La sicurezza dei dati personali

Introduzione a obblighi e responsabilità

Scuola universitaria professionale della Svizzera italiana (SUPSI), 22 settembre 2020

Avv. Gianni Cattaneo, Lugano

CBM Studio legale e notarile

www.cbm-lex.ch

gianni.cattaneo@cbm-lex.ch

I quesiti

A. La sicurezza dei dati personali: quali le basi legali?
B. Esistono standard minimi raccomandati oppure prescritti?
C. La violazione della sicurezza può dare adito a responsabilità penale degli organi e dirigenti?

A. La sicurezza dei dati personali: quali le basi legali?

Art. 7 LPD: Sicurezza dei dati

[1] I dati personali devono essere protetti contro ogni trattamento non autorizzato, mediante provvedimenti tecnici ed organizzativi appropriati.

[2] Il Consiglio federale emana disposizioni più dettagliate circa le esigenze minime in materia di protezione dei dati.

Art. 7 pLPD Sicurezza dei dati personali (revisione: Link)

[1] Il titolare e il responsabile del trattamento garantiscono, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio.

[2] I provvedimenti devono permettere di evitare violazioni della sicurezza dei dati.

[3] Il Consiglio federale emana disposizioni sui requisiti minimi in materia di sicurezza dei dati.

A. La sicurezza dei dati personali: quali le basi legali?

Art. 143bis CP (Accesso indebito a un sistema per l'elaborazione di dati)

1. Chiunque si introduce indebitamente, per mezzo di un dispositivo di trasmissione dei dati, in un sistema altrui per l'elaborazione di dati ***specialmente protetto contro ogni suo accesso*** *è punito, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria.*

2. Chiunque mette in circolazione o rende accessibili password, programmi o altri dati, sapendo o dovendo sapere che sono destinati allo scopo di cui al capoverso 1, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

Art. 143 CP (Acquisizione illecita di dati)

1. Chiunque, per procacciare a sé o ad altri un indebito profitto, procura, per sé o altri, dati a lui non destinati e ***specialmente protetti contro il suo accesso non autorizzato****, registrati o trasmessi elettronicamente o secondo un modo simile, è punito con una pena detentiva sino a cinque anni o con una pena pecuniaria.*

2. L'acquisizione illecita di dati a danno di un congiunto o di un membro della comunione domestica è punita soltanto a querela di parte.

B. Esistono standard minimi raccomandati oppure prescritti?

<u>Misure generali minime di protezione</u> (art. 8 OLPD)

- assicurare il carattere confidenziale, la disponibilità e l'integrità dei dati («CIA» → sicurezza)
- proteggere i sistemi segnatamente contro i rischi di distruzione accidentale o non autorizzata, perdita accidentale, errori tecnici, falsificazione, furto o uso illecito, modificazione, copia, accesso o altro trattamento non autorizzati
- valutare i rischi potenziali per le persone interessate
- riesaminare periodicamente le misure di protezione

B. Esistono standard minimi raccomandati oppure prescritti?

Misure particolari minime di protezione (art. 9 OLPD)

- controllo dell'entrata nelle installazioni: le persone non autorizzate non hanno accesso ai locali e alle installazioni utilizzate per il trattamento dei dati personali
- controllo dei supporti di dati personali: le persone non autorizzate non possono leggere, copiare, modificare o rimuovere supporti di dati
- controllo del trasporto: le persone non autorizzate non possono leggere, copiare, modificare o cancellare dati personali al momento della comunicazione o del trasporto di supporti di dati
- controllo di comunicazione: i destinatari ai quali vengono comunicati dati personali con l'ausilio di impianti di trasmissione possono essere identificati

B. Esistono standard minimi raccomandati oppure prescritti?

- controllo di memoria: le persone non autorizzate non possono né introdurre dati personali nella memoria né prendere conoscenza di dati memorizzati, modificarli o cancellarli;
- controllo di utilizzazione: le persone non autorizzate non possono utilizzare i sistemi di trattamento automatizzato di dati personali con l'ausilio di impianti di trasmissione;
- controllo d'accesso: le persone autorizzate hanno accesso soltanto ai dati personali di cui abbisognano per svolgere i loro compiti;
- controllo dell'introduzione: è possibile verificare a posteriori le persone che introducono dati personali nel sistema nonché i dati introdotti e il momento dell'introduzione.

B. Esistono standard minimi raccomandati oppure prescritti?

Ulteriori misure di protezione (artt. 10 – 12 OLPD)

- verbalizzare i trattamenti automatizzati di dati personali degni di particolare protezione o di profili della personalità se le misure preventive non sono sufficienti a garantire la protezione dei dati
- elaborare un regolamento che descrive in particolare l'organizzazione interna e le procedure di trattamento e di controllo dei dati e comprende i documenti relativi alla pianificazione, elaborazione e gestione della collezione e dei mezzi informatici
- informare il destinatario al momento di ogni comunicazione sull'attualità e l'affidabilità dei dati personali

B. Esistono standard minimi raccomandati oppure prescritti?

Standard raccomandati dall'Ufficio federale per l'approvvigionamento economico del paese

- Fondamento: *NIST Cybersecurity Framework Core (link)*
- Principi e finalità: costituiscono la parte consultiva e contengono informazioni di base sulla sicurezza TIC
- Parte strutturale *(framework)*: propone agli utenti una serie di misure concrete, 106 in tutto, suddivise in cinque temi: «identificare», «proteggere», «intercettare», «reagire» e «ripristinare».
- *Auto-assessment* e tool di valutazione (Excel): consentono a organismi o imprese di verificare lo stato di avanzamento delle misure e di farlo analizzare anche da ditte terze *(audit)*.

Standard minimo TIC (PDF, 1 MB, 27.08.2018)

Standard minimo TIC - tool di valutazione (XLS, 1 MB, 27.08.2018)

C. La violazione della sicurezza può dare adito a responsabilità penale degli organi e dirigenti?

Art. 55 pLPD Violazione degli obblighi di diligenza (revisione: Link)

Sono puniti con la multa fino a 250 000 franchi i privati che intenzionalmente:

a. comunicano dati personali all'estero in violazione dell'articolo 13 capoversi 1 e 2 e senza che sussistano le condizioni di cui all'articolo 14;
b. affidano il trattamento di dati a un responsabile senza che sussistano le condizioni di cui all'articolo 8 capoversi 1 e 2;
c. non rispettano i requisiti minimi in materia di sicurezza dei dati emanati dal Consiglio federale in virtù dell'articolo 7 capoverso 3.

C. La violazione della sicurezza può dare adito a responsabilità penale degli organi e dirigenti?

Art. 29 CP Rapporti di rappresentanza

Se fonda o aggrava la punibilità, la violazione di un dovere particolare che incombe unicamente alla persona giuridica, alla società o alla ditta individuale è imputata a una persona fisica allorquando essa agisce:

a. in qualità di organo o membro di un organo di una persona giuridica;
b. in qualità di socio;
c. in qualità di collaboratore di una persona giuridica, di una società o di una ditta individuale nella quale esercita competenze decisionali autonome nel proprio settore di attività;
d. in qualità di dirigente effettivo senza essere organo, membro di un organo, socio o collaboratore.

Grazie!


Il diritto alla protezione dei
dati è l'inizio di ogni libertà