SICUREZZA INFORMATICA. ASPETTI LEGALI

L'evoluzione normativa

Sassari 25.10.2019

1

Primi passi

Le prime norme che si interessano di sicurezza informatica risalgono al 1989 (DPCM 15.2.1989 che impone misure di sicurezza ai CED tenuti al segreto d'ufficio).

La legge 675/1996 (Legge sulla privacy) introduce la «*Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno*». Il regolamento di attuazione (DPR 318/1999) prevede le misure minime per il trattamento di dati mediante sistemi automatizzati:

- "**misure minime**", complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto (identificazione utente, autorizzazione all´accesso alle funzioni, ai servizi, ai locali, ai dati, registrazione ingressi e limiti al riutilizzo di supporti di archiviazione);
- "**strumenti**", i mezzi elettronici o automatizzati con cui si effettua il trattamento;
- "**amministratori di sistema**", soggetti che hanno il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne la utilizzazione.

2

Codice Privacy (D.Lgs. 196/2003)

MISURE MINIME DI SICUREZZA – Art. 34 ***(Trattamenti con strumenti elettronici)***

«1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.»

3

GDPR – Regolamento UE 2016/679

Accountability (Articoli 5, comma 2, e 24 GDPR) = responsabilizzazione

- il Titolare del trattamento è tenuto a strutturare e organizzare un modello di gestione dati conforme al GDPR, che rispetti ed assicuri la corretta applicazione del Regolamento, nonché a fornire prova di questa conformità.
- L'identificazione delle misure di sicurezza adeguate rispetto al tipo di dati raccolti ed all'attività svolta avviene sulla base di diversi criteri, in coerenza con il principio di *protection by default*, che prevede la raccolta dei soli dati necessari, e con la valutazione del rischio.

4

Protection by default

- **Minimizzare la quantità di dati raccolti**, optando per quelli che rendano meno immediata l'identificazione dell'interessato
- **Minimizzare l'utilizzo e l'estensione del trattamento in base alle finalità specifiche**, ad esempio evitando la conservazione dei dati quando non necessaria
- **Minimizzare la durata del periodo di conservazione**
- **Minimizzare l'accesso ai dati personali**, sia dal punto di vista di dove questi sono conservati, sia rispetto ai diritti di accesso in capo a terzi.

5

Protection by design

- **prevenire non correggere**: agire prima che si sviluppino i problemi;
- **privacy come impostazione di default**: nel caso in cui siano richieste informazioni personali deve sussistere uno scopo o un motivo per raccoglierle;
- **privacy incorporata nella progettazione**;
- **massima funzionalità:** su una serie di obiettivi non ne prevale uno solo, ma tutti insieme concorrono alla realizzazione degli obiettivi;
- **sicurezza fino alla fine**: solo con la sicurezza è possibile assicurare la gestione delle informazioni in maniera corretta per tutto il ciclo di utilizzo delle stesse;
- **visibilità e trasparenza**: solo così sarà possibile instaurare quel grado di fiducia ed affidabilità necessari a permettere ai soggetti interessati di fidarsi;
- **centralità dell'utente**: il sistema di tutela dei dati personali deve porre l'utente al centro, in tal modo obbligando ad una tutela effettiva da un punto di vista sostanziale e non solo formale.

6

Art. 32 GDPR – Sicurezza del trattamento

«*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.»

7

Valutazione del rischio (art. 32 comma 2 GDPR)

«*2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*»

- Tipologie di rischio da valutare:

distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

- La misura di sicurezza è adeguata se in grado di prevenire e contrastare efficacemente questi eventi.
- Valutare anche i parametri della probabilità e della gravità del rischio per i diritti e le libertà dell'interessato.

8

Ricapitolando

- **Definizione del contesto e delle operazioni di trattamento dati effettuate**, sia rispetto alle tipologie di dati raccolti, sia rispetto all'uso che ne viene fatto
- **Valutazione del potenziale impatto sui diritti e libertà degli interessati** nell'eventualità di incidenti o violazioni della sicurezza, in base alle specificità del trattamento effettuato
- **Definizione delle minacce e valutazione della loro probabilità**, dove per minaccia si intende qualsiasi circostanza o evento in grado di pregiudicare la sicurezza dei dati personali
- In aggiunta alla valutazione del rischio, ci sono altri elementi da tenere in considerazione affinché le misure progettate assicurino un adeguato livello di sicurezza: lo stato dell'arte (il grado di avanzamento tecnologico), i costi, la natura, l'oggetto, il contesto e le finalità del trattamento.
- La valutazione è rimessa al Titolare e al Responsabile (accountability), in rapporto alla specificità del trattamento; il bilanciamento fra i vari criteri viene effettuato caso per caso.

9

Codice dell'Amministrazione Digitale (CAD) – D.Lgs. 7 marzo 2005 n. 82

- L'originario testo del **CAD** ha subito nel tempo diverse modifiche ed integrazioni, da parte di numerosi interventi normativi: **D.Lgs. 159/2006** (obbligo per la PA di dotarsi di mail istituzionale e PEC), **L. 2/2009** (obbligo di avere una casella PEC per professionisti iscritti in albi ed elenchi), **D.Lgs. 235/2010** (istituzione dei conservatori accreditati di documenti informatici), **L. 221/2012** (recante i principi dell'Agenda Digitale), **L. 98/2013** (decreto del fare), **D.Lgs. 179/2016** (riforma Madia), **D.lgs. 217/2017** (introduce le linee guida)

10

AGID – Linee Guida

- Previste dagli artt. 14 bis e 71 CAD ed emanate dall'AGID:
- *Linee guida di indirizzo*: contenenti regole generali la cui definizione degli aspetti di dettaglio è demandata alla singola Amministrazione
- *Linee guida contenenti regole tecniche*: contenenti le regole generali di cui al comma 1 lettera a. e la definizione degli aspetti di dettaglio, in un apposito Allegato tecnico, costituente parte integrante delle linee guida stesse.

11

Esempi di Linee Guida

- Linee guida di design per i servizi digitali della PA
- Linee guida per il *disaster recovery* delle PA
- Linee guida contenenti Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate
- Caratterizzazione dei sistemi *cloud* per la PA
- Linee guida per la razionalizzazione dell'infrastruttura digitale della PA

12

Direttiva 2016/1148 del Parlamento Europeo e del Consiglio

- La **Direttiva 2016/1148** recante «*misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*», è nota come **Direttiva NIS** (Network and information security).
- Si propone la difesa delle reti e dei sistemi informativi, dal rischio di **incidenti** e si riferisce agli operatori di servizi essenziali ed i fornitori di di servizi digitali.
- L'*incidente* è definito (art. 4) come «*ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi*», cioè tale da comprometterne la disponibilità, l'autenticità, l'integrità o la riservatezza.

13

Direttiva NIS – destinatari

- Gli **operatori di servizi essenziali** sono soggetti, pubblici o privati, i quali svolgono servizi "strategici", che dipendono dalla rete e dai sistemi informativi, nei settori dell'energia, del trasporto, bancario, delle infrastrutture dei mercati finanziari, sanitario e di fornitura e distribuzione di acqua potabile.
- Il **fornitore di servizio digitale** è qualsiasi persona giuridica che fornisce un servizio digitale di mercato *on line*, di motore di ricerca *on line*, di *cloud computing*.
- La Direttiva NIS non si applica agli *Internet Service Providers* che sono già soggetti agli specifici obblighi della Direttiva 2002/21/CE concernente il settore delle comunicazioni elettroniche

14

GDPR e Direttiva NIS

- Entrambi prescrivono misure di sicurezza (sia informatiche, sia organizzative) a presidio di reti, sistemi e dati; si propongono di realizzare legislazioni uniformi in materia ed una stretta collaborazione tra autorità nazionali; promuovono, attraverso l'innalzamento del livello di sicurezza, lo sviluppo di un mercato digitale comune.
- Entrambi prevedono obbligo di comunicazione e sanzioni.
- Diversi destinatari ed oggetto: il GDPR si rivolge a tutti ma riguarda solo la protezione dei dati personali, la Direttiva NIS riguarda solo gli operatori ed i fornitori ma si applica a qualsiasi *incidente*.

15

Norme penali – 1

- **L. 547/1993**, mediante la quale furono introdotti i primi reati informatici: "*reati commessi tramite o ai danni di un computer*".
- Inizialmente il legislatore italiano decise di introdurre pochi nuovi reati vicino a quelli più somiglianti ai crimini informatici, per reagire al caso dell'*hacker* che entrava nel computer altrui.
- Accesso abusivo a sistema informatico (615 ter c.p.) che richiama la violazione di domicilio.
- Danneggiamento informatico (art. 635-bis), che richiama il danneggiamento.
- Frode informatica (art. 640 ter), che richiama la truffa.
- Oggetto era la tutela del bene giuridico (persona, patrimonio).

16

Norme penali – 2

- Nel 2001 il Consiglio d'Europa emana la Convenzione di Budapest (convenzione *cyber crime*), ratificata dall'Italia con **legge 248/2008**.
- Art. 1 della Convenzione contiene le definizioni di sistema informatico, dato informatico, service provider e trasmissione di dati.
- Sistema informatico: computer dedicato a raccolta ed elaborazione di dati
- Sistema telematico: due computer in collegamento fra di loro.
- Reati che gli stati membri sono obbligati ad inserire nel proprio ordinamento:
- Art. 2 – accesso illegale ad un sistema informatico
- Art. 3 – intercettazione abusiva
- Art. 4 – attentato all'integrità dei dati
- Art. 5 – attentato all'integrità di un sistema
- Art. 6 – abuso di apparecchiature
- Art. 7 – falsificazione informatica
- Art. 8 – frode informatica

17

Norme penali – 3

- Attualmente abbiamo diversi reati specifici.
- **Artt. 615 ter** (accesso abusivo ad un sistema informatico o telematico), **615 quater** (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), **615 quinquies** (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico).
- **Artt. 635 ter** (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o altro ente pubblico o di pubblica utilità), **635 quater** (danneggiamento di sistemi informatici o telematici), **635 quinquies** (danneggiamento di sistemi informatici o telematici di pubblica utilità).
- **Artt. 640 ter** (frode informatica), **640 quater** (reato commesso con abuso della qualifica di operatore del sistema) **640 quinquies** (frode informatica del soggetto che presta servizi di certificazione di firma elettronica).

18