CINDI
Centro Innovazione & Diritto

DITEDI
DISTRETTO
DELLE TECNOLOGIE
DIGITALI

Aspetti legali dell'information security: data breach e responsabilità

Avv. David D'Agostini

Udine, 30 novembre 2013

Open Source Day

CINDI
Centro Innovazione & Diritto

Centro Innovazione & Diritto

Proprietà intellettuale e industriale

Trattamento dei dati personali e privacy

Documenti informatici e firme elettroniche

Computer crimes e digital forensics

Ottobre 2013

Adobe warns 2.9 million customers of data breach after cyber-attack

Software company discloses hack and advises customers that names and encrypted credit card numbers may have been stolen

Aprile 2011

77 milioni di account violati (e altri 25 milioni a maggio '11)

25 giorni di inattività
Danni: € 120.000.000
Sanzione: £ 250.000

PLAYSTATION® Network

Gennaio 2009

Compromesse 130 milioni di carte di credito e di debito

Heartland PAYMENT SYSTEMS

The Highest Standards | The Most Trusted Transactions

Danni stimati: € 140.000.000

Fatti di cronaca

Unencrypted laptop stolen, 11,000 dialysis patients impacted

Unauthorized third party compromises payroll card company data

More than 800,000 accounts compromised in MacRumors Forums breach

Shopping cart malware compromises credit card information

Milwaukee contractor loses flash drive, compromises thousands

Two hard drives stolen from Washington State University office

Reati informatici

378.000.000 di vittime all'anno

1.035.000
al giorno

12
al secondo

Virus
Malware
Hacking
Phishing
Frauds
Thefts

Fonte: Norton report 2013

Costi diretti...

...del crimine informatico:

113.000.000.000 $
all'anno

300 $
media per vittima

Fonte: Norton report 2013

In Italia

3.000.000.000 $ all'anno

7.000.000 vittime

Media per vittima: 400,00 $

Fonte: Norton report 2013

Nei prossimi 10 anni...

...probabilità del 10% che si verifichi un grave incidente nelle infrastrutture critiche informatizzate in grado di causare danni per **250 miliardi di dollari**

WORLD ECONOMIC FORUM

Le imprese nell'UE

Soltanto il 26% delle imprese ha formalmente definito una politica di sicurezza informatica

Commissione europea

Piano di sicurezza informatica

European Commission – IP/13/94

IP/13/94

1) conseguire la resilienza informatica

2) ridurre la criminalità informatica

3) sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune

4) sviluppare le risorse industriali e tecnologiche per la sicurezza informatica

5) istituire una politica internazionale del ciberspazio

ENISA

Regolamento (CE) n. 460/2004 del Parlamento Europeo e del Consiglio 10.03.2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione

Regolamento (CE) 460/2004

Definizione di **sicurezza informatica**:
La capacità di una rete o di un sistema d'informazione di resistere a eventi imprevisti o atti illeciti o dolosi che compromettano la **disponibilità**, l'**autenticità**, l'**integrità** e la **riservatezza** dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema

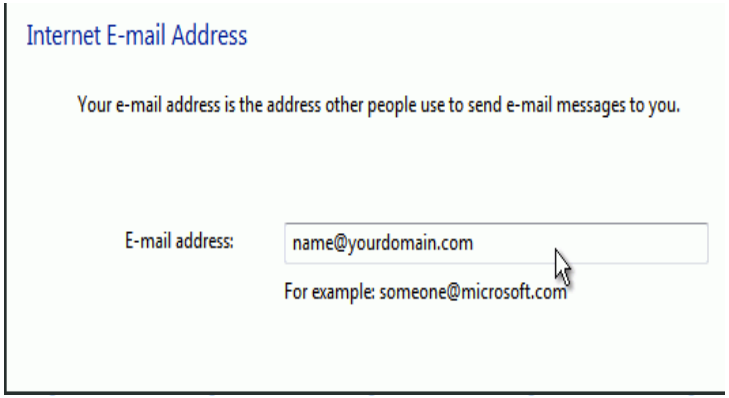
Normativa italiana

- **D.lgs. 30 giugno 2003 n. 196**

- **D.L. 6 dicembre 2011 n. 201** ("Salva Italia" convertito con L. 22 dicembre 2011 n. 214)

- **D.L. 9 febbraio 2012 n. 5** ("Semplificazioni" convertito con L. 4 aprile 2012 n. 35)

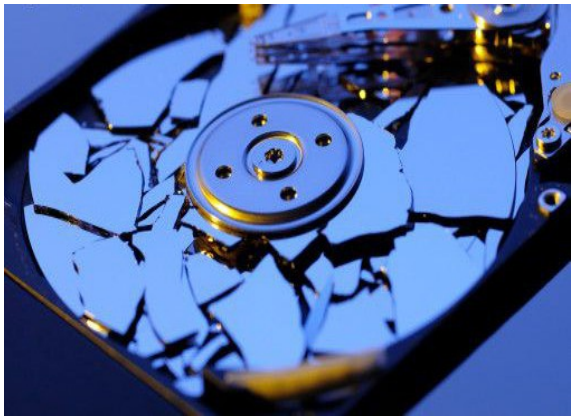
Dati personali?



C'era una volta il D.P.S.

CINDI
Centro Innovazione & Diritto

...e la sicurezza?



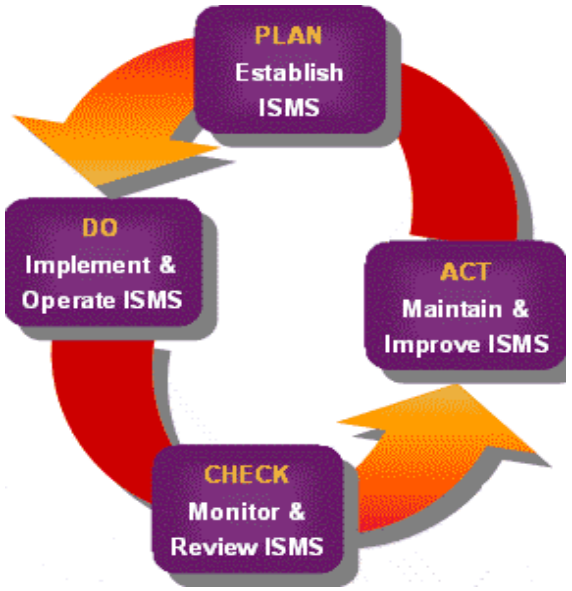
Art. 31 codice privacy

I dati personali sono **custoditi** e **controllati**, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di **idonee e preventive misure di sicurezza**, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Quali misure idonee?

Es. Standard internazionali:
ISO/IEC 27.000

Definizione e attuazione di un **Information Security Management System** (ISMS)



Art. 15 codice privacy

Chi cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al **risarcimento** se non prova di avere adottato **tutte le misure idonee** a evitare il danno.

Risarcibilità anche del **danno non patrimoniale!!!**

La giurisprudenza

Sentenza 9 giugno 2011 Tribunale di Palermo

Prelievo illecito da conto corrente

"*...avrebbe dovuto adottare tutte le misure di sicurezza, tecnicamente idonee e conosciute in base al progresso tecnico, a prevenire danni non essendo sufficiente la non violazione di norme di legge.*"

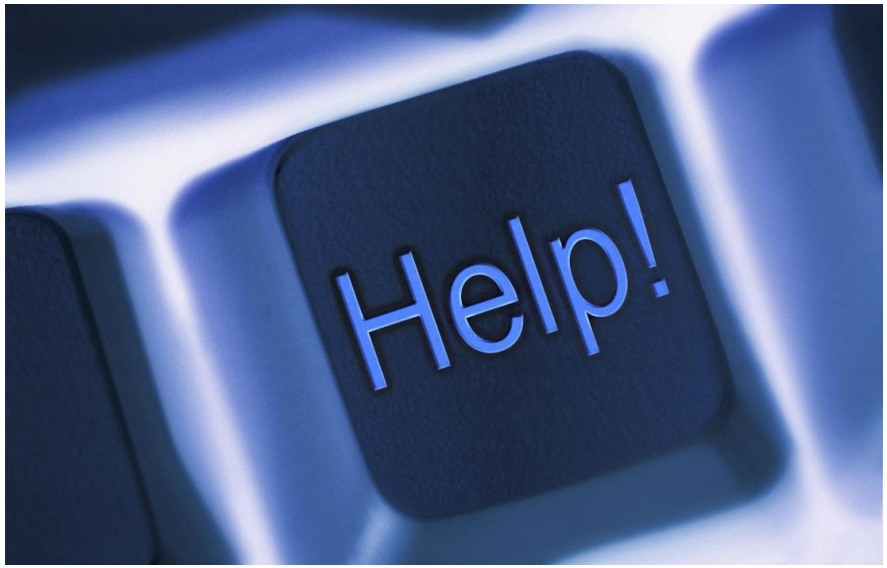
D.lgs. 28 maggio 2012, n. 69

Definizione di data breach:

violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali

In caso di data breach

Cosa è obbligatorio fare per legge?



Violazione alla sicurezza informatica

Warning

Il d.lgs. 69/12 riguarda i soli *"fornitori di servizi di comunicazione elettronica accessibili al pubblico"*

Obblighi preventivi

- adottare misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei servizi
- informare contraenti e utenti se sussiste un particolare rischio di violazione della sicurezza

Al momento del data breach

- comunicazione della violazione al Garante privacy senza indebiti ritardi (entro 24 ore)
- comunicazione anche al contraente e a terzi se la violazione rischia di arrecare pregiudizio ai dati personali o alla riservatezza

Provvedimento 4 aprile 2013

- i dati identificativi del titolare del trattamento
- la sintetica descrizione del data breach
- l'indicazione della data e del luogo della violazione
- la sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti

Entro 3 giorni

- il tipo di violazione
- il dispositivo oggetto della violazione
- il numero di persone colpite dal data breach
- la tipologia di dati coinvolti
- le misure tecniche e organizzative adottate dal titolare del trattamento

Adempimenti successivi

Inventario delle violazioni:

- **circostanze in cui si sono verificate**
- **conseguenze**
- **provvedimenti adottati per porvi rimedio**

Sanzioni amministrative

Omessa o ritardata comunicazione al Garante: da € 25.000 a 150.000

Omessa o ritardata comunicazione al contraente o a terzi: da € 150 a 100 per ciascuna persona

Omessa o irregolare tenuta dell'inventario: da € 20.000 a 120.000

Warning

Il d.lgs. 69/12 riguarda i soli *"fornitori di servizi di comunicazione elettronica accessibili al pubblico"*

COM(2012) 11

Bozza del nuovo regolamento europeo sulla privacy estende tali obblighi a tutti i titolari!!!

- **Notifica/comunicazione del data breach**
- **Valutazione d'impatto**

Ruolo del privacy officer

Nel futuro

Cambiamento di mentalità

'We're going to need a bigger rug or we're sunk.'

Contatti

www.avvocatidagostini.it

www.cindi.it

studio@avvocatidagostini.it

info@cindi.it

@daviddagostini

Via Vittorio Veneto 32

Udine