"Cybersecurity law": una panoramica sulla disciplina nazionale e comunitaria in tema di sicurezza informatica

Author : Redazione

Date : 10 Luglio 2020

Il volume - a cura di Alfonso Contaldo e Davide Mula, con un'introduzione di Giuseppe Busia, segretario generale del Garante per la protezione dei dati personali - contiene saggi di numerosi Autori che ripercorrono i passaggi fondamentali della normativa di cybersecurity italiana ed europea.
L'intento è descrivere analiticamente la disciplina valorizzandone le molteplici e variegate norme tecniche, anche internazionali, che si sono progressivamente consolidate in materia, per illustrare la graduale e costante espansione delle frontiere della sicurezza cibernetica.

Il **primo capitolo** offre un quadro definitorio della *cybersecurity* e della *cyberdefence*, focalizzandosi sulle *policies* del Consiglio europeo in materia di *cybersecurity*, *cyberesilienza* e diplomazia cibernetica; sulla disciplina giuridica del settore a seguito della direttiva comunitaria in materia di protezione delle infrastrutture critiche; infine, sulle disposizioni del regolamento eIDAS e della direttiva NIS.

Il **secondo capitolo** – Campara F. – ha come oggetto d'analisi il *Cybersecurity Act* (primo contributo in Italia sull'argomento), ossia il Regolamento (UE) n. 2019/881 del Parlamento europeo e del Consiglio del 17/04/2019, destinato a innovare profondamente la materia, prefiggendosi due finalità principali: rafforzare il ruolo dell'ENISA (Agenzia dell'Unione europea per la sicurezza cibernetica) attraverso importanti interventi riformatori e, soprattutto, dettare una cornice normativo-regolamentare europea per la certificazione della sicurezza informatica di prodotti, servizi e processi ICT.

Il **terzo capitolo** – Peluso F. – guarda ai confini nazionali, soffermandosi sul *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, adottato con DPCM 17/02/2017, in cui sono individuati gli indirizzi interpretativi, gli obiettivi da raggiungere e la linea d'azione da seguire per l'attuazione del Quadro Strategico Nazionale per la sicurezza del cyberspazio (QSN), il quale non si pone come mero aggiornamento del precedente Piano ma anzi si dà l'obiettivo di imprimere un immediato impulso all'ulteriore fase di sviluppo dell'architettura nazionale *cyber*. Altri oggetti di studio del capitolo sono il ruolo dei CSIRT (*Computer Security Incident Response Team*) e le disposizioni del d. lgs. n. 65/2018 riguardanti la gestione degli incidenti e gli obblighi degli operatori in tali circostanze. Infine, si riporta un'analisi sulle regole

tecniche del CAD (Codice dell'Amministrazione Digitale) e sulla loro applicabilità alla *cybersecurity*.

Il **quarto capitolo** – Mula D. – è incentrato sul rapporto esistente tra *privacy*, *data protection* e *cybersecurity*; sulla Direttiva NIS e sul Regolamento ENISA e il loro impatto sulla disciplina in materia di trattamento dei dati personali; sulla misurazione del rischio *privacy*; sugli incidenti e violazioni dei dati; infine, sulle data *security* e *cybersecurity* dei *servizi cloud*.

Il **quinto capitolo** – Contaldo A. – verte sulla disciplina della sicurezza del perimetro cibernetico nazionale anche alla luce dello standard 5G, prendendo in considerazione le norme internazionali, europee ed italiane sulle tecnologie e gli *standard* di quinta generazione. In particolare, il capitolo analizza il rapporto tra *golden power* e 5G; le procedure di notifica di incidenti informatici impattanti sul perimetro cibernetico e le procedure di notifica relative alle forniture di beni e servizi ICT necessari alle reti strategiche; i soggetti vigilanti (il Centro Valutazione e Certificazione Nazionale e il MISE); i compiti della Presidenza del Consiglio e, infine, le sanzioni amministrative e penali previste in caso di lesioni, reali e potenziali, del perimetro cibernetico.

Il **sesto** e ultimo **capitolo** – Salandri L. – analizza il rapporto tra IT e gli *standard* di *cybersecurity*, descrivendone le norme tecniche e la competitività nella globalizzazione produttiva. Si evidenzia, poi, l'importanza dell'implementazione della sicurezza informativa nell'automazione industriale, la rilevanza in Europa dell'Organizzazione internazionale per la normazione e l'importanza della standardizzazione negli USA.

Paradossalmente, la *cybersecurity* entrerà davvero a far parte della nostra quotidianità nel momento in cui non la distingueremo più dal concetto generale di sicurezza e la percepiremo come la naturale necessità di proteggere noi stessi e le nostre comunità, sentendola come parte essenziale del nostro agire.
Dopotutto, viviamo in un mondo dove gran parte dell'esistenza dei singoli e delle istituzioni, non solo si proietta, ma si svolge e realizza attraverso e nelle reti telematiche. Motivo per cui allora la *cybersecurity* – nata come branca limitata e specifica relativa alla protezione degli apparati e dei sistemi informatici, oltre che delle informazioni che su essi sono conservati e viaggiano – ha visto progressivamente espandere i propri confini e rilevanza, avvicinandosi a ricomprendere **l'intero perimetro della sicurezza** *lato sensu*.

Ciò rappresenta l'obiettivo più profondo del volume, dedicato alla *cybersecurity* e volto ad analizzarne e spiegarne significato e applicazioni: quindi a far sì che dalla conoscenza del suo ruolo, nasca una consapevolezza piena e diffusa. L'esigenza di una simile sfida, a un tempo culturale e scientifica, emerge laddove si osservi come ancora allo stato, nella percezione più immediata dell'opinione pubblica, l'espressione *cybersecurity* continui troppo spesso ad essere legata a realtà suggestive, lontane dalla vita di tutti i giorni. Essa riesce molte volte a incuriosire o appassionare, alla stregua di come potrebbe farlo un film di fantascienza, perché continua ad essere percepita come una questione riservata ai soli protagonisti della *governance* statale e internazionale.

A tale "esclusivo *club*" di operatori si aggiunge qualche studioso della materia, nel ristretto

perimetro fra una branca specialistica del diritto e i tecnologi del settore. Chiaramente la realtà in cui siamo immersi è totalmente differente: le tecnologie sono fondamentali nel quotidiano e ci accompagnano in ogni nostra azione, vivendo in ambienti sempre più affollati di oggetti connessi e "intelligenti". La nostra esistenza sempre più spesso viene a dipendere da tali tecnologie ed è, quindi, evidente che **la sicurezza cibernetica riguarda la nostra sfera, pubblica e privata**, toccandoci da vicino più di quanto immaginiamo o vogliamo immaginare.

Nel contesto economico e produttivo, l'irreversibile affermazione delle tecnologie digitali ci ha portato a quella che è stata definita la Quarta Rivoluzione Industriale, nel c.d. sistema di produzione 4.0, legando indissolubilmente l'uomo a *Internet*, come un tempo l'automazione dei sistemi produttivi, con le conseguenti trasformazioni strutturali delle economie nazionali, lo aveva legato alle macchine e poi all'elettronica. È indubbio che la trasformazione digitale in corso operi anche un profondo **cambiamento dei modelli sociali** consolidati sui quali poggia la stabilità e la tenuta degli Stati, con una capacità di riflettersi immediatamente anche sui suoi cittadini. Ancora oggi gli utenti sembrano vivere nel *web* in una dimensione quasi giusnaturalistica, in una sorta di Stato di natura digitale che, sebbene si fondi su una fenomenologia del tutto virtuale, plasma, condizione e determina in concreto l'esistenza dei singoli. Al contempo il cyberspazio non può essere abbandonato all'*homo homini lupus* di hobbesiana memoria, ma deve conoscere forme di regolamentazione e, soprattutto, di tutela di coloro che si muovono nell'ambito dei suoi (non)confini, tanto inesistenti quanto immateriali.

Nel riportare la disciplina in materia, il volume richiama l'attenzione del lettore su un punto essenziale: se le frontiere della cybersecurity sono in continua espansione, allora la materia non può non interessare sempre più da vicino anche i singoli, che ormai interagiscono quotidianamente nel cyberspazio, un (non)luogo vero, in cui trovano allocazione pure – spesso tramite i sistemi *cloud* sempre più pervasivi e performanti – le grandi **banche dati strategiche** che custodiscono le più rilevanti raccolte di dati, a volte di natura sensibile, riguardanti tutti noi. Ecco perché l'iniziale distacco verso quell'insieme di tecnologie, programmi, processi e tecniche concepiti e realizzati per proteggere dispositivi, dati e reti informatiche deve essere tramutato in una presa di coscienza collettiva, che porta a concepire la cybersicurezza come un bene di tutti, da difendere, anche tramite un progressivo allineamento tra interessi pubblicistici e privatistici o, meglio, attraverso la loro convergenza in un unico obiettivo: la sicurezza *tout court*. Non a caso già la *Strategia dell'Unione Europea per la cybersicurezza: un ciberspazio aperto e sicuro* (2013) si basa su una serie di principi che pongono la persona al centro del sistema, quali la protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della privacy; l'accesso alla rete garantito a chiunque; una "*multi-stakeholder governance*" democratica ed efficiente; la responsabilità condivisa tra tutti gli attori coinvolti.

Un ulteriore aspetto evidenziato dagli autori riguarda i rischi legati alla rapida **propagazione degli attacchi cibernetici**. L'universo *cyber* ha infatti una sua caratteristica dimensione transnazionale, per cui gravi perturbazioni del sistema, indipendentemente dal luogo in cui si verificano, possono coinvolgere altri Stati, diffondersi rapidamente attraverso l'intera UE e anche oltre i suoi confini. In un mondo sempre più interconnesso ma privo di confini territoriali da presidiare, le vulnerabilità strutturali di uno Stato non si arrestano ai suoi confini nazionali. Ed anche solo la percezione del rischio di danni gravi per i singoli e le collettività nazionale finisce per minare la fiducia degli operatori, pregiudicando le prospettive di crescita. La

cybersecurity diventa perciò un fattore di sviluppo economico essenziale.

Se ci si fermasse a questo, tuttavia, non si comprenderebbero fino in fondo le ragioni per le quali la *cybersecurity* tocca la quotidianità di ogni persona e non solamente la vita di istituzioni o imprese strategiche. Gli ultimi anni non sono stati caratterizzati solo dal sempre più rapido raggiungimento di nuovi traguardi nelle tecnologie digitali, ma anche dalla fornitura di servizi personalizzati. Questi ultimi si basano sulla **raccolta ed elaborazione di un numero crescente di dati personali**, spesso attraverso sistemi di intelligenza artificiale, al fine di offrire servizi personalizzati, tanto nel settore pubblico quanto in quello privato. Tutto ciò fa sì che sulle reti e nei sistemi informatici vengano raccolti in misura crescente dati di carattere personale, anche quando apparentemente "anonimizzati". Le vulnerabilità dei sistemi informatici dunque non mettono solo a rischio informazioni strategiche relative alla vita delle istituzioni di un Paese, ma direttamente i cittadini. Proteggere i dati significa proteggere insieme la collettività e le singole persone che la compongono.

Il crescente uso delle tecnologie digitali da parte di tutti noi non solamente amplia la superficie di attacco, rendendo ancora più evidente l'esigenza di misure di sicurezza cibernetica, ma espone in modo diretto i singoli a tali pericoli, perché l'eventuale attacco coinvolgerebbe nella maggior parte dei casi anche dati e informazioni a loro riferibili, con conseguenze immediate sulle loro persone.

Ecco allora che – come emerge dalle pagine del libro – esiste un legame sempre più stretto fra le misure di sicurezza, che sono da sempre parte essenziale della disciplina sulla protezione dei dati personali, e la *cybersecurity*. Naturalmente non si può negare che le due normative nascono da filoni normativi differenti e mantengono una chiara separazione, a partire dalle diverse finalità perseguite: la Direttiva NIS – che ormai lascia il posto al *Cybersecurity Act* (CSA), il Regolamento (UE) n. 2019/881 del Parlamento europeo e del Consiglio del 17/04/2019 destinato ad innovare totalmente la materia – e il relativo d. lgs. n. 65/2018 di recepimento si prefiggono il compito di dettare specifiche misure di sicurezza finalizzate al conseguimento di un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, così da incrementare anche i livelli di sicurezza a livello UE.
Ed è anche innegabile che per vari aspetti le due discipline si differenziano, specie laddove, per finalità di sicurezza cibernetica, si richieda la raccolta di informazioni personali, dovendo tale esigenza essere bilanciata con i principi di pertinenza e minimizzazione propri della normativa sui dati personali.

Tali differenze si sono mostrate con evidenza laddove qualcuno ha pensato, in nome della protezione cibernetica, di poter svolgere raccolte massive di informazioni personali, magari da conservare per periodi di tempo indefiniti. Appare chiaro infatti che il monitoraggio dei sistemi di controllo stabiliti dalla disciplina NIS non possono determinare un'ingerenza sproporzionata nella sfera di riservatezza di coloro i cui dati sono custoditi negli archivi degli operatori OSE. E tuttavia, proprio l'inarrestabile aumento del ricorso alle tecnologie digitali per la raccolta ed elaborazione di dati personali, oltre che per l'inderogabilità del rispetto dei principi fondamentali in materia di protezione dei dati personali, hanno realizzato un progressivo avvicinamento delle due discipline, facendo prevalere gli elementi di sovrapposizione rispetto a quelli di potenziale tensione. Non si può invero nascondere che sempre più spesso gli attacchi a sistemi "critici"

per lo Stato possono comportare, come effetto immediato, il **trattamento illecito di dati personali** gestiti nell'infrastruttura violata.

Questo spiega perché, sul piano pratico, molte delle misure organizzative e tecniche necessarie per salvaguardare le informazioni di carattere personale ai sensi della disciplina sulla protezione dati sono efficaci e concretamente utilizzate anche in adempimento degli obblighi di *cybersecurity*, e viceversa. Questo è tanto più vero dopo la piena applicazione del GDPR e le conseguenti modifiche al nostro Codice in materia di protezione dati personali, che non reca più un insieme di misure minime applicabili ad ogni *database*, ma sposa integralmente la logica dell'**approccio *risk-based***, responsabilizzando i soggetti pubblici e privati che trattano i dati a garantire misure proporzionate ed adeguate al genere di attività svolta e ai rischi connessi. Ciò spiega, altresì, perché il Garante per la protezione dei dati personali sia intervenuto in più occasioni per segnalare anche al Governo possibili criticità nella protezione dei sistemi e delle infrastrutture.

D'altro lato, in entrambe le aree di intervento gli individui divengono protagonisti (e sono quindi tenuti ad occuparsi della materia) non solo come oggetto di possibili attacchi cibernetici ma, purtroppo, anche come oggetti che – spesso inconsapevolmente – finiscono per favorire la riuscita di tali attacchi. Invero è particolarmente frequente la circostanza che sistemi tecnologicamente ben protetti dalle minacce esterne, vengano violati proprio a causa dell'**errore umano** di un soggetto dell'organizzazione (fenomeno conosciuto come *insider threat*), con ruoli a volte del tutto secondari, che, a causa delle scarse misure di sicurezza adottate per i propri apparati elettronici, si trasformano involontariamente nella porta di accesso per produrre danni a volte ingentissimi a soggetti privati ed istituzioni pubbliche. Tale legame trova conferma anche nella rispettiva disciplina: invero non è un caso se la già richiamata Direttiva NIS abbia sostanzialmente mutuato l'obbligo di notifica degli incidenti rilevanti, dalla notifica delle violazioni dei dati personali, oggi generalizzata dall'art. 33 del GDPR. Ed è chiaro che tale parziale sovrapponibilità presupporrà un crescente coordinamento – peraltro già avviato – da parte delle autorità destinatarie di tali notifiche, al fine non solo di semplificare gli adempimenti da parte dei destinatari di tale obbligo, ma anche e soprattutto per permettere alle medesime di avere un quadro complessivo delle problematiche emergenti in materia di sicurezza.

In entrambi gli ambiti la sicurezza diviene un fattore abilitante per il corretto funzionamento e l'efficienza delle infrastrutture, ed è necessario prevederne ogni componente fin dalla progettazione dei sistemi, secondo la logica propria della ***security* e *privacy by design***, alla base delle rispettive normative.

Serve in ogni caso un salto di qualità in una duplice consapevolezza di fronte ai maggiori rischi derivanti dalla progressiva dipendenza dei singoli, delle comunità e degli Stati dalle reti, dagli apparati e dai sistemi informatici. Da un lato, occorre ampliare notevolmente gli ambiti sui quali attivare le misure di sicurezza in quanto, se tutto è sempre più connesso, le **vulnerabilità** possono verificarsi anche alla periferia della rete e anche lì occorre intervenire. Dall'altro, è chiaro che un simile compito non può essere lasciato alle forze di polizia e di sicurezza, né ai grandi *players* economici che gestiscono le principali infrastrutture materiali e immateriali: occorre invece il contributo attivo di tutti i cittadini che, in maniera più o meno ampia e diretta,

sono nodi di una rete e come tali esposti a rischi, parallelamente decisivi per proteggere sé stessi e gli altri.

Ecco allora l’insegnamento che il libro intende trasmettere e del quale fare tesoro: la cybersicurezza - che oggi è sicurezza *tout court* - è compito alto e qualificante per tutti. E solo se ognuno di noi saprà fare la propria parte potremo esercitare, in modo maturo e responsabile, il nostro essere cittadini nell’epoca difficile e affascinante in cui ci è dato di vivere.

Il volume è pubblicato, nella collana "Diritto e Innovazione", dall'**InnoLawLab** dell'Università Europea di Roma.