Tuttavia, la sicurezza informatica rimane una preoccupazione significativa. Le minacce intenzionali comportano lo sfruttamento delle vulnerabilità dell'IA per causare danni, mentre le minacce non intenzionali derivano dai limiti di affidabilità, robustezza e sicurezza dell'IA e dell'apprendimento automatico attuali. metodi. Entrambi i tipi di rischio sottolineano la necessità di solide protezioni nei sistemi AV.

Le minacce alla sicurezza informatica dei veicoli autonomi includono l'hacking remoto, che compromette i sistemi del veicolo, la manipolazione dei sensori che interrompe funzioni critiche come il rilevamento degli ostacoli, la violazione dei dati che espone informazioni sensibili e gli attacchi DoS che degradano le prestazioni o immobilizzano i veicoli.

Le contromisure comprendono sistemi di rilevamento delle intrusioni per monitorare le minacce, crittografia per proteggere l'integrità dei dati, aggiornamenti regolari per risolvere le vulnerabilità e protocolli di autenticazione per impedire l'accesso non autorizzato. L'insieme di queste misure aumenta la sicurezza e la protezione.

Le normative europee e internazionali si sono concentrate sull'abilitazione della mobilità cooperativa, connessa e automatizzata, garantendo al contempo la sicurezza e la cybersecurity. L'Unione Europea ha introdotto diverse strategie, piattaforme e regolamenti, tra cui la strategia per i sistemi di trasporto intelligenti cooperativi del 2016, la piattaforma C-Roads per le attività di implementazione e la Direttiva generale sui veicoli del 2019.
Regolamento sulla sicurezza, che impone sistemi avanzati di assistenza alla guida e stabilisce un quadro giuridico per i veicoli automatizzati e senza conducente.

L'ONU ha stabilito il Regolamento n. 155, che richiede un sistema di gestione della cybersicurezza dei veicoli per identificare, attenuare e prevenire i rischi di accesso non autorizzato, e il Regolamento n. 156, che garantisce procedure adeguate per gli aggiornamenti del software, compresi i controlli di compatibilità e la consegna sicura. Queste misure mirano a salvaguardare i veicoli da attacchi informatici e a mantenere l'integrità del sistema.

La legislazione dell'UE pone l'accento su regole armonizzate per le modifiche al software, la gestione degli accessi remoti non autorizzati e la fornitura di dati diagnostici per la manutenzione. Stabilisce inoltre i requisiti tecnici per i veicoli automatizzati, compresi i sistemi di controllo del conducente, il monitoraggio in tempo reale, le informazioni sulla sicurezza e i registratori di dati sugli eventi, garantendo un funzionamento sicuro e affidabile sulle strade pubbliche.

Internet delle cose

L'Internet degli oggetti (IoT) è inteso come una rete di oggetti fisici e virtuali interconnessi che comunicano tra loro e con l'ambiente circostante utilizzando sensori e tecnologie avanzate di informazione e comunicazione. Consente di rendere autonomi
interazione senza l'intervento umano, creando un sistema che fa da ponte tra il mondo fisico e quello digitale. I sistemi IoT sono strutturati in tre livelli: il **livello di percezione**, che raccoglie i dati attraverso i sensori; il **livello di elaborazione**, in cui i dati vengono analizzati e vengono prese decisioni; **il livello di applicazione**, in cui vengono forniti servizi e funzionalità agli utenti.

L'IoT pone diversi **rischi per la sicurezza** a vari livelli. A livello di **informazioni**, ci si preoccupa dell'integrità dei dati, della privacy e della riservatezza. A livello di **accesso**, i problemi riguardano l'autenticazione, l'autorizzazione e il controllo degli accessi. A **livello funzionale**, le sfide includono la resilienza a guasti o attacchi e la capacità del sistema di auto-organizzarsi e adattarsi alle minacce.

La protezione dei dati nell'IoT è complessa a causa del grande volume e della diversità dei dati raccolti. Le sfide includono la garanzia di trasparenza, l'ottenimento di un consenso valido da parte degli utenti e l'evitare un trattamento dei dati eccessivo o non intenzionale. I rischi per la privacy sono aggravati dalla difficoltà di controllare l'uso dei dati e dal coinvolgimento di molteplici attori, spesso sconosciuti. Le normative europee, come il **Regolamento 1807/2018**, assicurano il libero flusso dei dati proteggendo la privacy attraverso principi come la limitazione delle finalità, i limiti di conservazione e la conformità nei trasferimenti di dati.

Il **Cyber Resilience Act** prevede che i prodotti con elementi digitali rispettino gli standard di cybersecurity per tutto il loro ciclo di vita.
I produttori devono valutare i rischi durante la progettazione, la produzione e la manutenzione, concentrandosi sulla riservatezza, l'integrità e la sicurezza dei dati.
disponibilità (CIA) dei dati. I requisiti di sicurezza includono la minimizzazione dei dati, la resilienza agli attacchi, i principi di progettazione sicura e gli aggiornamenti gratuiti per la gestione delle vulnerabilità. Inoltre, i produttori devono conservare i registri delle attività interne e condividere le informazioni sulla sicurezza con i fornitori di componenti di terze parti per ridurre al minimo i rischi.

La privacy by design e la sicurezza by design prevedono l'inserimento di misure di sicurezza e privacy nel processo di sviluppo fin dall'inizio. Questi approcci garantiscono che i prodotti siano progettati per proteggere i dati e la privacy degli utenti, utilizzando solidi protocolli di sicurezza e assicurando aggiornamenti tempestivi, segnalazione delle vulnerabilità e trasparenza sulle politiche di sicurezza.

La responsabilità per i danni nell'Internet degli oggetti (IoT) è affrontata dal GDPR, che ritiene le parti responsabili del trattamento dei dati, e dalla direttiva sulla responsabilità dei prodotti, che prevede il risarcimento dei danni causati da prodotti difettosi. La proposta di direttiva sulla responsabilità per l'intelligenza artificiale stabilisce regole uniformi per la responsabilità civile relativa ai danni causati dai sistemi di intelligenza artificiale. Questa direttiva mira a garantire
che le vittime di danni causati dall'IA siano tutelate e che le imprese debbano affrontare una minore incertezza giuridica, introducendo al contempo una presunzione di causalità per semplificare le richieste di risarcimento.

Internet delle cose per la salute

L'ecosistema dell'Internet of Things (IoT) comprende dispositivi connessi alle reti tramite sensori, che interagiscono con il mondo fisico e scambiano informazioni in modo autonomo. L'ecosistema è strutturato in tre livelli: il livello di percezione (che include i dispositivi indossabili) e il livello di percezione.
e dispositivi impiantati e ospedali), il livello di elaborazione (che coinvolge i servizi middleware) e il livello di applicazione (che fornisce servizi di alto livello).

Il trattamento dei dati sanitari, come definito dal GDPR, comprende i dati personali relativi alla salute fisica o mentale di un individuo. Il trattamento di categorie speciali di dati richiede una base giuridica specifica, come il consenso, la protezione degli interessi vitali o le finalità di salute pubblica. È necessario implementare misure di sicurezza per proteggere i dati personali dal trattamento non autorizzato o dalla perdita, come indicato nell'articolo 32 del GDPR.

In caso di non conformità, l'Autorità francese per la protezione dei dati ha imposto una multa a un'azienda per non aver protetto i dati medici, evidenziando violazioni in aree quali la crittografia, la migrazione dei dati e la sicurezza dei server. Il regolamento sui dispositivi medici (MDR) definisce i dispositivi medici come prodotti utilizzati per la diagnosi, il trattamento o la prevenzione di malattie. Include il software destinato a scopi medici, sia autonomo che collegato ad altri dispositivi.

I dispositivi IoT con finalità mediche rientrano nel campo di applicazione dell'MDR, mentre quelli che non hanno tale finalità non sono regolamentati, anche se possono raccogliere dati relativi alla salute. L'MDR richiede la certificazione e l'adesione agli standard di sicurezza e i produttori devono segnalare gli incidenti gravi, con tempistiche specifiche in base alla gravità dell'incidente. Le azioni correttive, come richiami o
aggiornamenti del software, e gli utenti devono essere informati tramite avvisi di sicurezza.

I dispositivi medici IoT devono essere conformi sia al GDPR che al MDR. L'interazione tra queste normative solleva dubbi sul fatto che gli organismi nazionali responsabili della conformità all'MDR verifichino anche la conformità al GDPR, in particolare per quanto riguarda le misure di sicurezza richieste da entrambi i quadri normativi.

Il Cyber Resilience Act (CRA) si applica ai prodotti con elementi digitali, compresi software e hardware, ma esclude quelli già definiti come dispositivi medici ai sensi dell'MDR. I prodotti soggetti all'MDR devono soddisfare standard di sicurezza e protezione, mentre i prodotti soggetti al CRA devono soddisfare requisiti di cybersecurity. Il CRA prevede che i prodotti con elementi digitali siano progettati e fabbricati per garantire un livello adeguato di sicurezza informatica prima di essere immessi sul mercato. Devono essere consegnati
senza vulnerabilità note sfruttabili e distribuiti con configurazioni predefinite sicure.

I produttori devono notificare alle autorità competenti, come CSIRT ed ENISA, le vulnerabilità attivamente sfruttate. Le notifiche devono essere effettuate entro tempi rigorosi, tra cui un allarme tempestivo entro 24 ore, una notifica di vulnerabilità entro 72 ore e un rapporto finale entro 14 giorni dopo la disponibilità di misure correttive.

Tra le questioni aperte relative al CRA vi è il coordinamento tra la legislazione generale e quella specifica del settore, in particolare per quanto riguarda la distinzione tra dispositivi medici e sanitari e la questione degli standard generici. C'è anche preoccupazione per il sovraccarico di notifiche, con tempi che si sovrappongono, autorità diverse e requisiti diversi per le notifiche.

Cloud Computing

Secondo il National Institute of Standards and Technology (NIST), un servizio cloud è definito da cinque caratteristiche: self-service su richiesta, ampio accesso alla rete, pooling delle risorse, elasticità rapida e servizio misurato.

I servizi cloud sono classificati in diversi modelli, tra cui Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). Esistono anche diversi tipi di ambienti cloud: cloud privati, comunitari, pubblici e ibridi. I servizi cloud operano a più livelli: dati, applicazioni, rete e host, ognuno dei quali coinvolge risorse diverse, tra cui storage dei dati, elementi di rete, applicazioni e componenti di virtualizzazione.

La cybersecurity nei servizi cloud deve affrontare delle sfide, come la mancata corrispondenza tra la domanda e l'offerta per quanto riguarda le funzioni di cybersecurity. Queste lacune sono spesso legate a responsabilità poco chiare per l'implementazione e il mantenimento delle misure di sicurezza.
Il mercato della cybersecurity coinvolge stakeholder quali fornitori di servizi cloud, utenti finali, ricercatori ed enti normativi. Il rapporto tra cybersecurity e cloud computing è multidimensionale e comprende la sicurezza da, per e all'interno del cloud.

I contratti cloud includono caratteristiche tecniche specifiche, come lo spostamento dell'archiviazione dei dati dai server fisici dell'utente ai sistemi del fornitore, l'uso di infrastrutture condivise (modello multi-tenant) e la dipendenza da Internet per l'accesso ai servizi. I servizi cloud sono tipicamente offerti su base pay-as-you-go, consentendo di scalare in modo flessibile per soddisfare esigenze mutevoli, come l'aggiunta di storage o di potenza di calcolo.

L'operazione di trattamento prevede il trattamento di diverse tipologie di dati personali, tra cui dati di contatto, informazioni mediche, e
dati amministrativi o finanziari. Lo scopo di questo trattamento è quello di fornire servizi di assistenza sanitaria, come diagnosi, trattamento, ricovero e fatturazione, e gli interessati sono i pazienti, i loro parenti, i medici e gli infermieri. I destinatari di questi dati sono i medici, gli infermieri, i reparti amministrativi e contabili, i sistemi sanitari pubblici e i pazienti stessi. In questo contesto, un fornitore di servizi cloud IaaS agisce come responsabile del trattamento dei dati.

Per quanto riguarda le sfide della protezione dei dati, tecniche come la privacy by design, la gestione efficace dei dati, la cancellazione e la portabilità sono considerazioni fondamentali. Le sfide della cybersecurity coinvolgono un'ampia gamma di questioni come il controllo degli accessi, l'audit, l'autorizzazione, la disponibilità e la garanzia di conformità. Altre aree di interesse sono il mantenimento della riservatezza, la sicurezza della catena di fiducia e di responsabilità, la gestione degli incidenti di cybersecurity e la salvaguardia della sicurezza di rete, della privacy e dell'archiviazione, il tutto garantendo trasparenza e sicurezza.
visibilità, oltre a prevenire il ripudio

Architettura della sicurezza informatica nel cloud computing

- **Controllo degli accessi**: Si tratta di meccanismi come l'autenticazione e l'autorizzazione per regolare chi può accedere ai dati e ai sistemi.
- **Crittografia**: Questo processo trasforma i dati in un formato codificato, garantendone la sicurezza sia in fase di archiviazione (a riposo) che di trasmissione (in transito).
- **Backup e ripristino dei dati**: Queste strategie assicurano che i dati possano essere ripristinati in caso di violazione o guasto del sistema. I backup possono essere archiviati separatamente in servizi cloud o in centri dati on-premise.
- **Sicurezza di rete**: Include protezioni come firewall, sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS) e reti private virtuali (VPN) per proteggersi da attacchi informatici e accessi non autorizzati.
- **Conformità**: L'adesione a normative come il GDPR e a standard come il PCI DSS è fondamentale per mantenere una solida sicurezza informatica.

Le sfide della cybersecurity comportano spesso l'utilizzo di strumenti come firewall, IDS/IPS e VPN per proteggere i dati. In un ambiente cloud,
I processi di digital forensics comprendono diverse fasi. L'acquisizione si concentra sulla raccolta di dati ampi, distribuiti ed elastici legati a un incidente o a un'accusa. La conservazione garantisce che gli artefatti digitali rimangano intatti attraverso tecniche come l'imaging, l'hashing e la duplicazione. La fase di esame comporta la revisione dei dati forensi raccolti per informare le analisi successive. L'analisi comporta un esame approfondito, compresa la fusione e la correlazione dei dati, per trarre conclusioni. Infine, la fase di reporting consiste nel presentare e documentare i risultati dell'analisi forense.

DSA

La direttiva sul commercio elettronico (direttiva 2000/31/CE) si applica a tutti i servizi della società dell'informazione (SSI) all'interno dell'UE, compresi gli intermediari online, e mira a garantire il corretto funzionamento del mercato interno. Essa opera secondo il principio del Paese d'origine, consentendo eccezioni limitate solo sulla base di ragioni specifiche e di requisiti procedurali. Gli intermediari sono esenti da responsabilità, anche se ciò non influisce sulle ordinanze dei tribunali. La legge sui servizi digitali (DSA), che ha sostituito la direttiva sul commercio elettronico in materia di responsabilità
esenzioni, si concentra sul miglioramento della sicurezza online, sulla limitazione dei contenuti illegali, sulla promozione della trasparenza e sulla tutela della libertà di parola e dei minori. Si applica a tutti gli intermediari online e ai contenuti illegali, definendo l'illegalità in base al diritto nazionale o dell'UE. La DSA stabilisce obblighi di due diligence per gli intermediari, garantendo che non siano ritenuti responsabili per i contenuti, a condizione che si conformino a requisiti normativi.

Il Digital Services Act (DSA) si basa sulla Direttiva sul commercio elettronico, in particolare attraverso gli articoli 4, 5 e 6, che corrispondono agli articoli 12, 13 e 14 della Direttiva. Questi articoli distinguono tra diversi tipi di fornitori di servizi online, come semplici conduit, caching e servizi di hosting, con responsabilità derivanti da qualsiasi contenuto illegale, indipendentemente dalla sua natura o origine. La DSA introduce nuove disposizioni, tra cui l'articolo 6(3), che affronta la responsabilità nell'ambito della legge sulla protezione dei consumatori e stabilisce eccezioni legate agli obblighi di diligenza.

La Corte di Giustizia dell'Unione Europea (CGUE) sottolinea che i fornitori di servizi Internet (ISP) devono rimanere neutrali ed evitare di assumere un ruolo attivo nei confronti dei contenuti che porterebbe a conoscerli o a controllarli. La clausola del buon samaritano di cui all'articolo 7 del DSA consente ancora esenzioni dalla responsabilità quando vengono adottate misure volontarie per affrontare i contenuti illegali.

In termini di governance, la progettazione delle piattaforme deve dare priorità ai rischi sociali, con un approccio dinamico per identificare e affrontare tali rischi attraverso sistemi come i termini e le condizioni e le scelte algoritmiche. La supervisione è fondamentale e coinvolge
audit indipendenti, supervisione normativa e controllo pubblico attraverso rapporti di trasparenza, accesso ai dati per i ricercatori e consultazioni sulle linee guida.

A livello nazionale, il Coordinatore dei Servizi Digitali (DSC) è responsabile di garantire la conformità e di coordinarsi con le altre autorità, mentre la Commissione europea ha poteri di applicazione diretta sulle piattaforme online molto grandi (VLOP) e sui motori di ricerca online molto grandi (VLOSE). La comunicazione al pubblico delle violazioni non è obbligatoria, a meno che non vi sia un rischio elevato per la sicurezza dei dati.
diritti delle persone e, in questi , può essere utilizzata. La trasparenza delle violazioni dei dati svolge un ruolo importante nel creare fiducia, proteggere la reputazione di un'organizzazione e aumentarne il valore, soprattutto in situazioni come fusioni o acquisizioni.

Legge UE sull'intelligenza artificiale

L'Artificial Intelligence Act (AI Act) dell'UE mira a migliorare il mercato interno e a promuovere l'uso di un'intelligenza artificiale affidabile e incentrata sull'uomo, garantendo al contempo la protezione della salute, della sicurezza, dei diritti fondamentali e dell'ambiente. Il regolamento si applica orizzontalmente a tutti i settori dell'UE ed è direttamente applicabile negli Stati membri. Definisce l'IA come un sistema basato su una macchina progettato per operare
in modo autonomo e con vari livelli di adattabilità, deducendo output come previsioni o decisioni dagli input ricevuti.

La legge affronta diverse problematiche, tra cui le tecniche subliminali, la categorizzazione biometrica e la polizia predittiva, con regolamenti specifici per i sistemi di IA ad alto rischio che potrebbero avere un impatto sulla salute pubblica, sulla sicurezza o sui diritti fondamentali. Questi sistemi ad alto rischio sono elencati negli allegati e la loro portata può essere modificata dalla Commissione europea. Gli obblighi per questi sistemi includono la gestione del rischio, la gestione dei dati e il controllo della sicurezza.
governance, documentazione tecnica, trasparenza, supervisione umana e misure di sicurezza informatica.

La legge sull'IA copre anche i modelli di IA per scopi generali (GPAI), come ChatGPT o GPT-3, con obblighi di trasparenza,
documentazione e gestione del rischio. I modelli con rischi sistemici, tipicamente quelli con una portata significativa o con il potenziale di influenzare la società su larga scala, sono soggetti a requisiti aggiuntivi come la valutazione del modello e i test di cybersecurity.

L'AI Act affronta vari tipi di attacchi ai sistemi di IA, tra cui gli attacchi di avvelenamento, in cui i dati vengono alterati durante l'addestramento per spostare il confine decisionale del modello; gli attacchi avversari, in cui gli input vengono manipolati per spingere le decisioni in modo inappropriato; il furto del modello, che comporta la replica del modello osservando i suoi input e output; e il furto della privacy, in cui i dati di addestramento e
vengono estratti i parametri.

L'articolo 15 della legge sull'IA enfatizza la robustezza e la cybersicurezza dei sistemi di IA ad alto rischio. Questi sistemi devono essere in grado di resistere a errori, guasti o incoerenze e le organizzazioni devono implementare misure tecniche e organizzative adeguate per ridurre i rischi quali output distorti o loop di feedback. La legge richiede anche che i sistemi di IA ad alto rischio siano protetti da manipolazioni non autorizzate da parte di terzi, comprese le misure per affrontare vulnerabilità come l'avvelenamento dei dati, gli esempi avversari e i difetti del modello.

Le sfide includono la garanzia di misure organizzative per la cybersecurity, l'allineamento dei requisiti di cybersecurity e di robustezza e il bilanciamento con le esigenze specifiche dei modelli di IA per scopi generali (GPAI). La legge riconosce che raggiungere la perfetta accuratezza, robustezza, privacy ed equità è tecnicamente impossibile e sottolinea la necessità di strategie di gestione del rischio per bilanciare questi requisiti contrastanti. La documentazione tecnica per i sistemi di IA deve tenere conto di tutti i compromessi fatti quando si implementano soluzioni per soddisfare gli standard della legge.

Sicurezza dei prodotti

La Commissione europea si è concentrata sul miglioramento della cybersecurity dei dispositivi connessi incorporando requisiti minimi di cybersecurity nella legislazione sulla sicurezza dei prodotti, in particolare nell'ambito del Nuovo quadro legislativo (NLF). A partire dal 2019, la Commissione ha iniziato a rivedere direttive come la Radio Equipment Directive (RED) e altri regolamenti sulla sicurezza dei prodotti per includere requisiti essenziali di cybersecurity. Questo fa parte di uno sforzo più ampio per affrontare le vulnerabilità dei prodotti connessi, come gli indossabili, e garantire una cybersicurezza continua durante il loro ciclo di vita.

La Commissione ha inoltre avviato la revisione della direttiva sulla sicurezza generale dei prodotti e della direttiva sulle macchine, proponendo nuovi regolamenti per includere i requisiti di sicurezza informatica. Il problema principale deriva dalle diffuse vulnerabilità dei prodotti con elementi digitali, dall'inadeguatezza delle patch di sicurezza e dall'insufficiente accesso degli utenti alle informazioni sulla sicurezza informatica. I cyberattacchi minacciano sempre più spesso i prodotti hardware e software, mettendo a rischio le organizzazioni e le catene di fornitura.

La proposta di legge sulla resilienza informatica (Cyber Resilience Act, CRA) mira ad affrontare questi problemi garantendo che i produttori migliorino la sicurezza dei prodotti con elementi digitali fin fase di progettazione. L'obiettivo è stabilire un quadro coerente di cybersecurity, migliorare la sicurezza dei prodotti.
trasparenza sulla sicurezza dei prodotti e consentire un utilizzo sicuro sia per le aziende che per i consumatori. Il CRA si applica ai prodotti con elementi digitali collegati a reti o dispositivi, ma esclude alcune categorie, come i dispositivi medici, i prodotti per la sicurezza nazionale e i pezzi di ricambio.

I produttori ai sensi del CRA avranno l'obbligo costante di gestire le vulnerabilità, di segnalare le vulnerabilità sfruttate ai Computer Security Incident Response Teams (CSIRT) e all'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) e di affrontare qualsiasi incidente grave che abbia un impatto sulla sicurezza dei prodotti. Il regolamento enfatizza un approccio proattivo alla sicurezza informatica, garantendo che i prodotti rimangano sicuri per tutto il loro ciclo di vita.

I produttori sono tenuti a valutare e documentare i rischi di cybersecurity per i prodotti con elementi digitali, considerando anche l'uso previsto e prevedibile. Questo processo deve essere aggiornato durante tutto il ciclo di vita del prodotto. I prodotti devono essere progettati per soddisfare gli standard di sicurezza informatica, tra cui configurazioni sicure, protezione da accessi non autorizzati e crittografia di dati personali o sensibili. Le vulnerabilità devono essere identificate, affrontate con aggiornamenti e divulgate pubblicamente una volta apportate le correzioni.
I produttori devono fornire la documentazione tecnica per 10 anni dopo l'immissione del prodotto sul mercato e devono informare gli utenti delle vulnerabilità e delle azioni correttive.

Nella fase di manutenzione, i produttori devono segnalare gli incidenti e le vulnerabilità, con scadenze specifiche per le notifiche e gli aggiornamenti. Se un produttore non informa gli utenti entro i tempi richiesti, possono i Computer Security Incident Response Teams (CSIRT). I produttori devono anche informare i fornitori di componenti sulle vulnerabilità delle parti integrate, compresi i componenti open-source.

Le autorità di sorveglianza del mercato (MSA) assicurano la conformità con il Cyber Resilience Act (CRA), collaborando con enti come ENISA e altre autorità nazionali. Se un prodotto non è conforme, l'MSA può richiedere azioni correttive o richiamare il prodotto. Le sanzioni per la mancata conformità possono essere sostanziali, fino a 15 milioni di euro o al 2,5% del fatturato globale totale del produttore.

Recenti sviluppi nella legislazione sulla criminalità informatica

La risoluzione dell'Assemblea generale delle Nazioni Unite per il 2019 sottolinea la duplice natura delle tecnologie dell'informazione e della comunicazione (TIC) che, se da un lato favoriscono lo sviluppo, dall'altro creano opportunità per le attività criminali, in particolare nel cyberspazio. L'aumento dei crimini informatici minaccia le infrastrutture critiche, le imprese e gli individui. Per combattere questo fenomeno, la risoluzione chiede che a livello internazionale
e propone di creare un comitato per sviluppare una convenzione globale che affronti l'abuso criminale delle TIC. La bozza di convenzione mira a migliorare la prevenzione e il perseguimento dei crimini informatici, a rafforzare la cooperazione internazionale e a sostenere lo sviluppo di capacità, soprattutto nei Paesi in via di sviluppo.

Gli aspetti chiave di questa iniziativa includono il crescente utilizzo delle TIC, la responsabilità dei governi di proteggere la società e le sfide legate all'ottenimento e alla gestione delle prove elettroniche tra le varie giurisdizioni. L'iniziativa sottolinea inoltre la necessità di una cooperazione tra gli Stati e il settore privato, nonché il miglioramento delle procedure legali per la divulgazione dei dati archiviati e la gestione dell'assistenza reciproca in caso di emergenza.

La risoluzione del Parlamento europeo del 2017 sottolinea ulteriormente i danni sociali ed economici causati dalla criminalità informatica, in particolare attraverso la crittografia e il ransomware, ed evidenzia le minacce ai diritti fondamentali e alla stabilità democratica. Chiede definizioni più chiare dei termini legati alla criminalità informatica e una maggiore responsabilità per i fornitori di servizi, concentrandosi al contempo su una migliore cooperazione tra le forze dell'ordine, in particolare nella gestione delle prove elettroniche.

Il "Pacchetto E-Evidence" (Regolamento 2023/1543 e Direttiva 2023/1544) introduce misure per aiutare l'applicazione della legge
ottenere e conservare efficacemente le prove elettroniche, con l'obiettivo di combattere la criminalità informatica. Il pacchetto si concentra sull'adattamento del quadro procedurale all'era di Internet, con i fornitori di servizi che svolgono un ruolo chiave nel sostenere le indagini e le azioni penali. Vengono introdotti strumenti giuridici come l'ordine di produzione e l'ordine di conservazione dell'UE, che impongono ai fornitori di servizi di produrre o conservare le prove elettroniche. Inoltre, il pacchetto garantisce la tutela dei diritti fondamentali imponendo ai fornitori di designare rappresentanti legali nell'UE.

La legge 90/2024 affronta sia la cybersecurity che la criminalità informatica, con un approccio tradizionale alla criminalità informatica ma con un aumento delle sanzioni e un ampliamento delle procedure per far fronte a problemi crescenti, come il ransomware. La legge introduce anche la responsabilità delle imprese per i crimini informatici e ridefinisce alcuni reati. Le disposizioni della legge riflettono gli sforzi più ampi dell'UE, tra cui la direttiva EUNIS2 del 2022, che sottolinea la necessità per gli Stati membri di segnalare i crimini informatici come il ransomware e pone l'accento sul coordinamento tra le autorità.

La legge rafforza le sanzioni per il ransomware, criminalizzandolo ed estendendo i regimi procedurali speciali per i crimini informatici che colpiscono le infrastrutture critiche.

Gli attacchi ransomware sono diventati sempre più frequenti e gravi, coinvolgendo diversi metodi di attacco, richieste di riscatto e l'uso di tecnologie come le criptovalute. L'UE e i contesti globali sottolineano la necessità di migliori risposte legali a questi crimini, con il Processo di Oxford che sostiene la tutela dei diritti umani e la criminalizzazione del ransomware. La legge italiana criminalizza il ransomware e la cyberestorsione, imponendo pene detentive e multe. La legge prevede anche l'obbligo di segnalazione delle violazioni di dati e degli incidenti di ransomware, in linea con gli sforzi legislativi internazionali, come il disegno di legge statunitense sui pagamenti di ransomware.

Internet degli oggetti e responsabilità

L'interazione tra IoT, IA e responsabilità rivela sfide tecniche e legali significative. I sistemi IoT sono versatili ma spesso centralizzati e dipendenti dal cloud, con una potenza di calcolo periferica limitata, che ostacola le misure di crittografia e protezione. Problemi come la congestione del traffico internet, il diluvio di dati e l'inquinamento indotto dalla tecnologia aggravano questi problemi.

La responsabilità nei sistemi IoT abbraccia molteplici scenari, dagli obblighi precontrattuali alle responsabilità contrattuali ed extracontrattuali. Le direttive UE (2019/770 e 2019/771) hanno introdotto regole per i beni che incorporano elementi digitali, come i dispositivi IoT, tra cui obblighi di conformità, inversione dell'onere della prova e rimedi per la non conformità.

La legge sull'IA introduce un'ampia definizione di IA, classificando i sistemi come vietati, ad alto rischio o di uso generale. IA ad alto rischio
I sistemi IoT sono soggetti a obblighi rigorosi, tra cui la trasparenza, la supervisione e la certificazione. Tuttavia, la sovrapposizione tra le normative sull'IA e la responsabilità dei prodotti IoT rimane poco chiara, soprattutto per i sistemi integrati come gli strumenti medici.

La revisione della direttiva UE sulla responsabilità da prodotto include il software e l'IA, enfatizzando gli standard di sicurezza e conformità del prodotto. Le nuove norme riguardano la divulgazione delle prove e introducono presunzioni confutabili di causalità per i danni legati all'IA, con requisiti più severi per i sistemi ad alto rischio. I futuri adeguamenti normativi mireranno a colmare le lacune tecnologiche e legali, garantendo l'armonizzazione con quadri normativi come il GDPR e le leggi sulla cybersicurezza. Le proposte normative sono ancora in evoluzione, con particolare attenzione all'ibridazione dell'IoT con l'IA, la blockchain e i gemelli digitali.