ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

IoT e Privacy

Dr. Maria Letizia Perugini

Roma 17/12/2015

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
  - Casi pratici
  - V Tech
- Hallo Barbie
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
- Casi pratici
  - V Tech
  - Hallo Barbie
- Q&A
- Bibliografia & sitografia

Presentazione del relatore

- **Maria Letizia Perugini**
- *Dottoranda in Diritto e Nuove Tecnologie Curriculum in Computer Forensics*
- *CIRSFID – Centro Interdipartimentale di Ricerca in Storia, Sociologia, Filosofia del Diritto e Informatica Giuridica*
- *Alma Mater Studiorum – Università degli Studi di Bologna*

- *https://www.unibo.it/sitoweb/maria.perugini*

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
- Casi pratici
  - V Tech
  - Hallo Barbie
- Q&A
- Bibliografia & sitografia

Consultazione pubblica su IOT – Deliberazione GPDP 26 .03.2015

- L'*Internet of Things* (IoT) fa riferimento ad infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es. RFID, *bluetooth* etc.), sia tramite una rete di comunicazione elettronica.
- I dispositivi interessati non sono soltanto i tradizionali computer o *smartphone*, ma anche quelli integrati in oggetti di uso quotidiano ("*things*"), come dispositivi indossabili (cd. *wearable*), di automazione domestica (cd. domotica) e di georeferenziazione e navigazione assistita; ciò comporta la raccolta e la gestione di dati relativi a comportamenti, abitudini, preferenze e stato di salute degli utenti spesso inconsapevoli, con l'effetto di consentirne l'identificazione, diretta o indiretta, mediante la creazione di profili anche dettagliati.
- Se ne induce, quindi, l'importanza di fornire agli utenti un'informazione trasparente, con particolare riguardo ai dati raccolti, agli scopi per i quali ciò avviene e alla durata della conservazione dei dati stessi, anche ai fini dell'eventuale prestazione di un valido consenso al trattamento dei dati.
- In tale quadro, una attenzione particolare deve essere allora riservata ai rischi relativi alla qualità dei dati […] nonché ai rischi che vengano realizzati, quali un invasivo monitoraggio dei comportamenti degli utenti, anche a loro insaputa […] Al pari occorre considerare gli ulteriori rischi relativi alla sicurezza indotti, in particolare, da operazioni di comunicazione a terzi, dall'utilizzo improprio e dalla perdita delle informazioni oggetto di trattamento, soprattutto in ragione del novero dei soggetti coinvolti, dei volumi e dei tipi di dati trattati […]

Trasferimento dati verso gli USA 1/3

- Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo
- Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona
- Vista la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) secondo la quale i "Principi di approdo sicuro in materia di riservatezza" allegati alla medesima decisione, applicati in conformità agli orientamenti forniti da talune "Domande più frequenti" (FAQ) parimenti allegate, garantiscono un livello adeguato di protezione dei dati personali trasferiti dalla Comunità ad organizzazioni aventi sede negli Stati Uniti sulla base della documentazione pubblicata dal Dipartimento del commercio statunitense ivi menzionata

Trasferimento dati verso gli USA 2/3

- Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g))
- Ritenuta la necessità di adottare una misura necessaria per l'applicazione della Decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE
- Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile

Trasferimento dati verso gli USA 3/3

- Vista la FAQ n. 5 sul ruolo che le autorità di garanzia degli Stati membri dovrebbero svolgere con la cooperazione delle organizzazioni statunitensi che ricevano dati personali dall'Unione europea, anche nell'ambito di un comitato (panel) informale di autorità costituito a livello europeo cui il Garante intende partecipare
- **TUTTO CIÒ PREMESSO IL GARANTE**
- autorizza i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati sulla base e in conformità ai "Principi di approdo sicuro in materia di riservatezza", applicati in conformità alle "Domande più frequenti" (FAQ) e all'ulteriore documentazione allegata alla Decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE
- si riserva di svolgere, in conformità alla normativa comunitaria, alla legge n. 675/1996, all'art. 3 della Decisione della Commissione e all'allegata FAQ. n. 5, i necessari controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti medesimi, nonché sul rispetto dei predetti Principi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento

Safe Harbour 1/2

- NOTIFICA
  Le organizzazioni devono informare i singoli individui in merito alle finalità per cui vengono raccolte e utilizzate le informazioni su di essi, alle modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, alla tipologia dei terzi a cui vengono fornite le informazioni, e infine ad opzioni e mezzi che le organizzazioni mettono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni.
- SCELTA
  Un'organizzazione deve offrire agli individui la possibilità di scegliere (facoltà di rifiuto) se le informazioni personali che li riguardano vadano a) rivelate a terzi(2), ovvero b) utilizzate per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati dall'interessato.
- TRASFERIMENTO SUCCESSIVO
  Le organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta.
- SICUREZZA
  Le organizzazioni che detengono, aggiornano, utilizzano o diffondono informazioni personali devono prendere ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati.

Safe Harbour 2/2

- INTEGRITÀ DEI DATI
  un'organizzazione deve prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati.
- ACCESSO
  Gli individui devono poter accedere alle informazioni personali che li riguardano in possesso di una data organizzazione, ed altresì poterle correggere, emendare o cancellare se ed in quanto esse risultino inesatte, salvo il caso specifico in cui l'onere o la spesa che tale accesso comporta siano sproporzionati ai rischi per la riservatezza degli interessati oppure vengano violati i diritti di persone che non siano i diretti interessati.
- GARANZIE D'APPLICAZIONE
  Per tutelare efficacemente la riservatezza dei dati personali occorre disporre meccanismi volti a garantire il rispetto dei principi, la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi.

Federal Trade Commission report 2015

- Nel mondo ci sono oltre 25 miliardi di device connessi e il loro numero è destinato a salire poiché le società che producono beni di consumo, i produttori di auto, i fornitori di sevizi sanitari e altri imprenditori continuano a investire in strumenti connessi
- L'*Internet of Things* è definito come l'insieme dei device o sensori – diversi da computer, smartphone, o tablet – che connettono, conservano o trasmettono informazioni, anche tra di loro, via internet.
- Lo scopo del report FTC è limitato ai device IoT utilizzati dai consumatori: vengono perciò rivolte specifiche raccomandazioni alle compagnie che sviluppano questi prodotti
- Considerato che alcuni device potrebbero essere privi di interfaccia utente, la FTC raccomanda che i produttori notifichino correttamente ai consumatori la raccolta dei dati, offrendo loro la possibilità di decidere quale uso potrà esserne fatto
- Le aziende vengono invitate a raccogliere i dati secondo il principio di necessità, limitandosi ai dati richiesti per il funzionamento dei device e tenendo in debita considerazione la possibilità di de-identificare I dati raccolti

FTC recommendations

- Inserire le istanze di security già in fase di progettazione, piuttosto che intervenendo in un secondo momento
- aggiornare adeguatamente gli impiegati riguardo l'importanza della sicurezza e assicurare la gestione di questi rischi a un livello aziendale appropriato
- Assicurarsi che i provider esterni offrano un livello di sicurezza adeguato, protraendo il controllo nel tempo con opportune verifiche
- Nel momento in cui si identifica un rischio specifico, adottare una strategia a castello in cui vengano posti in essere livelli multipli di sicurezza
- Attuare misure di sicurezza volte a prevenire l'accesso di terzi no autorizzati ai device, ai dati, o alle informazioni personali dei consumatori che sono conservate sul network
- Monitorare i device connessi per tutto la durata prevista del loro ciclo vitale e, quando possibile, mettere a disposizione le patch di copertura dei rischi previsti
- Utilizzare algoritmi di crittografia forti e un sistema di autenticazione adeguato

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
- Casi pratici
  - V Tech
  - Hallo Barbie
- Q&A
- Bibliografia & sitografia

High Court irlandese 1/2

- 34 Tuttavia, la High Court considera che tale causa verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell'Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli articoli 7 e 8 della Carta sia dai principi enunciati dalla Corte nella sentenza Digital Rights Ireland e a. (C‑293/12 e C‑594/12, EU:C:2014:238). Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.
-

High Court irlandese 2/2

- 35 La High Court osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale. Pertanto, anche se il sig. Schrems non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all'articolo 25, paragrafo 6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d'America garantiscono un livello di protezione adeguato, oppure se l'articolo 8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.
-
- 36 È in tale contesto che la High Court ha deciso di sospendere il procedimento e di sottoporre alla Corte la questione pregiudiziale

Corte di Giustizia: Motivi della decisone 1/3

- in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.
- la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

Corte di Giustizia: Motivi della decisone 1/3

- Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti

- Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

Corte di Giustizia: Motivi della decisone 1/3

- le autorità americane potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione.
- Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale. […] A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura.

Dispositivo

- Per questi motivi, la Corte (Grande Sezione) dichiara:
- 1) L'articolo 25, paragrafo 6, della direttiva 95/46/CE […] deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE […]con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.
- 2) La decisione 2000/520 è invalida.

Export.gov

U.S.-EU & U.S.-Swiss Safe Harbor Frameworks

Advisory

- On October 6, 2015, the European Court of Justice issued a judgment declaring as “invalid” the European Commission’s Decision 2000/520/EC of 26 July 2000 “on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce”
- In the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework. If you have questions, please contact the European Commission, the appropriate European national data protection authority, or legal counsel

Il garante italiano

- **Trasferimento dati in USA: decaduta l'autorizzazione "Approdo sicuro".**
  Le imprese dovranno mettere in campo altri strumenti per tutelare i dati delle persone
- Il Garante per la privacy ha dichiarato decaduta l'autorizzazione emanata a suo tempo con la quale si consentivano i trasferimenti di dati verso gli Stati Uniti sulla base del cosiddetto accordo "Safe Harbor". Per poter trasferire dati oltreoceano, società multinazionali, organizzazioni e imprese italiane dovranno di conseguenza ricorrere alle altre possibilità previste dalla normativa sulla protezione dei dati personali. Il provvedimento (pubblicato sulla Gazzetta ufficiale) è stato adottato dal Garante a seguito della recente sentenza della Corte di Giustizia dell'Unione Europea, che ha dichiarato invalido il regime introdotto in virtù dell'accordo "Approdo sicuro" (Safe Harbor), facendo venire meno il presupposto di legittimità per il trasferimento negli Usa di dati personali dei cittadini europei per chi utilizzava questo strumento. La decisione presa dal Garante è in linea con quanto concordato nelle settimane scorse nell'ambito del Gruppo che riunisce le Autorità della privacy dell'Ue.
- In attesa delle prossime decisioni che verranno assunte in sede europea, le imprese potranno dunque trasferire lecitamente i dati delle persone solo avvalendosi di strumenti quali, ad esempio, le clausole contrattuali standard o le regole di condotta adottate all'interno di un medesimo gruppo (le cosiddette BCR, Binding Corporate Rules). L'Autorità si è comunque riservata di effettuare controlli per verificare la liceità e la correttezza del trasferimento dei dati da parte di chi esporta i dati. *(6 nov. 2015)*

Intervista a Giovanni Buttarelli, Garante Europeo della Protezione dei Dati

- "Dal 6 ottobre scorso, circa 4.500 imprese hanno serie difficoltà nel loro ordinario business con gli Usa: non possono più esportare oltreoceano i dati relativi ad utenti, consumatori, abbonati, dipendenti e clienti qualora utilizzino il cosiddetto Safe Harbour, un controverso accordo tradotto in una decisione della Commissione europea del 2000. La ragione? La privacy e i diritti di tutti questi soggetti, che è risultata non adeguatamente tutelata al punto che la Corte di giustizia europea ha annullato la decisione adottata 15 anni or sono, con effetto retroattivo. È dai tempi delle prime rivelazioni di Snowden che la protezione dei dati non aveva un'evidenza così ampia sui media e sul piano politico nell'intero pianeta, considerato anche l'effetto domino che la sentenza può avere su altri accordi internazionali"
- "Cosa accadrà, adesso? Occorre distinguere tra breve e medio periodo. Per poche settimane e forse qualche mese, le imprese interessate dovranno utilizzare altri strumenti come il libero consenso informato, clausole contrattuali-tipo oppure regole vincolanti in un gruppo di imprese. Le autorità garanti della privacy si coordineranno nel procedere a investigazioni, nell'esaminare reclami e nell'adottare eventuali misure interdittive o sanzionatorie, confidando nel fatto che una risposta di più lungo possa arrivare sul piano politico, con una nuova soluzione negoziata che soddisfi i severi parametri affermati dalla nostra 'Corte costituzionale' europea. Ma non sarà facile"

Intervista a Andrus Ansip, vicepresidente della Commissione Ue e coordinatore per il mercato unico digitale

- E' necessario dare in fretta una adeguata protezione ai cittadini europei
- Una buona maggioranza di persone, qui a Bruxelles, sapeva che il Safe Harbor non era sicuro
- Dopo le rivelazioni sulla sorveglianza massiccia effettuata dalle autorità americane, è apparso proprio evidente, ed è per questo che la Commissione aveva già chiesto agli americani di modificare l'intesa
- Ora dobbiamo lavorare insieme con gli americani per trovare una soluzione sicura. Ora dobbiamo lavorare insieme con gli americani per trovare una soluzione sicura. Lo stesso Obama ha avviato la riforma dei Servizi lo scorso anno
- Non credo che i colossi ne soffriranno hanno avuto tutto il tempo per predisporre delle contromosse

Gli stakeholders

- EFF: i governi nazionali fanno a gara per tenere i dati fuori dalla disponibilità delle altre nations vie to keep data out of the hands of other countries, while seeking to keep it trackable by their own intelligence services.
- Già nel 2014, Google e Facebook avevano chiesto ai rappresentanti del congresso un intervento sui poteri della NSA che tenesse le aziende americane a riparo dai danni provocati dal datagate
- Il risultato più temuto è quello di un frazionamento di Internet, in cui ogni governo legiferi in maniera autonoma imponendo la localizzazione dei datacenter entro i confini nazionali
- Questo esito, antitetico rispetto alla struttura aperta della rete, produrrebbe un serio danno economico sia alle start-up, di dimensioni troppo ridotte per affrontare i costi della gestione locale, sia alle aziende che offrono il servizio a terzi
- Secondo i rappresentanti di Google e Facebook , la mancanza di fiducia nelle regole dell'ordinamento statunitense potrebbe causare un danno all'industria *tech* di oltre 180 miliardi si dollari entro la fine del 2016

Trasferimento dati verso paesi terzi

http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi

- Il trasferimento di dati personali da paesi appartenenti all'UE verso Paesi "terzi" (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio (articolo 25, comma 1, della **Direttiva 95/46/CE**), a meno che il Paese in questione garantisca un livello di protezione "adeguato"; la Commissione ha il potere di stabilire tale adeguatezza attraverso una specifica **decisione** (articolo 25, comma 6, della Direttiva 95/46/CE).
- In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei **casi menzionati dall'articolo 26**, **comma 1,** della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di **strumenti contrattuali** che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46).

Decisioni di adeguatezza

- La Commissione europea può stabilire, sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del **Gruppo ex Articolo 29** della **Direttiva 95/46/CE**, che il livello di protezione offerto in un determinato Paese è adeguato (articolo 25, comma 6, della dDrettiva 95/46/CE), e che pertanto è possibile trasferirvi dati personali. Di seguito sono riportate le decisioni della Commissione sinora pubblicate in materia di adeguatezza di Paesi terzi.

- **Decisioni di adeguatezza**
- **Andorra**, **Argentina**, **Australia – PNR**, **Canada**, **Faer Oer**, **Guernsey**, **Isola di Man**, **Israele**, **Jersey**, **Nuova Zelanda**, **Svizzera**, **Uruguay**, **USA – Safe Harbor** *(vedi Provvedimento del 22 ottobre 2015 e comunicato stampa del 6 novembre 2015),* **USA – PNR**

clausole contrattuali

- La Commissione europea, ai sensi dell'articolo 26(4) della **Direttiva 95/46/CE**, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi. Si tratta di una delle deroghe (stabilite nel comma 2 dell'articolo 26 della Direttiva 95/46/CE) al divieto di effettuare il trasferimento verso Paesi che non offrono garanzie "adeguate" ai sensi della Direttiva 95/46/CE.
- In pratica, incorporando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione. Sinora la Commissione ha adottato quattro decisioni in materia.
- **Decisioni**
- **- Decisione Commissione, clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95-46-CE** **(***5 febbraio 2010)*
- **- Decisione della Commissione del 27 dicembre 2004 per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi** **(***27 dicembre 2004)*
- **- Decisione Commissione, clausole contrattuali tipo per trasferimento dati a carattere personale verso paesi terzi a norma dir. 95-46-CE** **(***5 giugno 2001)*
- **- Decisione Commissione, clausole contrattuali tipo per trasferimento dati personali a incaricati del trattamento residenti in paesi terzi, dir. 95-46-CE** **(***27 dicembre 2001)*

BCR – binding corporate rules

- Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo d'impresa. Si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*).
- Le Bcr costituiscono un meccanismo in grado di **semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personal**i. Il rilascio di un'autorizzazione al trasferimento di dati personali tramite Bcr consente alle filiali della multinazionale che ne abbia fatto richiesta, anche se stabilite in diversi Paesi, di trasferire, all'interno del gruppo d'impresa, i dati personali oggetto delle Bcr, senza ulteriori adempimenti (quali ad esempio la sottoscrizione di Clausole contrattuali tipo, l'adesione all'*accordo Safe Harbour*, il rilascio di specifiche autorizzazioni ai sensi del **Codice**).
- Le Bcr traggono efficacia dalla concessione di una autorizzazione del Garante al trasferimento dei dati personali verso Paesi terzi (articolo 44, lettera a), del **decreto legislativo 196/2003** – " Codice"). L'autorizzazione è rilasciata dietro espressa richiesta della società interessata, con riferimento a trasferimenti di dati personali dall'Italia verso Paesi terzi che si svolgano nel rispetto di quanto stabilito all'interno del testo di Bcr e per le sole finalità ivi indicate.
- Il testo di Bcr contiene i principi fondamentali in materia di protezione dei dati personali sanciti dal Codice e dalla **Direttiva 95/46/CE**, secondo lo schema elaborato dal **Gruppo "Articolo 29"** dei Garanti Europei (*cfr.* il **WP 74** e il **WP 153).**

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
- Casi pratici
  - V Tech
  - Hallo Barbie
- Q&A
- Bibliografia & sitografia

Hello Barbie

- La versione interattiva della bambola Mattel® fa domande ai bambini, registra le loro risposte e le invia a un server remoto dove vengono analizzate e conservate
- Il tentativo è quello di instaurare una forma di dialogo basato sulle preferenze dei piccoli utenti, selezionando le risposte della bambola da un archivio di frasi preimpostate
- Il funzionamento del giocattolo dipende dall'attivazione di uno specifico account
- Mattel e la consociata Toy Talk affermano che si tratta di un server sicuro
- Nel giugno 2015 sono stati rubati i dati di 21.5 milioni di persone dall'ufficio del personale federale USA: i dati non erano stati criptati…

V-tech

- Nel novembre 2015 in un attacco hacker al server di Vtech, un produttore di giocattoli interattivi di Hong Kong sono stati rubati i dati di quasi 5 milioni di account, 200 mila dei quali intestati a minori
- La società non si è accorta di niente fino a quando l'hacker ha offerto lo scoop al magazine motherboard che ha contattato la Vtech per verificare la storia
- il database conteneva nomi, indirizzi e dati riguardo la parentela degli acquirenti che consentirebbero di collegare i piccoli utenti alle loro famiglie
- L'hacker dichiara di aver agito a scopo dimostrativo e che nessuno dei dati raccolti sarebbe stato reimpiegato
- I vertici di Vtech rassicurano comunque che i dati delle carte di credito non sarebbero stati toccati…

Agenda

- Presentazione relatore
- Trasferimento dati all'estero e previsioni di *safe harbour*
- La sentenza della Corte di Giustizia UE 6 ottobre 2015
  - Casi pratici
  - V Tech
- Hallo Barbie
- Q&A
- Bibliografia & sitografia

Siti web 1/2

- http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117it.pdf
- http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000D0520&from=IT
- http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids
- http://thehill.com/policy/technology/220176-google-head-without-reform-nsa-will-break-the-internet
- http://www.export.gov/safeharbor/
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/30939
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3898704
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3889962
- http://www.interlex.it/testi/00_520ce.htm

Siti web 2/2

- http://www.lastampa.it/2015/10/09/tecnologia/ansip-lavoriamo-a-un-nuovo-safe-harbor-che-protegga-i-cittadini-europei-9MgFXD2IrtuasRmWGlsq1H/pagina.html
- http://www.primaonline.it/2015/10/28/217645/giovanni-buttarelli-garante-europeo-per-la-protezione-dei-dati-sulla-corte-di-giustizia-ue-che-annulla-il-safe-harbour-difficolta-per-le-imprese-ma-decisione-giusta-perche-protegge-la-nostra-priv/
- https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance
- https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices
- https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf
- https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
- https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Contatti

- Maria Letizia Perugini
  maria.perugini@unibo.it

Grazie...