemente denominato come Schrems I. Al centro della contestazione avanzata da Schrems c'era il fatto che le leggi di sorveglianza degli Stati Uniti non offrivano una protezione adeguata dei dati personali dell'UE, in particolare in relazione alla condivisione da parte di Facebook dei dati personali dei cittadini dell'UE con l'Agenzia per la sicurezza nazionale degli Stati Uniti.

I punti chiave della sentenza Schrems II che ha invalidato il Privacy Shield

La Corte di giustizia europea ha dichiarato quanto segue:

1. Privacy Shield invalidato come meccanismo per il trasferimento di dati personali negli Stati Uniti

La CGUE ha ritenuto che, a causa del potenziale accesso e dell'utilizzo da parte delle autorità pubbliche statunitensi ai dati personali trasferiti negli Stati Uniti, non può essere garantito un livello di protezione sostanzialmente equivalente a quello garantito dal diritto comunitario. La sentenza continua indicando che "*i requisiti di sicurezza nazionale, di interesse pubblico e di applicazione della legge degli Stati Uniti prevalgono, evitando così le limitazioni imposte da i diritti fondamentali delle persone i cui dati sono trasferiti in quel paese terzo*". Inoltre, in relazione al principio di proporzionalità previsto dal diritto dell'UE, la CGUE ha ritenuto che i "programmi di sorveglianza statunitensi basati su tali disposizioni non si limitano allo stretto necessario". La CGUE ha ritenuto che il meccanismo del Privacy Shield Ombudsperson non fornisce un livello di protezione adeguato, in quanto gli interessati non hanno alcun motivo di agire dinanzi a un organismo che offra garanzie sostanzialmente equivalenti a quelle richieste dal diritto dell'UE.

2. Le clausole contrattuali standard continuano ad essere un meccanismo valido per il trasferimento di dati personali verso paesi al di fuori del SEE, ma soggetto a limitazioni
   La CGUE ha ritenuto che le clausole contrattuali standard non sempre costituiscono un mezzo sufficiente per garantire, in pratica, l'effettiva protezione dei dati personali trasferiti in un paese terzo. In particolare, *"qualora la legge di tale paese terzo consenta alle sue autorità pubbliche di interferire con i diritti degli interessati cui tali dati si riferiscono*". La sentenza ribadisce l'importanza che le imprese verifichino, prima di qualsiasi trasferimento, se nel paese terzo in questione è rispettato un livello di protezione adeguato. In mancanza di garanzie adeguate, il trasferimento di dati personali verso tale paese terzo dovrebbe essere sospeso dall'esportatore o, in mancanza, dall'autorità di controllo della protezione dei dati dello Stato membro interessato. Sebbene non sia esplicitamente menzionato nella sentenza, è probabile che tale obbligo si applichi anche ad altri meccanismi di trasferimento dei dati, comprese le binding corporate rules.

Cosa significa tutto questo per la vostra azienda?

La sentenza ha gravi implicazioni sul trasferimento di dati personali al di fuori dell'UE ed è un campanello d'allarme per le imprese dell'UE:

1. le imprese dovrebbero analizzare i flussi di dati che comportano il trasferimento di dati personali al di fuori dell'UE e determinare quale meccanismo di trasferimento (Privacy Shield, le clausole contrattuali standard, ecc.) viene attualmente utilizzato;
2. per quei trasferimenti che si basano sul Privacy Shield, è necessario trovare un meccanismo di trasferimento alternativo in via prioritaria;
3. per le imprese che attualmente utilizzano, o stanno considerando di utilizzare (in alternativa al Privacy Shield), le clausole contrattuali standard, le imprese devono valutare il livello di garanzie appropriate fornite da tale trasferimento per determinare se le clausole contrattuali standard sono un meccanismo disponibile. Gli effettivi rischi devono essere presi in considerazione, nel contesto del settore / industria e di altri fattori rilevanti, tra cui il paese di destinazione e l'identità del destinatario, che può essere difficile, in particolare data l'incertezza nella sentenza della CGUE in relazione alla possibilità di fare affidamento sulle clausole contrattuali standard per i trasferimenti di dati personali verso gli Stati Uniti;
4. le autorità di protezione dei dati dell'UE avranno il compito non invidiabile di determinare, in ultima analisi, l'adeguatezza delle garanzie appropriate; e
5. Le implicazioni della sentenza potrebbero innescare un ulteriore ciclo di discussioni politiche tra l'UE e gli Stati Uniti.

Nonostante le questioni sollevate dalla CGUE, le clausole contrattuali standard rimangono, per ora, l'opzione più realistica per il trasferimento di dati personali al di fuori del SEE. Ci aspettiamo che ci vorrà del tempo prima che le implicazioni pratiche della decisione possano essere pienamente applicate ed entrare in vigore.

Considerato l'impatto che questa decisione avrà sulle imprese, ci aspettiamo che le autorità di controllo della protezione dei dati degli Stati membri possano ritardare l'avvio di azioni esecutive per consentire alle imprese di valutare la situazione e di mettere in atto soluzioni alternative, come è successo dopo la sentenza Schrems I del 2015 e l'invalidazione del quadro normativo Safe Harbor. Tuttavia, non è garantito un periodo di grazia. Né impedirebbe ai singoli individui di presentare richieste di risarcimento private o di azioni legali di gruppo.

DLA Piper sta sviluppando una metodologia per assistere i nostri clienti nella navigazione dell'impatto della sentenza e nell'esecuzione del test richiesto quando ci si affida alle clausole contrattuali standard. E discuteremo la decisione oggi 17

luglio 2020 in un webinar i cui dettagli sono disponibili QUI.

Sanzione privacy di EUR1,24 milioni nei confronti di una compagnia di assicurazioni in Germania per attività di marketing senza consenso

Il Garante privacy dello stato federale tedesco del Baden-Württemberg ha emesso una sanzione nei confronti della compagnia di assicurazioni sanitarie AOK Baden-Württemberg (AOK) di EUR1,24 milioni poiché erano state svolte accidentalmente attività di marketing nei confronti di oltre 500 destinatari in assenza del relativo consenso.

La CGUE ha ritenuto che le clausole contrattuali standard non sempre costituiscono un mezzo sufficiente per garantire, in pratica, l'effettiva protezione dei dati personali trasferiti in un paese terzo. In particolare, "qualora la legge di tale paese terzo consenta alle sue autorità pubbliche di interferire con i diritti degli interessati cui tali dati si riferiscono". La sentenza ribadisce l'importanza che le imprese verifichino, prima di qualsiasi trasferimento, se nel paese terzo in questione è rispettato un livello di protezione adeguato. In mancanza di garanzie adeguate, il trasferimento di dati personali verso tale paese terzo dovrebbe essere sospeso dall'esportatore o, in mancanza, dall'autorità di controllo della protezione dei dati dello Stato membro interessato. Sebbene non sia esplicitamente menzionato nella sentenza, è probabile che tale obbligo si applichi anche ad altri meccanismi di trasferimento dei dati, comprese le binding corporate rules.

Da quanto emerge dalla ricostruzione pubblicata dall'Autorità, tra il 2015 e il 2019 AOK aveva organizzato in Germania diversi concorsi a premi, in occasione dei quali aveva raccolto i dati personali dei partecipanti – ivi inclusi i dati di contatto e i dati relativi alle coperture assicurative sanitarie – chiedendo altresì a questi ultimi di fornire il consenso al trattamento dei dati personali per l'invio di comunicazioni di marketing. Per garantire la sicurezza del trattamento dei dati personali ai sensi dell'articolo 32 del GDPR, la compagnia assicurativa aveva implementato procedure interne ed effettuato dei corsi di formazione in materia di privacy rivolti al personale.

Tuttavia, le misure tecniche e organizzative adottate non si sono rivelate sufficienti a garantire il rispetto della normativa sul trattamento dei dati personali applicabile. Dalle indagini effettuate dal Garante privacy tedesco, è emerso che erano stati inclusi quali destinatari delle comunicazioni non soltanto i partecipanti ai concorsi a premi che avevano prestato il loro consenso, ma anche oltre 500 interessati che non avevano mai prestato il consenso all'invio di comunicazioni di marketing. A seguito della contestazione, AOK ha immediatamente interrotto tutte le attività di marketing per rivedere le proprie procedure interne e la conformità dei trattamenti con il GDPR, ha creato una *task force* per la protezione dei dati personali nelle vendite e ha tempestivamente adattato dei processi interni e delle strutture di controllo.

Nonostante l'adozione di queste misure, l'autorità privacy ha emesso la sopra citata sanzione che ha tenuto conto dei seguenti fattori:

- la risposta tempestiva, proattiva e collaborativa della compagnia assicurativa;
- le considerevoli dimensioni di AOK, che conta oltre 4,5 milioni di assicurati e circa 230.000 imprese clienti;
- l'importanza di quest'ultima nell'ambito del sistema sanitario statale in quanto è una compagnia di assicurazione sanitaria pubblica e, quindi, responsabile del mantenimento, del ripristino o del miglioramento dello stato di salute dell'assicurato; e
- il particolare contesto di emergenza attuale, segnato dalla pandemia da COVID-19.

Alla luce di tutto quanto precede, il Garante privacy tedesco ha ritenuto che una sanzione di EUR1,24 milioni fosse adeguata rispetto alle violazioni riscontrate nel contesto di riferimento.

Technology Media & Telecom

L'AGCM invita le istituzioni a rimuovere gli ostacoli allo sviluppo della banda ultralarga

L'Autorità Garante della Concorrenza e del Mercato (AGCM) ha indirizzato ai Presidenti del Senato della Repubblica e della Camera dei Deputati, al Presidente del Consiglio dei Ministri, al Ministro dello Sviluppo Economico, all'Autorità per le Garanzie nelle Comunicazioni (AGCom) e all'Associazione Nazionale dei Comuni Italiani (ANCI) una segnalazione ai sensi dell'art. 21 della legge n. 287/90 relativa allo sviluppo delle infrastrutture di telecomunicazione fissa e mobile a banda ultralarga, in un'ottica di promozione degli investimenti e tutela di un necessario gioco concorrenziale.

A parere dell'AGCM, l'attuale contesto emergenziale ha mostrato come le infrastrutture di telecomunicazioni, sia mobili sia fisse, costituiscono un elemento fondamentale per lo sviluppo del tessuto imprenditoriale e la crescita economica. La

diffusione di infrastrutture a banda ultralarga sul territorio è altresì necessaria per la diffusione dell'informazione, la condivisione e l'accessibilità al patrimonio pubblico e lo sviluppo, l'adozione e il potenziamento di nuovi servizi digitali, sia nel settore pubblico che nel settore privato. Le infrastrutture a banda ultralarga sono elementi essenziali anche per la promozione dell'inclusione e della partecipazione dei cittadini a svariati aspetti della vita sociale ed economica.

L'AGCM ha ritenuto dunque di rinnovare l'invito, già rivolto con una segnalazione del dicembre 2018, alle amministrazioni ai vari livelli di governo di adoperarsi al fine di eliminare gli ostacoli per la creazione e l'installazione di reti di comunicazione elettronica. In questo contesto, l'Autorità Garante della Concorrenza e del Mercato auspica in particolare l'adozione di misure volte a ridurre gli oneri amministrativi e le barriere allo sviluppo delle infrastrutture di telecomunicazione, quali, ad esempio, la riduzione delle tempistiche e delle complessità legate alle procedure autorizzatorie, l'adozione di procedure e moduli uniformi per tutti gli enti locali, la revisione delle norme limitative del subappalto per il concessionario pubblico al fine di superare i limiti di produzione aprendo un maggior numero di cantieri e, infine, la valorizzazione e messa in piena operatività dello strumento del SINFI (catasto delle infrastrutture), anche mediante la creazione di un *database* delle coperture delle reti di comunicazione elettronica disponibili nel territorio nazionale. Al contempo, l'AGCM auspica la realizzazione di un *level* playing field che possa favorire il dispiegamento degli investimenti e il corretto svolgersi del gioco della concorrenza tra gli operatori.

L'Autorità ha altresì dichiarato di accogliere con favore la previsione di strumenti di sostegno della domanda privata quali l'erogazione di *voucher* e dispositivi elettronici e ritiene che gli ulteriori strumenti destinati alle famiglie e alle imprese debbano essere erogati esclusivamente per connessioni con velocità di almeno 100 Mpbs, al fine di evitare che parte rilevante della domanda si assesti su servizi a bassa potenzialità, inadeguati al soddisfacimento delle esigenze di connettività del Paese.

Infine, l'AGCM ha segnalato l'opportunità di modificare le norme relative al diritto di recesso, al fine di limitare l'uso di strumenti contrattuali che determinano effetti di *lock-in* ed ostacolano la mobilità degli utenti, quali, ad esempio, il pagamento di corrispettivi in caso di recesso anticipato dei consumatori che non siano commisurati ai costi reali sostenuti dall'operatore o che siano già stati completamente ammortizzati. Osserva l'AGCM che l'eliminazione dei meccanismi di *lock-in* favorirebbe la concorrenza per la fornitura di servizi sempre più veloci e lo sviluppo di migliori tecnologie e sosterrebbe gli investimenti legati alla domanda di connettività, senza oneri pubblici.

Intellectual Property

La CGUE si pronuncia sui limiti applicabili al copyright rispetto al caricamento di film su YouTube senza il consenso del titolare

Con la decisione relativa alla controversia *Constantin Film Verleih v YouTube LLC and Google Inc* (C-264/19) del 9 luglio 2020, la Corte di Giustizia UE ha dichiarato che, nell'ambito del caricamento di un film su una piattaforma di video online senza il consenso del titolare dei diritti di copyright, la Direttiva 2004/48 non obbliga le autorità giudiziarie a ordinare al gestore della piattaforma video di fornire l'indirizzo di posta elettronica, l'indirizzo IP o il numero di telefono dell'utente che ha caricato il film controverso. La Corte ha infatti riconosciuto come la direttiva, la quale prevede che sia fornito *l'"indirizzo"* delle persone che hanno violato un diritto di proprietà intellettuale, si riferisce con tale termine unicamente all'indirizzo postale delle persone interessate.

Nel caso di specie, nel 2013 e nel 2014 i film "*Parker*" e "*Scary Movie 5*" sono stati caricati sulla piattaforma YouTube senza il consenso della Constantin Film Verleih, titolare dei diritti di sfruttamento esclusivi su tali opere in Germania. Tali film sono stati visualizzati varie decine di migliaia di volte. La Constantin Film Verleih ha pertanto intimato a YouTube e Google di fornirle un insieme di informazioni in relazione a ciascuno degli utenti che aveva proceduto al caricamento dei film sulla piattaforma di video. Le due società hanno rifiutato di fornire alla Constantin Film Verleih le informazioni relative a detti utenti, in particolare i loro indirizzi di posta elettronica e numeri di telefono nonché gli indirizzi IP da loro utilizzati tanto al momento del caricamento dei file interessati quanto al momento dell'ultimo accesso al loro account Google/YouTube.

La controversia principale verteva pertanto sulla riconducibilità di simili informazioni alla nozione di "*indirizzo*" ai sensi della Direttiva 2004/48. A tal riguardo, la Corte ha rilevato in primo luogo che, quanto al significato ordinario e abituale del termine "*indirizzo*", esso riguarda unicamente l'indirizzo postale, vale a dire il luogo di domicilio o di residenza di una determinata persona. Secondo la Corte, ne consegue che tale termine, se utilizzato senza ulteriori precisazioni, come avviene nell'ambito della Direttiva 2004/48, non si riferisce all'indirizzo di posta elettronica, al numero di telefono o

all'indirizzo IP. In secondo luogo, la Corte ha ricordato come i lavori preparatori che hanno condotto all'adozione della Direttiva 2004/48 non contengono alcun indizio tale da suggerire che il termine "*indirizzo*" debba intendersi riferito non solo all'indirizzo postale, ma anche all'indirizzo di posta elettronica, al numero di telefono o all'indirizzo IP delle persone interessate. In terzo luogo, la Corte ha riconosciuto come dall'esame di ulteriori disposizioni del diritto UE che fanno riferimento all'indirizzo di posta elettronica o all'indirizzo IP emerge che nessuno di essi utilizza il termine " *indirizzo*", senza ulteriori precisazioni, per designare il numero di telefono, l'indirizzo IP o l'indirizzo di posta elettronica.

Life Sciences

La FDA approva un videogioco per l'ADHD

Il 15 giugno 2020 la Food and Drug Administration (FDA) statunitense ha autorizzato la commercializzazione di EndeavorRx, una terapia digitale basata su un videogioco pensato per migliorare l'attenzione nei bambini con disturbo da deficit di attenzione e iperattività (ADHD). La tecnologia è stata testata su un campione di circa 600 pazienti pediatrici affetti da ADHD attraverso 5 trial clinici svolti tra il 2016 e il 2017 in 20 istituti negli Stati Uniti e prevedeva la somministrazione del gioco per 25 minuti al giorno per 5 giorni a settimana. I risultati hanno mostrato che in quasi il 50% dei casi i genitori hanno rilevato un miglioramento dopo 4 settimane e, a distanza di un altro mese, la percentuale superava il 65%.

Durante il periodo di lockdown, la FDA ha adottato un approccio meno restrittivo all'applicazione delle norme sui dispositivi sanitari digitali impiegati per le patologie psichiatriche, al fine di fornire un supporto ai pazienti che non potevano accedere alle cure tradizionali a causa dell'isolamento. In questo contesto, EndeavorRx è stato messo gratuitamente a disposizione delle famiglie con bambini con diagnosi di ADHD, prima dell'approvazione formale della FDA. In particolare, il videogioco utilizza un algoritmo progettato per migliorare l'attenzione, la capacità di svolgere attività in parallelo e la gestione delle interferenze. Inoltre, tale algoritmo è in grado di modificare la terapia sulla base dei risultati ottenuti dal paziente, in maniera tale da rendere il videogioco gradualmente più complesso.

Sebbene EndeavorRx non possa sostituire i farmaci tradizionali, si tratta di un'efficace terapia di supporto, con un alto livello di accettabilità specialmente nei pazienti pediatrici. Inoltre, detto trattamento mette in evidenza l'attuale tendenza alla *gamification*, ossia lo sviluppo di giochi in contesti che tradizionalmente non li prevedono, come quello medico.

Commissione europea approva Veklury (remdesivir), primo farmaco contro il COVID-19

A pochi giorni dall'approvazione del Comitato per i medicinali per uso umano (CHMP) dell'Agenzia del farmaco europea (EMA), è arrivato il parere positivo della Commissione europea per l'autorizzazione all'immissione in commercio condizionata di Veklury (remdesivir), farmaco antivirale nato per combattere l'ebola, per il trattamento del COVID-19. In particolare, questo tipo di autorizzazione viene concessa a un medicinale quando il beneficio per la salute pubblica è immediato e supera il rischio legato al fatto che non tutti i dati sono ancora disponibili.

Remdesivir è il primo farmaco atto a contrastare il virus autorizzato nel territorio dell'Unione europea e, per il momento, potrà essere utilizzato solamente per il trattamento di pazienti con più di 12 anni in stadio avanzato di COVID-19 con polmonite, che richiedono ossigeno supplementare. Tenendo conto dei dati disponibili, infatti, l'EMA ha ritenuto che l'equilibrio tra benefici e rischi si sia dimostrato positivo, per il momento, solo nei pazienti con malattia grave. La valutazione del remdesivir era stata avviata a inizio maggio 2020, quando il farmaco veniva già utilizzato in via sperimentale in molti paesi, inclusa l'Italia, ed è avvenuta in un periodo di tempo particolarmente breve, grazie alla procedura di revisione a rotazione, un approccio utilizzato dall'EMA durante le emergenze sanitarie pubbliche per valutare i dati su base continuativa, ossia mano a mano che diventano disponibili.

La rubrica Innovation Law Insights è stata redatta dai professionisti dello studio legale DLA Piper con il coordinamento di Giordana Babini, Lara Mastrangelo, Filippo Grondona e Andrea Michelangeli.

Per maggiori informazioni sugli argomenti trattati, è possibile contattare i soci responsabili delle questioni Giulio Coraggio, Alessandro Ferrari, Gualtiero Dragotti, Roberto Valenti, Marco de Morpurgo e Alessandro Boso Caretta.

È possibile leggere le legal predictions per il 2020 dei professionisti del dipartimento di Intellectual Property and Technology di DLA Piper qui, acquistare il volume redatto dagli stessi in materia di intelligenza artificiale e digital transformation qui e consultare una pubblicazione di DLA Piper che illustra la normativa sugli Esports di 38 giurisdizioni

qui.

DLA Piper Studio Legale Tributario Associato tratta i dati personali in conformità con l'informativa sul trattamento dei dati personali disponibile qui.

Qualora non si volesse più ricevere gli Innovation Law Insights o ci si volesse iscrivere alla stessa, è possibile inviare un'email a Noemi Buttazzo.