Il diritto penale della Globalizzazione
Pacini Giuridica

Il Cybercrime e le strategie dell'Unione Europea.

di Rubinia Proli ed Elena Valguarnera – 28.08.2018

Il crime information, o cybercrime, può essere definito come quel fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica.
Rientrano nella struttura del cybercrime, infatti, l'accesso non autorizzato, il furto d'identità, la frode informatica ed elettronica, ma anche la diffusione di immagini diffamatorie, messaggi offensivi inviati per posta elettronica, il download di risorse protette dal diritto d'autore.
Generalmente, l'identificazione dell'autore di un reato informatico risulta essere difficile per molteplici fattori, in quanto un sistema come internet, non controllato da alcuna autorità, che consente agli utenti l'anonimato e dove i dati vengono diffusi con una rapidità elevatissima e dove cancellare le tracce è relativamente semplice, identificare il responsabile di un reato è un'operazione complessa.
La casistica e la tipologia dei crimini informatici è piuttosto ampia, alcuni reati sono finalizzati allo sfruttamento commerciale della rete internet ed a mettere a rischio i sistemi informativi di sicurezza nazionale di uno Stato.
Il fenomeno dei crimini informatici è in continua crescita, in quanto un numero sempre crescente di persone si connette ad internet mediante portatili, smartphone, tablet.
I crimini informatici possono essere suddivisi in due principali categorie:
i reati singoli, come ad esempio l'installazione di virus "ladro" di dati personali;
i reati ripetuti, come il cyberbullismo, l'estorsione, la distribuzione di materiale pedopornografico, l'organizzazione di attacchi terroristici.
A causa dell'elevato numero di tecniche impiegate dai cybercriminali per attaccare i computer ed i dati degli utenti, le difese multilivello sono una necessità.
L'Unione Europea, da tempo, si è posta l'obiettivo di proteggere il mercato informatico da potenziali esternalità negative rappresentate dalle minacce cibernetiche, ma ciò che è divenuta ancor più evidente è la necessità di dotare l'Unione Europea di una strategia complessiva in materia di cybersicurezza.
Prima di procedere all'analisi delle strategie adottate dall'Unione Europa, ci preme dare una definizione di cybersicurezza che altro non è che l'insieme di tutte quelle discipline impiegate per preservare i sistemi informatici dall'intrusione di hacker o di ospiti indesiderati.
Nello specifico si tratta di tecnologie, processi e pratiche elaborate per proteggere reti, computer e dati, da attacchi informatici, danni o accessi non autorizzati.

Le azioni legislative dell'Unione Europea contribuiscono alla lotta contro la criminalità informatica.
Nel 2013, infatti, l'Unione Europea ha adottato una direttiva sugli attacchi ai sistemi informatici che mira a contrastare su larga scala richiedendo agli Stati membri di rafforzare le leggi nazionali sulla criminalità informatica e ad introdurre sanzioni penali più severe. Nel 2017 la Commissione ha pubblicato una relazione che valuta in che misura gli Stati membri hanno adottato provvedimenti necessari per conformarsi alla direttiva.
Nel 2011 è stata adottata una direttiva sulla lotta allo sfruttamento sessuale dei bambini online e alla pedopornografia, per meglio affrontare i nuovi sviluppi nell'ambiente online, come la diffusa pratica di presentarsi come minori per attirare minori con lo scopo di abuso sessuale.
Nel 2002, ancora, l'Unione Europea ha adottato una direttiva sulla Privacy, in base alla quale i fornitori di servizi di comunicazione elettronica devono garantire la sicurezza dei loro servizi e mantenere la riservatezza delle informazioni dei clienti. Nel 2017 la Commissione ha proposto di abrogare la direttiva e sostituirla con un

regolamento relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche.
Infine, nel 2001, l'Unione Europea ha adottato una decisione quadro sulla lotta alla frode e alla contraffazione di mezzi di pagamento diversi dai contanti, che definisce i comportamenti fraudolenti che gli Stati membri dell'UE devono considerare reati punibili.
La prima Strategia UE in questo ambito, adottata nel 2013, ha segnato un punto di svolta, ma gli attacchi sempre più dannosi e le crisi internazionali scaturite da eventi occorsi nello spazio cibernetico hanno imposto un nuovo slancio.
I leader dell'UE considerano la riforma della cybersicurezza uno dei principali aspetti in corso di attuazione sul cammino verso il completamento del mercato unico digitale dell'Unione. Di fronte a sfide sempre maggiori in materia di cybersicurezza, l'Unione Europea deve migliorare la consapevolezza e la risposta ai cyberattacchi nei confronti degli Stati membri o delle istituzioni dell'Unione stessa. L' "Internet delle cose" è già una realtà: entro il 2020 sono previsti decine di miliardi di dispositivi digitali connessi.
Si calcola che i cyberattacchi costino all'economia mondiale 400 miliardi di euro ogni anno.

Importante è dire che nel 2015 gli incidenti di sicurezza in tutti i settori industriali sono aumentati del 38%.
L'80% delle società europee ha subito nel 2015 almeno un incidente di cybersicurezza.
L'86% degli europei ritiene che il rischio di reati informatici sia in aumento.
Molte imprese e amministrazioni in tutta l'UE si affidano alle reti e alle infrastrutture digitali per fornire i loro servizi essenziali. Ciò significa che quando si verifica un incidente a carico della sicurezza delle reti e dell'informazione, l'impatto può essere considerevole poiché i servizi vengono compromessi e le imprese non possono lavorare correttamente.
Inoltre, un incidente di questo tipo verificatosi in un paese può avere ripercussioni in altri paesi e persino in tutta l'UE. Oltre a ciò, gli incidenti di sicurezza indeboliscono la fiducia dei consumatori nei sistemi di pagamento online e nelle reti TIC.
Nonostante la crescente minaccia, la consapevolezza e la conoscenza della cybersicurezza sono ancora insufficienti, il 51% dei cittadini europei ritiene di essere disinformato per quanto concerne le minacce informatiche, il 69% delle società non dispone di conoscenze di base sulla loro esposizione ai rischi informatici.
L'8 giugno 2018 il Consiglio Europeo ha concordato l'orientamento generale sul cosiddetto regolamento sulla cybersicurezza, il cui obiettivo è aumentare la cyberresilienza istituendo un quadro europeo di certificazione per prodotti, servizi e processi TIC e potenziare l'attuale Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA).
Il 20 dicembre 2017 le istituzioni dell'UE hanno compiuto un importante passo avanti nel rafforzamento della loro cooperazione nella lotta ai cyberattacchi.
Un accordo interistituzionale ha istituito una squadra permanente di pronto intervento informatico (CERT-EU) per l'insieme delle istituzioni, degli organi e delle agenzie dell'UE.
CERT-EU assicurerà una risposta coordinata dell'UE ai cyberattacchi nei confronti delle sue istituzioni.
Il 20 novembre 2017 il Consiglio "Affari generali" ha chiesto il rafforzamento della cybersicurezza a livello europeo e il potenziamento della cyberresilienza in tutta l'UE.
Il 24 ottobre 2017 il Consiglio "Telecomunicazioni" ha convenuto di definire un piano d'azione per la riforma della cybersicurezza nell'UE. I ministri hanno sottolineato che la sicurezza online è fondamentale per le imprese e i cittadini europei.
Il 19 e 20 ottobre 2017 il Consiglio europeo ha chiesto l'adozione di un approccio comune in materia di cybersicurezza nell'UE in seguito al pacchetto di riforme proposto dalla Commissione europea.

Nel suo pacchetto di riforme del settembre 2017 la Commissione europea ha proposto l'introduzione di sistemi di certificazione a livello di UE per prodotti, servizi e processi TIC, iniziativa volta a consentire la crescita del mercato della cybersicurezza dell'UE.
I sistemi di certificazione consisterebbero, in buona sostanza, in norme, prescrizioni tecniche e procedure, il cui ruolo sarebbe di ridurre la frammentazione del mercato e di eliminare gli ostacoli normativi, instaurando al tempo stesso un clima di fiducia, e riconosciuti in tutti gli Stati membri facilitando gli scambi transfrontalieri delle imprese.
La direttiva dell'Unione Europea sulla sicurezza delle reti e dell'informazione è intesa ad aumentare la cooperazione tra gli Stati membri sulla questione vitale della cybersicurezza.

European Cybercrime Centre - Centro europeo per la criminalità informatica (EC3)
Il 13 settembre 2017 la Commissione Europea ha proposto una nuova direttiva intesa ad aggiornare l'attuale quadro giuridico, col fine di rimuovere gli ostacoli alla cooperazione operativa e di migliorare la prevenzione e l'assistenza delle vittime dei crimini informatici, per fare azioni di contrasto contro la frode e la contraffazione dei mezzi di pagamento diversi dai contanti.
L'EC3 funge da punto focale nella lotta contro la criminalità informatica nell'Unione mettendo in comune le competenze europee in materia di criminalità informatica, per sostenere le indagini dei criminali informatici degli Stati membri e fornire una voce collettiva degli investigatori europei in materia di criminalità informatica tra le forze dell'ordine e la magistratura.
EC3 ha dato un contributo significativo alla lotta contro la criminalità informatica, in quanto è stata coinvolta in decine di operazioni di alto profilo e centinaia di spiegazioni sul supporto operativo in loco che hanno provocato centinaia di arresti ed ha analizzato centinaia di migliaia di file, la stragrande maggioranza dei quali si sono rivelati dannosi.
Mentre è difficile fornire stime attendibili, alcuni rapporti del settore suggeriscono che i costi globali del crimine informatico sono dell'ordine di centinaia di miliardi di euro l'anno.
Ogni anno, l'EC3 pubblica la Internet Threatised Crime Threat Assessment (IOCTA) il suo rapporto strategico di punta sui risultati chiave e le minacce emergenti e gli sviluppi nel crimine informatico.
L'IOCTA, Internet Organised Crime Threat Assessment, dimostra quanto sia ampia e varia la criminalità informatica e come l'EC3 sia una parte fondamentale della risposta di Europol e dell'Unione Europea.
Ma come funziona l'European Cybercrime Center?
EC3 adotta un triplice approccio alla lotta contro la criminalità informatica: analisi forense, strategia e operazioni.
Il Board del programma EC3 la direzione su come raggiungere i propri obiettivi e adempiere ai compiti assegnati ufficialmente basandosi su partnership, responsabilità condivisa e cooperazione con tutti i membri del consiglio di amministrazione.
L'EC3 è composto da due forensics team, digital forensics e document forensics, ognuno dei quali si concentra su propri focus operativi di ricerca e di sviluppo.
Due sono i team strategici:
sensibilizzazione e sostegno, che istituiscono i partenariati e coordinano misure di prevenzione e sensibilizzazione;
strategia e sviluppo, responsabili di analisi strategica, formulazione di misure politiche e legislative, sviluppo della formazione standardizzata.
A livello operativo, l'European Cybercrime Center si concentra su alcuni tipi di reati informatici, crimine cibernetico, sfruttamento sessuale dei minori online, frode di pagamento.

Queste attività sono supportate dal Cyber Intelligence Team (CIT), i cui analisti raccolgono ed elaborano le informazioni relative al crimine informatico da fonti pubbliche, private e aperte e identificano le minacce e i modelli emergenti.
L'EC3 si basa sulla capacità di applicazione della legge di Europol, ma si espande anche in modo significativo su altri fronti, in particolare offrendo supporto operativo e analitico alle indagini degli Stati membri.
Per ciascuna delle tre categorie di criminalità informatica, l'EC3 funge da hub centrale per informazioni e intelligence criminali, sostiene le operazioni e le indagini degli Stati membri offrendo analisi operative, coordinamento, fornisce una varietà di prodotti di analisi strategica che consente di prendere decisioni informate a livello tattico e strategico sulla lotta e la prevenzione della criminalità informatica, fornisce una vasta attività di sensibilizzazione che collega le autorità di contrasto, le quali affrontano la criminalità informatica con il settore privato, il mondo accademico e altri partner non incaricati dall'applicazione della legge, sostiene la formazione e il rafforzamento delle capacità, in particolare per le autorità competenti degli Stati membri, fornisce capacità di supporto tecnico legale e digitale altamente specializzate a indagini e operazioni, rappresenta la comunità di applicazione della legge dell'Unione Europea in aree di interesse comune (requisiti di ricerca e sviluppo, governance di internet e sviluppo di politiche).[1]
Pur senza disconoscere la validità di quanto sinora fatto, l'Unione Europea tende a basare la propria dottrina su tre assi fondamentali:
la resilienza, intesa sia come la capacità degli Stati membri e dell'Ue nel suo complesso, di dotarsi di infrastrutture informatiche o interdipendenti dai sistemi informatici più solidi ed efficaci, sia come la capacità di produrre tecnologie sicure da immettere nel mercato europeo;
la deterrenza, ossia la capacità politico-diplomatica e militare di dissuadere i potenziali avversari, statali e non, dal lanciare un attacco nei confronti degli Stati membri UE e quella operativa di anticipare e/o reagire agli attacchi subiti;
la cooperazione internazionale in ambito cyber, che ha il principale obiettivo di facilitare la cooperazione con i principali stakeholders dello spazio cibernetico, siano essi privati, Stati esterni all'Unione o Organizzazioni internazionali, in primis Onu, Osce e Nato, al fine di mitigare i rischi di misunderstanding ed escalation.
La resilienza è quella condizione indispensabile per garantire una cybersecurity efficace ed efficiente. Dal 2004 l'organo deputato a questo obiettivo nel settore europeo è l'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA), competente per il dialogo tra i Computer Emergency Response Teams nazionali, lo scambio di best practices, l'early warning su minacce specifiche.
Il suo campo di azione, tuttavia, è limitato da un mandato temporaneo che non permette all'Agenzia di agire in chiave strutturata e strategica.
Per questo motivo la Commissione Europea ha proposto di modificare il mandato dell'ENISA da temporaneo a permanente, al fine di garantire una maggiore incidenza dell'Agenzia sia sul fronte interno dell'Unione (nel rapporto orizzontale e verticale tra Bruxelles e gli Stati membri) sia sul fronte esterno (attraverso il coordinamento e il dialogo con i Paesi partner).
L'azione dell'UE non si limita al solo aspetto "security", ma tende anche ad intravedere le potenzialità e le opportunità offerte dall'arena digitale anche da un punto di vista economico.
In questo modo, attraverso un approccio di "sicurezza fin dalla produzione" (security by design) si tenderà a creare un circolo virtuoso basato sugli investimenti in ricerca e sviluppo per prodotti e servizi "certificati" i quali, in ultima analisi, avranno una ricaduta positiva sull'innalzamento del livello di sicurezza informatica dell'UE.
Il cardine dell'azione operativa svolta dall'Unione Europea nel settore cyber è sempre l'obiettivo strategico che porterà ad un innalzamento della consapevolezza dei cittadini e dei policy maker sulle minacce provenienti dal dominio cyber.

Per tale motivo, uno degli aspetti fondamentali che la Commissione intende perseguire è l'avvio di campagne di sensibilizzazione sulla minaccia cibernetica e la necessità di potenziare, tra operatori economici e semplici utenti, la cosiddetta igiene cibernetica (cyber hygiene), così da evitare tutta quella massa di incidenti che si potrebbero evitare con il semplice uso buon senso (ricordiamoci che il malware WannaCry, che tanto ha spaventato nei mesi scorsi, sarebbe stato del tutto innocuo se gli utenti avessero gratuitamente aggiornato i loro sistemi).
Altrettanta attenzione la Commissione ha dedicato al tema delle fake news, le quali costituiscono un serio pericolo per la stabilità dei paesi dell'Unione. Anche in questo caso, uno specifico ruolo è assegnato alla nuova ENISA.
In questo senso, la nuova cyber strategy dell'Unione Europea promuove un approccio proattivo per la gestione degli attacchi cybernetici. Gli strumenti individuati dalla Comunicazione congiunta sono essenzialmente quattro:
la deterrenza,
la difesa attraverso un partenariato pubblico-privato,
la diplomazia in campo cyber,
la cooperazione esterna con partner ed altre organizzazioni.
Per quanto riguarda la materia della creazione di una deterrenza cibernetica efficace nell'Unione Europea, il presupposto fondamentale sarà costituito dalla capacità dell'Unione di dotarsi di una serie di misure capaci di risolvere l'annosa questione dell'attribuzione degli attacchi, cercando quindi di creare una capacità fattuale di "tracciabilità" delle azioni commesse nel dominio cyber.
La deterrenza sarà tanto più efficace quanto più credibile sarà la capacità dell'UE di dotarsi di sistemi di difesa capaci di contrastare e dissuadere gli attacchi informatici.
Ulteriore elemento fondamentale della nuova cyber strategy è poi l'ideazione di un quadro per una risposta diplomatica comune dell'Ue nei confronti delle azioni ostili commesse tramite gli strumenti cyber. Attraverso questo quadro l'Ue mira a strutturare un'azione di prevenzione dei conflitti e mitigazione delle minacce cibernetiche nel breve, medio e lungo periodo, al fine di influenzare il comportamento di eventuali attori aggressivi e contribuire ad una maggiore stabilità delle relazioni internazionali. A tal fine, la risposta diplomatica europea avrà pieno accesso a tutti gli strumenti previsti dalla Common Foreign and Security Policy, incluse, se necessario, misure restrittive e sanzioni.
Infine, l'Unione Europea si impegna a portare avanti in un'ottica di miglioramento le relazioni con i suoi paesi partner, la cooperazione Ue-Nato e il dialogo con le organizzazioni internazionali e regionali. Di particolare interesse, in questo settore, è la volontà dell'Unione Europea di adottare un piano di cooperazione allo sviluppo nel campo della cyber security attraverso programmi di capacity building indirizzati a quei Paesi extra UE che, a causa di inadeguati livelli di sicurezza informatica, possono rivelarsi fattori di rischio per la sicurezza dell'Unione e degli Stati membri. Allo stesso tempo, l'UE riconosce le iniziative di cyber diplomacy e di trust building avviate anche da altri attori internazionali e regionali, come l'Onu e l'Osce, sottolineando come una più efficace diplomazia in questo settore debba basarsi non solo sulle iniziative bilaterali ma anche sui fori multilaterali, al fine di produrre degli strumenti utili per mitigare il rischio di escalation politico-militare dentro e fuori i confini dell'UE.
Secondo un nuovo studio dell'Eurobarometro pubblicato nel mese di maggio, due terzi degli europei pensa che l'uso delle più recenti tecnologie digitali abbia un impatto positivo sulla società, sull'economia e sulle proprie vite.
Uno degli obiettivi principali della Commissione Europea è quello di portare avanti gli aspetti procedurali e i principi sulla rimozione di contenuti illegali, basati sulla trasparenza e protezione dei diritti fondamentali.
In materia di lotta anti-frode informatica, la Commissione Europea mira a rafforzare la cybersicurezza dell'Unione includendo un piano relativo a come rispondere ai cyberattacchi su vasta scala, un centro europeo di ricerca e competenza in materia di cybersicurezza, affiancato da una rete di centri analoghi a livello di Stati membri, una risposta alla criminalità informatica più efficace sul piano del diritto penale attraverso una nuova direttiva volta

a contrastare la frode e la falsificazione dei mezzi di pagamento diversi dai contanti ed il rafforzamento della stabilità globale attraverso la cooperazione internazionale.
L'Unione Europea rafforza di continuo le sue norme in materia di cybersicurezza al fine di combattere la crescente minaccia dei cyber-attacchi e approfittare delle opportunità della nuova era digitale, questo perché norme sempre più "forti" in materia di cybersicurezza consentono l'innovazione e contribuiscono a dare maggiore sicurezza al futuro digitale dell'Europea, e ciò vuol dire dare sicurezza al futuro digitale dell'Europa significa pertanto:
affrontare le minacce alle piattaforme online e consentire loro di apportare un contributo positivo alla società
sostenere le piccole e medie imprese affinché siano competitive nell'economia digitale
investire nell'uso dell'intelligenza artificiale e dei supercomputer in settori quali le cure mediche e l'efficienza energetica.

[1] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3