Gli effetti della Digital Transformation sugli scenari della Cyber Security

Roma, 4 luglio 2017

selta.com

Direttiva Nis e responsabilità giuridiche in materia di Cybersecurity

di Paolo Galdieri

Le minacce nel cyberspace

- cyber crimes (qualsiasi reato commesso attraverso le tecnologie dell'informazione)

- cyber war (conflitto tra soggetti di diritto internazionale condotto tramite operazioni informatiche)

Strumenti di difesa

- tecnologica (cyber security)

- giuridica (Diritto interno ed internazionale)

Approccio al tema della cyber security

- inizialmente il contrasto alle cyber minacce viene risolto esclusivamente sul piano della sicurezza

- manca piano strategico globale, tutto affidato alla spontaneità del singolo
assenza di vincoli giuridici

- iniziali tentativi legislativi frammentari e non deterrenti

Approccio al tema della cyber security

- assenza di coordinamento delle strategie sulla cyber security con le strategie di carattere giuridico

- frammentazione della normativa, frammentazione degli interventi sulla cyber security

- verso una regolamentazione giuridica globale della cyber security

Approccio al problema delle cyber minacce sul piano giuridico

-iniziale sottovalutazione del fenomeno

- mancanza di dati certi (omessa denuncia)

- mancanza di norme

- convinzione che sistema giuridico sufficiente

Approccio al problema delle cyber minacce sul piano giuridico

- presa atto del dover legiferare

- legislazione dapprima concentrata sul diritto sostanziale

- legislazione che affronta le questioni procedurali e processuali

- legislazione che si concentra sulla cyber security

Normativa europea in materia di cyber crime

- Raccomandazione n. 89/9 sulla criminalità informatica

- Raccomandazione n.R (95) 13 del Consiglio dei Ministri agli Stati membri relativa ai problemi di procedura penale legati alla tecnologia dell'informazione

- Convenzione del Consiglio d’Europa sulla criminalità informatica del 2001

Legislazione Nazionale

- Legge 23 dicembre 1993, n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"

- Legge 18 marzo 2008, n.48 “Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica”

Legislazione Nazionale

Pedofilia telematica

- Legge 3 agosto 1998, n. 269, "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù"

- Legge febbraio 2006, n.38 “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”

- Legge 1 ottobre 2012 n. 172 “Ratifica ed esecuzione della Convenzione del Consiglio d’Europa per la protezione dei minori contro lo sfruttamento e l’abuso sessuale

Legislazione Nazionale

Terrorismo internazionale

- Legge 15 dicembre 2001, n.438 che ha convertito, con modificazioni, in legge, il decreto-legge 18 ottobre 2001, n.374 intitolato " Disposizioni urgenti per contrastare il terrorismo internazionale"

- Legge 17 aprile 2015, n. 43 che ha convertito, con modificazioni, in legge, il decreto-legge 18 febbraio 2015, n. 7 recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale

Problemi aperti

- accertamento del reato ed individuazione dell’autore

- computer forensics

- cooperazione in ambito giudiziario e di polizia

Rapporti cyber security e diritto

- I fase: cyber security e non diritto

- II fase: diritto per contrastare cyber minacce

- III fase: diritto che si occupa della cyber security

Iniziale concezione della cyber security nella legislazione

- singoli interventi per determinati settori

- norme incomprensibili agli informatici

- cyber security affrontata nelle aziende con fatalismo

- cyber security vista come problema giuridico da affrontare in un momento successivo

- Regole cyber security come ostacolo e non come opportunità

- incomunicabilità tra esperto sicurezza e giurista

Cambio di prospettiva in materia di cyber security

- la sicurezza non può essere lasciata al “buon cuore” del singolo

- servono norme che prevedono obblighi e responsabilità

La cyber security prima arma di contrasto alle cyber minacce

- 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, "Direttiva NIS"

- mira a rafforzare la cyber security dell'Unione Europea

- prevede obblighi comuni di sicurezza per gli operatori di servizi essenziali e per i fornitori di servizi digitali

La cyber security prima arma di contrasto alle cyber minacce

- gli operatori di servizi essenziali (soggetto pubblico o privato, energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari) dovranno prendere appropriate misure di sicurezza per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi, e notificare gli incidenti rilevanti all'autorità nazionale competente

- i fornitori di servizi digitali (motori di ricerca, cloud computing e online marketplaces) dovranno conformarsi ai requisiti di sicurezza e al regime delle notifiche previsti dalla direttiva

Normativa nazionale in materia di sicurezza

- Piano nazionale per la protezione cibernetica e la sicurezza informatica (Gazzetta ufficiale n. 125 del 31 maggio 2017)

- Decreto del Presidente del Consiglio dei Ministri del 17 febbraio 2017 “Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali”(Gazzetta ufficiale n. 87 del 13 aprile 2017)

- Circolare AgID 17 marzo 2017, n. 1/2017, recante le “Misure minime di sicurezza ICT per le pubbliche amministrazioni”.

- Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali

Normativa nazionale in materia di sicurezza

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE

- Decreto Legislativo 8 giugno 2001, n. 231, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell´articolo 11 della legge 29 settembre 2000, n. 300"

Nuova strategia aziendale in materia di cyber security

- problema cyber security non più rinviabile

- accanto al problema di natura tecnica si aggiunge quello della responsabilità giuridica

- cyber security diventa opportunità e non ostacolo all'attività di impresa

Nuova strategia aziendale in materia di cyber security

- strategia cyber security unitaria in grado di fornire risposte alla normativa in modo globale

- strategia cyber security e giuridica da considerarsi un tutt'uno

- necessità di una stretta comunicazione tra esperto sicurezza e giurista

Conclusioni

- l’Italia si è dotata e si sta ulteriormente dotando di regole per quanto concerne la cyber security prevedendo in ambito pubblico e privato responsabilità e sanzioni

- si tratta di norme che provengono da ambiti diversi e comportano oneri differenti ma in un’ottica strategica sana possono e devono essere trattate in modo unitario e complessivo

- nel momento in cui verranno stabiliti i nuovi obblighi si potrebbe incorrere anche in sanzioni penali in virtù art. 40 c.p., che prevede la punibilità del soggetto che non impedisce l’evento che aveva l’obbligo giuridico di impedire

Conclusioni

- la sicurezza non deve essere più percepita come un costo ed un fastidio, ma come un’opportunità, sia per evitare problemi giuridici, che di immagine

- la sicurezza non può più essere affrontata esclusivamente come un fatto tecnico, ma anche giuridico e quindi servono entrambe le competenze per interpretare correttamente le norme