29/03/2019

Il Sole 24 ORE

Pagina 22

EAV: € 64.449
Lettori: 281.841

Argomento: Società e Imprese

Standard globali in difesa della trasformazione digitale

Paola Severino


Commenti

STANDARD GLOBALI IN DIFESA DELLA TRASFORMAZIONE DIGITALE

L'UMANESIMO INDUSTRIALE NON È TRAMONTATO

Cybersecurity e digital transformation rappresentano un binomio inscindibile. Vi è infatti una strettissima correlazione tra i due ambiti: senza la cybersecurity il processo di digitalizzazione rischia non solo di non giungere agli esiti sperati, ma addirittura esso finisce con il rivelarsi un boomerang per gli operatori dei diversi settori. La rivoluzione digitale è un fenomeno sotto gli occhi di tutti e sono evidenti i vantaggi che anzitutto le imprese e gli attori istituzionali possono conseguire grazie a queste tecnologie. La digital transformation ha letteralmente cambiato il volto della realtà aziendale: ha modificato gli aspetti strutturali delle organizzazioni complesse, le logiche di funzionamento delle imprese e i modelli di business. La tecnologia, invero, ha mutato a fondo gli aspetti operativi, strategici e di governance, inducendo un profondo cambiamento nelle logiche competitive del mercato. Dalla fine degli anni 90 abbiamo assistito allo sviluppo di reti digitali e di infrastrutture di comunicazione che permettono l' accesso a quella che è stata definita una "piattaforma globale". Si sono costruite nuove modalità attraverso cui persone e organizzazioni possono interagire, comunicare, collaborare, cercare informazioni e avviare strategie di vendita o di fornitura di servizi. Questa nuova rivoluzione, Industria 4.0, è diretta conseguenza del processo di digitalizzazione. Per effetto di questo mutamento di paradigma le aziende, ma anche le organizzazioni pubbliche, hanno iniziato a confrontarsi con una duplice realtà: quella della gestione delle risorse fisiche e virtuali. La digitalizzazione è tuttavia un Giano bifronte. Da un lato, si stagliano gli indubbi vantaggi che essa è in grado di generare: essere digitalizzati significa saper rispondere alle esigenze di mercato in tempo reale, un mercato in continuo mutamento e che richiede alle aziende capacità di adattamento e competitività. La tecnologia permette una migliore gestione di tempo e risorse e consente di creare una rete virtuale di condivisione delle informazioni interne ed esterne, che risulta funzionale a un processo di continuo miglioramento delle performance aziendali. Non è certo un caso che la Internet economy sia divenuta la

colonna portante dell' economia globale. La trasformazione digitale ha però il suo lato oscuro, rappresentato dalla vulnerabilità dei sistemi e dei dati informatici. Il volume, la rapidità, il livello di sofisticatezza degli attacchi informatici è in costante aumento, e sempre più rilevanti risultano i danni prodotti da siffatti attacchi in termini di compromissione di dati sensibili, di alterazione della loro integrità, di incidenza sul regolare funzionamento di infrastrutture critiche. L' importanza della cybersecurity va di pari passo al crescere del ventaglio delle minacce informatiche. I dati sono al riguardo impietosi: il 2018 è stato l' anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, soprattutto dal punto di vista qualitativo, evidenziando una tendenza di crescita degli attacchi, della loro gravità e dei danni conseguenti, mai registrata in precedenza. Dal punto di vista quantitativo si evince invece che nel quinquennio 2014-2018 la crescita degli attacchi gravi è stata del +77,8 per cento. È un vero e proprio cambiamento epocale nelle scelte di gestione dell' azienda, collocando in posizione centrale la valutazione e la gestione dei rischi provenienti dallo spazio virtuale. Al cuore della questione non c' è solo un problema di tipo tecnologico quanto piuttosto culturale, economico e di framework normativo. Bisogna organizzare i processi aziendali tenendo conto delle minacce per la sicurezza delle reti e dei sistemi di informazione. La sfida posta al giurista è impegnativa: contrastare i fenomeni criminosi - e fare in modo che gli strumenti in campo siano efficaci - ma al contempo progettare meccanismi preventivi e di cooperazione tra i diversi attori impegnati sul fronte del contrasto. Si riconosce inoltre la necessità e l' urgenza di regolamentare lo spazio cibernetico e la cooperazione tra Autorità, per dare concretezza a un approccio globale e cooperativo alla sicurezza delle reti e dei sistemi di informazione. Gli illeciti commessi in rete si caratterizzano per la dimensione essenzialmente transnazionale, derivante dalla aterritorialità del cyberspazio. Ciò ha condotto gli Stati e le organizzazioni internazionali a intraprendere numerose iniziative a livello locale per porre un argine al dilagare della criminalità informatica. Sul piano sovranazionale, la lotta contro il crimine informatico si è incardinata su tre fronti: la creazione di una base legale comune nella definizione degli illeciti; la cooperazione tra autorità giudiziarie; il coordinamento investigativo e la mutua assistenza nelle attività d' indagine. L' armonizzazione delle disposizioni di diritto penale sostanziale garantisce agli Stati una base giuridica comune per la lotta al cybercrime. Tra le istituzioni internazionali, quella che ha raggiunto i traguardi più significativi in quest' ambito è senza dubbio il Consiglio d' Europa, a cui si deve la elaborazione della Convenzione di Budapest sul cybercrime. Fatte queste doverose premesse sul quadro normativo di riferimento, sento di dover porre l' accento sulla importanza della compliance aziendale in materia di cybersecurity. Il secondo piano su cui si deve intervenire è di carattere preventivo. La partnership pubblico-privata è diventata il volàno di una nuova idea di contrasto ai fenomeni criminosi. È chiaro come il raggiungimento dell' obiettivo sicurezza rappresenti un primario interesse per le stesse imprese tenute all' adempimento. In uno spazio virtuale dinamico e in continua evoluzione l' autoresponsabilizzazione degli attori economici, la valutazione continua dei rischi provenienti dal cyberspazio e la compliance sono gli strumenti più flessibili ed efficaci. Due provvedimenti che riguardano da vicino questa materia sono stati

approvati dal legislatore europeo nel 2016. Il Regolamento generale sulla protezione dei dati personali guarda l' information security dalla prospettiva del dato personale. La Direttiva sulla sicurezza delle reti e dei sistemi di informazione, che disciplina la cybersecurity a livello nazionale, rappresenta il trait d' union della regolazione pubblica nel settore della sicurezza informatica, essendo rivolta tanto agli operatori pubblici quanto a quelli privati. Tra le sfide da affrontare, il rafforzamento della cooperazione internazionale in materia di contrasto al cybercrime è, a mio modo di vedere, il traguardo più importante. Un fenomeno per sua natura transazionale non potrebbe essere affrontato, se non attraverso una presa d' atto globale. Una seconda sfida è nel superamento delle barriere tra settore pubblico e settore privato. In questa direzione si sta muovendo il Consiglio d' Europa con l' istituzione di numerosi tavoli d' intesa con i service provider e con le imprese che erogano servizi di accesso alla rete. Occorre oggi più che mai stabilire un accordo quadro sulla collaborazione tra fornitori di servizi e l' Autorità giudiziaria, per rendere efficiente e rapido l' enforcement delle decisioni giudiziarie e l' individuazione delle fonti di prova. L' armonizzazione a livello sovranazionale e la realizzazione di un "mercato unico digitale" rende auspicabile la creazione di uno standard di certificazione cybersecurity comune a tutti gli Stati, secondo una formula già sperimentata in altri settori. A tal riguardo, gli Stati dovrebbero concordare sulla importanza delle certificazioni di sicurezza e della definizione degli standard minimi di cybersecurity: in questa direzione si stanno muovendo le Istituzioni dell' Unione europea.