CNR - Roma, 9 novembre 2016

# Data Privacy e cybersicurezza. Quali sviluppi

**Prof. Maurizio Mensi**

**SNA e Luiss Guido Carli**

# LE PRINCIPALI QUESTIONI

- **Privacy e cybersicurezza: temi strettamente collegati**
- **Il tema delle regole e la loro adeguatezza - I dati come valore**
- **La *distruptive innovation* e le nuove frontiere: IoT, intelligenza artificiale, dati biometrici**
- **Un cantiere normativo aperto (UE, COE)**
- **Lo scambio trasfrontaliero dei dati (rapporti USA –EU – Il Privacy Shield)**

# L'USO DEI DATI

- Le informazioni trasmesse (i ***metadati,*** gli elementi estrinseci delle comunicazioni effettuate e/o ricevute, esclusi i contenuti), contengono informazioni personali sugli individui, la loro posizione e attività *on-line*.
- Tali dati sono memorizzabili, talora accessibili e consultabili. Il loro l'utilizzo è **in gran parte non regolamentato** e la loro analisi può essere altamente invasiva, in particolare quando i dati vengono combinati e aggregati.

# DALLA PRIVACY ALLA PROTEZIONE DEI DATI

Occorre perseguire un **equilibrio tra la tutela della sicurezza e il rispetto della *privacy*.**

- Le innovazioni tecnologiche si sono sviluppate parallelamente ad un evoluzione dell'approccio verso la sorveglianza delle comunicazioni.
- **La prima teorizzazione del diritto alla privacy** risale al 1890, Samuel Warren e Louis Brandeis, "diritto ad essere lasciati soli" ("*right to be let alone*"), in applicazione del concetto privatistico di proprietà e del relativo sistema di tutela alla sfera privata della vita.
- **1975, Corte di Cassazione,** diritto dei singoli alla riservatezza, o alla "***tutela dell'intimità privata***" rispetto a quelle circostanze e vicende intrinsecamente personali e familiari che non abbiano per i terzi un interesse "socialmente apprezzabile".

# *PRIVACY* COME DIRITTO UMANO FONDAMENTALE

## ➢ Livello internazionale

- Dichiarazione universale dei diritti dell'uomo del 1948 (art. 12)
- Patto internazionale sui diritti civili e politici del 1966 (art. 17)
- Convenzione sui diritti del fanciullo del 1989 (art. 16)
- Convenzione internazionale sulla protezione di tutti i lavoratori migranti e dei membri delle loro famiglie - 1990 (art. 14)

## ➢ Livello «regionale»

- Convenzione europea dei diritti dell'uomo del 1950 (art. 8)
- Convenzione americana sui diritti umani del 1969 (art. 11).

# LE REGOLE - UNIONE EUROPEA E COE

## Le regole

- ***DATA PRIVACY***

- **Direttiva 95/46/CE - Direttiva 2002/58 *e-privacy***
- **Il *Privacy Package* del 27 aprile 2016** (Regolamento e Direttiva)
- **La revisione della Convenzione COE n. 108/1981**

- ***CYBERSECURITY***

- **Convenzione del Consiglio d'Europa sul *Cybercrime*** (Budapest, 23 novembre 2001)
- **La Direttiva 2008/114/CE –** *Network* fisico (energia e trasporti)
- **La Direttiva 2013/40/UE –** Attacchi contro i sistemi di informazione – Standard minimi per la definizione dei reati
- **La Direttiva NIS 1148/2016– *Network and Information Security*-** Settore pubblico e privato - 5 elementi: nuova strategia nazionale – rete di cooperazione - requisiti di sicurezza – standards – *enforcement*

# IL PACCHETTO PRIVACY UE

Il 27 aprile 2016 sono stati approvati, dopo un percorso legislativo di oltre quattro anni, il c.d. "**pacchetto protezione dati**", che si compone di due diversi elementi:

- 1) il **Regolamento 2016/679, concernente la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati"**, volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE ("Direttiva 95/46") che ha portato in Italia, all'adozione del vigente D.lgs. 30 giugno 2003 n. 196 ("Codice Privacy");
- 2) la **Direttiva 2016/68, relativa alla "regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali"**, che sostituisce la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia.

# LA TEMPISTICA PER L'ENTRATA IN VIGORE

La pubblicazione del nuovo Regolamento sulla Gazzetta UE è avvenuta in data **4 maggio 2016.**

A partire dal ventesimo giorno dalla pubblicazione (24 maggio p.v.), gli Stati membri hanno **due anni di tempo** per allineare la normativa nazionale alle nuove prescrizioni del Regolamento, che diventerà definitivamente applicabile in tutto il territorio UE a partire dal **25 maggio 2018.**

Per quanto riguarda la Direttiva, gli Stati membri hanno due anni per recepirla all'interno dell'ordinamento nazionale.

# GLI OBIETTIVI

Il nuovo "pacchetto protezione dati" mira a:

1. **adeguare la *Data Protection*** rispetto all'evoluzione tecnologica che ha determinato un aumento dei flussi transfrontalieri e, quindi, dei dati scambiati tra attori pubblici e privati, rendendo così necessari una più libera circolazione di dati all'interno dell'UE oltre ad un più elevato livello di protezione;
2. **eliminare la frammentazione applicativa** della normativa in materia di protezione dei dati personali nel territorio dell'UE, dovuta alle diverse leggi di recepimento della Direttiva 95/46.

# LE PRINCIPALI INNOVAZIONI

- In base al nuovo regolamento, è previsto **un unico corpus normativo** in tema di protezione dei dati in tutta l'UE e **una sola autorità per la protezione dei dati** responsabile (secondo il modello "***one-stop-shop***") per una società che opera in diversi paesi: quella dello Stato membro in cui la società ha la propria sede principale.
- L'estensione del **campo di applicazione territoriale**. Le norme Ue si applicano anche ai dati personali trattati all'estero da imprese che sono attive sul mercato unico e offrono servizi ai cittadini dell'Unione.
- Facilitazione dei **trasferimenti internazionali di dati**. In linea di principio, qualsiasi trasferimento di dati deve essere oggetto di una **decisione della Commissione** che attesta che il Paese in questione assicura un "**livello di protezione adeguato**".

- **I diritti delle persone risultano rafforzati**. Il regolamento fornisce agli individui un maggior controllo sui propri dati personali attraverso disposizioni che si rivolgono specificamente ai *social network*.
- **Il consenso degli individui al trattamento dei propri dati personali deve essere "esplicito"** , vale a dire deve essere manifestato da un'azione affermativa o da una dichiarazione, oltre che "libero, specifico e informato", e revocabile in qualsiasi momento.
- L'introduzione del cd. **diritto all'oblio** (per la prima volta codificato in diritto positivo dopo la sentenza Google Spain) consente di gestire meglio i rischi connessi alla protezione dei dati online: chiunque potrà richiedere al motore di ricerca la cancellazione dei propri dati se non sussistono motivi legittimi perché siano mantenuti.
- Un nuovo **diritto alla portabilità dei dati:** è agevolato il trasferimento dei dati da un fornitore di servizi a un altro, con un miglioramento della concorrenza tra servizi.

# NUOVE ONERI E RESPONSABILITÀ

- **La nomina di un responsabile della protezione** dei dati per le aziende con oltre 250 dipendenti, la valutazione dei rischi di protezione dei dati.
- L'introduzione dei principi di "***privacy by default***" **e** "***privacy by design***" (misure da prevedere nei prodotti e servizi fin dalle loro fasi di sviluppo) per garantire che gli individui siano informati in modo facilmente comprensibile su come saranno trattati i loro dati.
- Un obbligo generale di **notifica della violazione di dati**: in caso di perdita, furto o *hacking* di dati personali imprese e organizzazioni sono tenute a comunicare tale circostanza quanto prima, possibilmente entro 24 ore, alle autorità nazionali di controllo.

# LO SCAMBIO TRANSFRONTALIERO DI DATI

- **Il *Safe Harbour* del 2000** - La Comunicazione CE 27/11/2013- Le Linee Guida CE 6/11/2015
- **La sentenza *Schrems* (CGUE) – ottobre 2015**
- Lo scambio transfrontaliero di dati – **Art. 25 Dir. 95/46/CE**
- Scambi commerciali e *signal intelligence activities*

# IL PRIVACY SHIELD – L'ACCORDO

**- Accordo politico - 2 febbraio 2016**

**- Decisione di adeguatezza - 12 luglio 2016**

Due anni di negoziato fra Commissione europea e Dipartimento di Commercio USA.

**Nota del 23/2/2016 del Segr. Commercio USA Penny Pritzker al Comm. UE Véra Jurovà.**

**- 2 allegati** (ITA – *International Trade Administration* del Dipartimento del Commercio – Impegni del Dipartimento del Commercio circa il nuovo modello arbitrale).

**- 5 lettere** (sull'attuazione dell'accordo da parte di *Federal Trade Commission*, Dipartimento dei Trasporti, Ufficio del Direttore della *National Intelligence* ODNI, Dipartimento di Stato con allegato il Memorandum sull'*Ombudsperson*, Dipartimento di Giustizia).

**Comunicazione CE 29 febbraio 2016.**

# IL PRIVACY SHIELD – LA GENESI

**Genesi dell'accordo**

Il ruolo dello scambio di dati fra USA e UE

→ **Art. 25 Dir. 95/46/CE**

**Decisione *Safe Harbour* 2000/520** (ex Art. 25, par. 6): USA garantiscono un «adeguato livello di protezione».

**La Comunicazione CE del 27/11/2013** – evidenziati diversi aspetti critici – necessità di revisione.

**13 raccomandazioni** (assicurare il rispetto delle regole in tema di *privacy* e la trasparenza del sistema di autocertificazione delle imprese USA, migliore sistema di controllo e supervisione, introdurre un sistema di soluzione delle controversie in seguito a reclami individuali, esercizio dei poteri di intervento da parte dei servizi di intelligence e limitazione della *privacy* (eccezione prevista dal *Safe Harbour* del 2000) secondo criteri di necessità e proporzionalità.

# LA *CYBER-SECURITY* E L'UNIONE EUROPEA

Due obiettivi specifici in materia, in linea anche con le raccomandazioni contenute nella Strategia di sicurezza interna dell'**UE** e dell'**Agenda Digitale Europea** dell'agosto 2010:

(i) accrescere la **consapevolezza dei principali rischi** connessi alla *cybersecurity*;

(ii) migliorare la **preparazione e le capacità di risposta** europee e nazionali a **possibili attacchi o incidenti informatici**.

**Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (ENISA)**

# STANDARD NORMATIVI PER LE MISURE DI SORVEGLIANZA

- Le norme in materia debbono **garantire che le misure di sorveglianza delle comunicazioni**:

a) siano stabilite dalla legge, con un livello di **chiarezza e precisione** tale da assicurare che gli individui ne abbiano contezza e possano prevederne applicazione;

b) siano strettamente e manifestamente **necessarie per raggiungere uno scopo legittimo** e

c) rispettino il **principio di proporzionalità**, e non vengano impiegati quando vi siano misure meno invasive disponibili e non siano ancora state utilizzate.

# LE REGOLE - UNIONE EUROPEA

## Gli attori

- **ENISA**, istituito nel 2005 (Reg. 460/2004)
- **EC3 - Centro europeo per la lotta alla criminalità informatica** (Europol)
- **Emergency Response Team** per le istituzioni EU (11 settembre 2012)

**Direttiva 2008/114/EC dell'8 dicembre,**
**Settori dell'energia e dei trasporti**. Non pone alcun obbligo agli operatori di segnalare danni ai sistemi di sicurezza o di cooperare fra loro

## "Infrastruttura Critica Europea"

un'infrastruttura il cui danneggiamento o distruzione comporti un impatti su almeno due Stati membri. Individua poi i criteri e stabilisce le procedure per l'individuazione delle **infrastrutture critiche** nei settori in questione e delinea un primo livello generale per la preparazione dei relativi piani di sicurezza a cura dei proprietari/operatori di tali *asset* fisici.

- **decreto legislativo n. 61/2011** e **legge n. 33/2012**

# LA DIRETTIVA UE RELATIVA AGLI ATTACCHI CONTRO I SISTEMI DI INFORMAZIONE

- La **direttiva 2013/40 del 12 agosto 2013** relativa agli attacchi contro i sistemi di informazione.
- **Obiettivi**: armonizzazione del diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione attraverso la definizione di **standard minimi** circa la definizione dei reati e delle relative sanzioni e miglioramento della cooperazione tra le autorità competenti, comprese le forze di polizia e gli altri servizi incaricati dell'applicazione della legge, nonché le competenti agenzie dell'Unione e gli organismi specializzati, come *Eurojust*, *Europol* e l'*European Network and Information Security Agency* (ENISA).

➢**Febbraio 2013**: la **Commissione europea** ha pubblicato una

- strategia sulla sicurezza informatica contestualmente a
- proposta di direttiva in materia di sicurezza delle reti e dell'informazione: "***Uno spazio informatico aperto e sicuro***".

## Direttiva *Network and Information Security* (NIS) 1148/2016 – 6 luglio 2016

un passaggio cruciale per la costruzione di un sistema di sicurezza europeo, sebbene costituisca l'esito di un compromesso che lascia irrisolti alcuni aspetti significativi.

# DIRETTIVA NIS 1148/2016
## Punto di arrivo e di partenza

Riconoscimento di un insufficiente livello di protezione.

Rischio per il mercato interno (vedi doc su *Impact Assessment*) – sistemi interconnessi –incidenti superano confini nazionali – interventi regolamentari degli SM non coordinati dannosi – alcuni settori chiave a supporto del mercato interno:

- **banche**
- **borse valori**
- **energia (generazione, trasmissione e distribuzione**
- **trasporti**
- **salute**

Necessità di scambiare e condividere informazioni sugli incidenti.

# 3 OBIETTIVI

1. stabilire un livello minimo comune di NIS negli Stati membri
2. migliorare la cooperazione
3. creare una cultura della gestione del rischio e migliorare lo scambio di informazioni fra pubblico e privato.

Approccio regolamentare.

Fiducia reciproca – ambiente on-line

***I Data controllers*** (banche, ospedali) sono costretti a porre in essere misure di sicurezza proporzionate al livello di rischio che fronteggiano, ma sono tenuti a notificare le violazioni di sicurezza soltanto nel caso in cui siano compromessi dati personali.

# L'APPLICAZIONE DELLA DIRETTIVA

- Dal momento dell'entrata in vigore, i singoli Stati hanno **21 mesi** per l'adozione delle norme di trasposizione e la creazione delle **authorities** (o la revisione di quelle già operanti).
- A questi si aggiungono ulteriori **sei mesi** per il censimento degli **operatori dei servizi essenziali.** Si tratta di un lasso di tempo notevole, perché le minacce cyber evolvono molto rapidamente.
- La sua adozione è stata velocizzata dagli attacchi terroristici in Francia e Belgio e dalla dimensione del cybercrime.
- Gartner ha stimato in 86MLD di dollari per il 2016 i costi per privati e Pa per difendersi da cyber attacchi.
- Nel mondo i più colpiti sono *intelligence*, comunicazioni, servizi on line, educazione, finanza, sicurezza, sanità.

# LE REGOLE - ITALIA

## Il quadro di riferimento in Italia

- 2010- Relazione sulla politica di informazione per la sicurezza
- **Evoluzione normativa – La sicurezza della Repubblica (Legge n. 801/1977 - n. 124/2007 – n. 133/2012)**
- **DPCM 24 gennaio 2013** – La protezione dello spazio cibernetico italiano – Soggetti pubblici e privati – Architettura istituzionale a tre livelli: politico/strategico (**CISR**) - operativo (Nucleo per la sicurezza cibernetica - **NSC**) – gestione di crisi (Tavolo interministeriale). Il **DIS** (Dipartimento delle informazioni per la sicurezza)
- **Quadro strategico nazionale e Piano nazionale per la protezione cibernetica e la sicurezza informatica** (19 febbraio 2014) - **Il Tavolo Tecnico Cyber (TTC)**