CONVEGNO CESIFIN
"Privacy digitale e protezione dei dati personali tra persona e mercato"
Firenze, Palazzo Incontri
23 ottobre 2017

PRIVACY, SICUREZZA DEI DATI E RISCHIO INFORMATICO

Sara Landini [*]

Il titolo della relazione parla di rischio informatico che io intenderei come **rischio dello spazio cibernetico**. Si parla sempre più spesso di rischio cibernetico, ma l'aggettivo cibernetico deve essere riferito allo spazio in cui il rischio opera piuttosto che alle qualità del rischio. Lo spazio cibernetico può essere definito come il network delle infrastrutture della information tecnology inclusivo delle rete internet, delle sistema di telecomunicazioni, dei sistemi informatici…

La definizione di spazio cibernetico la troviamo in Italia nella direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali D.P.C.M., 17/02/2017 , G.U. 13/04/2017.

Questa nuova direttiva emanata con DPCM del 17 febbraio 2017 aggiorna la precedente direttiva del 24 gennaio 2013 tenuto conto in particolare delle novità introdotte con l'emanazione della direttiva(UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS).

Qui (art. 2) si definisce:

-spazio cibernetico: l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi;

-sicurezza cibernetica: condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel controllo indebito, danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi.

Si individuano poi i soggetti referenti di funzioni e responsabilità a partire dal Presidente del CDM responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della repubblica, al Comitato interministeriale per la sicurezza della Repubblica.

[*] *Università degli Studi di Firenze.*

La risorsa principale dello spazio cibernetico sono i **dati**, il valore commerciale di questi è in crescita. Le società che possiedono le informazioni degli utenti presentano una valutazione maggiorata.

La sicurezza nelle linee guida italiane si articola in misure strategiche di:

- Miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
- Potenziamento delle capacità di difesa delle "Infrastrutture critiche nazionali" nonché degli attori di rilevanza strategica nazionale.
- Incentivazione della cooperazione tra istituzioni e imprese
- Promozione e diffusione della cultura della sicurezza cibernetica
- Rafforzamento della capacità di contrasto alla diffusione di attività e contenuti illegali on line
- Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica
- Maggiore cooperazione internazionale
- Compliance con gli obblighi internazionali
- Compliance a standard e protocollli di sicurezza

In tale linea già nel 2016 è stato pubblicato il primo Framework Nazionale di Cyber Security.

Per comprendere la rilevanza del problema in Italia possiamo riprendere i dati di un'importante ricerca compiuta da Banca d'Italia (QEF 373- Febbraio 2017) con riferimento a società operanti nel settore non finanziario con più di 20 addetti. "per quanto solo l'1,5 per cento delle imprese non adotti alcuna misura difensiva, il 30,3 per cento – corrispondente al 35,6 per cento degli addetti – dichiara di aver subito danni a causa di un attacco informatico tra Settembre 2015 e Settembre 2016. Correggendo i risultati per tenere conto delle intrusioni non individuate o non dichiarate, l'incidenza degli attacchi sale al 45,2 per cento per le imprese e al 56 per cento per gli addetti; sono più colpite le imprese di maggiori dimensioni, quelle con elevato contenuto tecnologico e quelle esposte sui mercati internazionali. Il livello di rischio nel complesso dell'economia è probabilmente ancora più alto; il settore finanziario, così come la sanità, l'istruzione e i servizi sociali sono esclusi dal campione, ma secondo altre fonti sono particolarmente attraenti per gli attaccanti".

Le minacce cibernetiche hanno ad oggetto i dati presenti nello spazio cibernetico e consistono essenzialmente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima. Da qui l'accostamento con il concetto di **privacy** intesa come diritto di controllare l'uso e la circolazione dei propri **dati personali**.

Lo spazio cibernetico è però uno spazio di network, di rete, di correlazioni. I dati individuali acquistano rilevanza nella loro unione con altri e nella generazioni di big data, dati grandi: nella quantità, nella velocità della loro trasmissione, nella quantità di correlazioni cui possono dar vita.
Non è più solo un problema di privacy, è un problema, per quanto riguarda in specie le persone fisiche, di tutela del proprio essere persona nel momento in cui attraverso correlazioni un algoritmo definisce la nostra identità.

Tutto questo è chiaro al regolamento europeo 679/2016 che nel proprio 6° considerando sottolinea come:
"la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancor di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali garantendo al tempo stesso un elevato livello di protezione dei dati personali".

La tecnologia apre a nuove scenari e a nuove sfide nella tutela della persona individuando nuove minacce ma anche nuovi strumenti di difesa.

Zigmut Bauman in uno dei suoi ultimi libri "Società dell'incertezza", sulla scia delle sue teorie sulla società liquida, individua due modelli uno fondato sulla sicurezza e uno sulla libertà che però genera deregolamentazione e incertezza. Osserva quindi come alla deregolamentazione fa spazio un sistema di "autoregolamentazione".
La complessità della società contemporanea non si regola, si governa. Non è possibile risolvere i problemi con regole astratte e con meccanismi sanzionatori che intervengono ex post in caso di violazione.
Occorre trovare strategie per prevenire i problemi, perché quando questi si porranno non sarà più possibile una soluzione o lo sarà con costi altissimi. Le parole chiave della società contemporanea diventano Governance, Compliance, Risk Management.

Il rischio è che si faccia strada una compliance astratta e formale fatta di lunghe check list in cui l'attenzione è rivolta al flag ovvero alla nota dell'avvenuto completamento delle fasi della lista una per una.

Occorre pensare a modelli di gestione del rischio degli spazi cibernetici che riescano a prevenire o a minimizzare in concreto le minacce in concreto avuto riguardo alle peculiarità del caso concreto.