UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

Cybersecurity e protezione dei dati: scenari normativi, casi reali e prospettive future

Giulia Torella

0357219

Anno accademico 2024/2025

INDICE

ABSTRACT

Nell'era della trasformazione digitale, la società moderna intreccia sempre più la propria quotidianità con il mondo digitale. Il cosiddetto cyberspazio è oggi il luogo virtuale in cui utenti, dispositivi e sistemi informatici interagiscono attraverso reti telematiche, come Internet, per scopi personali, professionali, economici e istituzionali. In questo ambiente interconnesso, privo di confini fisici, si generano opportunità straordinarie ma al tempo stesso la sicurezza delle informazioni sta diventando una delle principali sfide per gli individui, le imprese e le istituzioni pubbliche. La progressiva digitalizzazione di servizi, dati e comunicazioni ha reso le infrastrutture informatiche sempre più esposte a rischi e attacchi cibernetici, con conseguenze potenzialmente gravi sia sul piano economico che su quello della tutela dei diritti fondamentali.

In questo contesto si inserisce il diritto digitale e, più in particolare, il tema della cybersecurity, ovvero l'insieme di misure tecniche, organizzative e giuridiche volte a proteggere sistemi, reti e dati da accessi non autorizzati, danni, furti o distruzioni. Ogni giorno miliardi di utenti si connettono a Internet, generando enormi quantità di dati – il cosiddetto *footprint digitale* – e rendendo il cyberspazio una vera e propria estensione della realtà. Proprio per questo motivo, la protezione delle infrastrutture digitali, dei dati personali e della privacy è diventata una priorità non solo tecnica, ma anche giuridica e politica, che coinvolge il diritto alla privacy, la protezione dei dati personali e la responsabilità degli operatori digitali. Gli attacchi informatici – come i ransomware o il phishing – non colpiscono soltanto i singoli cittadini, ma anche aziende e istituzioni pubbliche, provocando danni economici e sociali considerevoli.

Per far fronte a queste sfide, l'Unione Europea ha sviluppato nel tempo un quadro normativo sempre più ampio e strutturato. Sono state introdotte normative specifiche, come la Direttiva NIS2, il Cyber Resilience Act, il Digital Operational Resilience Act (DORA), il Regolamento eIDAS, il Data Act, l'AI Act e il Regolamento generale sulla protezione dei dati (GDPR). In Italia, tali norme sono state in parte recepite e attuate attraverso interventi specifici, come la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e l'adozione del Piano Nazionale di Cybersecurity.

Questo elaborato si propone di analizzare il fenomeno della cybersecurity dal punto di vista giuridico, con un focus sul quadro normativo europeo e italiano. Dopo aver illustrato le principali norme in materia, verranno presentate le forme di attacco informatico più comuni, come il ransomware e il phishing, per poi passare all'analisi di due casi concreti: l'attacco informatico al sistema sanitario della Regione Lazio nel 2021 e il fenomeno delle truffe tramite falsi messaggi di corrieri. Infine, si affronterà il rapporto sempre più stretto tra intelligenza artificiale e cybersicurezza, evidenziando come l'IA possa rappresentare sia una risorsa che una minaccia nel contesto digitale contemporaneo.

1. Quadro normativo in materia di cybersecurity

1.1 La normativa europea

La crescente dipendenza da tecnologie digitali ha spinto l'Unione Europea a sviluppare un quadro normativo robusto e articolato per garantire un alto livello di cybersecurity, ovvero la protezione dei sistemi informativi, dei dati, delle reti e delle infrastrutture critiche da minacce informatiche sempre più complesse e frequenti. L'approccio europeo mira a tutelare non solo la sicurezza tecnologica, ma anche i diritti fondamentali dei cittadini, l'integrità del mercato unico digitale e la solidità dei settori strategici. Tra le principali normative europee che costituiscono l'architettura giuridica della cybersecurity si possono individuare le seguenti:

- *Direttiva NIS2 (Network and Information Security Directive)*: entrata in vigore nel gennaio 2023, rappresenta l'evoluzione della precedente direttiva NIS del 2016. Essa ha l'obiettivo di rafforzare ulteriormente la sicurezza delle reti e dei sistemi informativi nei settori essenziali (energia, trasporti, sanità, finanza, ecc.) e nei servizi digitali. Tra le novità principali introdotte dalla NIS2 vi sono: un campo di applicazione più esteso, che coinvolge più soggetti pubblici e privati; obblighi più stringenti in termini di gestione del rischio e notifica degli incidenti; sanzioni più severe in caso di inadempienze; maggiore cooperazione tra Stati membri e ruolo potenziato dell'ENISA (Agenzia dell'UE per la cybersicurezza).
- *Cyber Resilience Act (CRA):* ancora in fase di approvazione definitiva, è una proposta legislativa che mira a introdurre requisiti minimi di cybersecurity per tutti i prodotti con elementi digitali immessi nel mercato europeo. Ciò include dispositivi connessi (Internet of Things), software e hardware. Il CRA stabilisce obblighi per i produttori lungo l'intero ciclo di vita del prodotto (dalla progettazione alla manutenzione), e mira a colmare le lacune in materia di sicurezza del prodotto digitale.
- *Regolamento DORA (Digital Operational Resilience Act):* adottato nel 2022 ed entrato in vigore nel 2023, è rivolto specificamente al settore finanziario, con lo scopo di rafforzare la resilienza operativa digitale di banche, assicurazioni, mercati e fornitori di servizi ICT. DORA impone alle istituzioni finanziarie di: adottare solidi piani di gestione del rischio ICT; notificare tempestivamente incidenti gravi; sottoporre fornitori terzi critici (es. cloud provider) a supervisione normativa.
- *Regolamento eIDAS (electronic IDentification, Authentication and trust Services)*: introdotto nel 2014 e recentemente aggiornato con la proposta eIDAS 2.0, ha l'obiettivo di fornire un quadro giuridico per l'identità digitale e i servizi fiduciari all'interno dell'UE. Con eIDAS

2.0, l'Unione introduce il Portafoglio europeo di identità digitale, uno strumento che consentirà ai cittadini e alle imprese di autenticarsi e condividere documenti digitali in sicurezza in tutti i paesi membri, contribuendo a rafforzare la fiducia nei servizi online.

- *Data Act (2023):* è una normativa fondamentale nel contesto della strategia europea sui dati. Approvato nel 2023, il regolamento disciplina l'accesso, l'uso e la condivisione dei dati non personali generati da dispositivi connessi e servizi digitali. Pur non trattando direttamente la cybersecurity, il Data Act si inserisce nel contesto della protezione delle informazioni sensibili e del controllo sui dati, con implicazioni anche in materia di sicurezza informatica.
- *AI Act:* adottato nel 2024, è la prima legge al mondo a regolamentare in modo sistemico i sistemi di intelligenza artificiale. L'obiettivo è garantire che l'IA sviluppata e utilizzata nell'UE sia sicura, trasparente, non discriminatoria e rispetti i diritti fondamentali. Alcune categorie di IA ad alto rischio – come quelle usate nella sorveglianza biometrica o nella gestione delle infrastrutture critiche – sono sottoposte a obblighi rigorosi. L'AI Act ha implicazioni dirette sulla cybersecurity, sia per i rischi legati all'utilizzo malevolo dell'IA, sia per il ruolo dell'IA nei sistemi di difesa informatica.

1.2 Le norme applicabili in Italia

L'Italia ha recepito e integrato nel proprio ordinamento giuridico il quadro normativo europeo in materia di cybersecurity, adattandolo al contesto nazionale e rafforzando le capacità di prevenzione, gestione e risposta alle minacce informatiche. La crescente rilevanza della sicurezza informatica ha spinto le istituzioni italiane a dotarsi di strumenti legislativi e organizzativi dedicati, finalizzati a tutelare la sicurezza digitale di cittadini, imprese e pubblica amministrazione.

Uno degli snodi fondamentali della strategia italiana in materia di cybersecurity è rappresentato dalla creazione, nel 2021, dell'*Agenzia per la Cybersicurezza Nazionale (ACN)*. L'ACN ha il compito di coordinare le attività di difesa e protezione del sistema informativo nazionale, promuovere la cultura della sicurezza informatica e supportare le istituzioni pubbliche e private nella gestione del rischio cyber. Attraverso l'ACN, l'Italia mira a garantire un approccio coordinato e integrato che coinvolga tutti i settori strategici, dalle infrastrutture critiche ai servizi essenziali.

Dal punto di vista normativo, l'Italia ha adottato diverse misure per conformarsi agli standard europei. Tra le principali, si possono citare:

- *Decreto Legislativo n. 65/2018*, che ha recepito la Direttiva NIS (Network and Information Security), ponendo le basi per la sicurezza delle reti e dei sistemi informativi nel paese. Tale

decreto ha introdotto obblighi specifici per gli operatori di servizi essenziali e i fornitori di servizi digitali, prevedendo misure di gestione del rischio e l'obbligo di notificare incidenti rilevanti all'autorità competente.

- *Piano Nazionale di Cybersecurity (PNC)*, aggiornato periodicamente dal Governo italiano, che definisce strategie, obiettivi e azioni per rafforzare la sicurezza informatica a livello nazionale. Il PNC coinvolge diversi ministeri e agenzie, ponendo particolare attenzione alla protezione delle infrastrutture critiche, alla formazione specialistica e allo sviluppo di capacità operative.
- *Normative specifiche per la Pubblica Amministrazione Digitale*, che includono misure per la sicurezza dei dati e dei sistemi pubblici, con particolare riferimento al Codice dell'Amministrazione Digitale (CAD) e ai suoi aggiornamenti, volti a garantire la resilienza informatica della PA.
- *Misure in materia di protezione dei dati personali*, attuate in conformità al GDPR, che impongono obblighi stringenti alle pubbliche amministrazioni e ai privati in merito alla sicurezza dei dati trattati, con particolare riguardo alla prevenzione di data breach e all'adozione di policy di sicurezza informatica.

Inoltre, l'Italia ha avviato iniziative di collaborazione internazionale e partenariati pubblico-privati per rafforzare la propria capacità di risposta alle minacce cyber. Questi sforzi si traducono anche in programmi di formazione, sensibilizzazione e sviluppo di tecnologie avanzate per la cybersecurity.

Nonostante i progressi, permangono sfide significative, come la carenza di personale specializzato, la complessità della gestione della sicurezza in ambiti molto diversificati e l'evoluzione continua delle minacce informatiche. Per questo motivo, l'azione legislativa e strategica italiana continua ad evolvere, in linea con le innovazioni tecnologiche e con gli orientamenti europei.

1.3 Cybersecurity e il c.d. GDPR (Regolamento UE 2016/679)

La crescente digitalizzazione e la conseguente diffusione di dati personali in ambito aziendale e istituzionale hanno reso sempre più urgente la necessità di un quadro normativo efficace per la tutela della privacy e della sicurezza informatica. In questo scenario, il Regolamento Generale sulla Protezione dei Dati (GDPR, Regolamento UE 2016/679), entrato in vigore nel maggio 2018, rappresenta una pietra miliare per la protezione dei dati personali nell'Unione Europea. Il GDPR non solo rafforza i diritti degli individui rispetto ai propri dati, ma impone anche alle organizzazioni obblighi stringenti per garantire un livello adeguato di sicurezza informatica.

L’articolo 32 del GDPR è particolarmente rilevante in ambito cybersecurity, poiché obbliga titolari e responsabili del trattamento a mettere in atto misure tecniche e organizzative adeguate per proteggere i dati personali da accessi non autorizzati, perdita, alterazione o divulgazione illecita. Queste misure devono essere proporzionate al rischio, considerando la natura dei dati, il contesto operativo e lo stato dell’arte tecnologico. Tra gli strumenti previsti rientrano l’uso di crittografia, controlli di accesso rigorosi, monitoraggio continuo delle reti e sistemi, nonché procedure di backup e disaster recovery. L’articolo 25 introduce il principio di “privacy by design e by default”, che impone alle organizzazioni di incorporare fin dalla progettazione dei sistemi e dei processi i principi di minimizzazione dei dati e protezione della privacy, al fine di ridurre al minimo i rischi per gli interessati. Un altro aspetto centrale del GDPR è l’obbligo di notificare tempestivamente le violazioni dei dati personali (data breach). Ai sensi dell’articolo 33, il titolare del trattamento deve comunicare la violazione all’autorità di controllo competente entro 72 ore dal momento in cui ne viene a conoscenza, mentre l’articolo 34 prevede che, in caso di rischio elevato per i diritti e le libertà degli interessati, debba essere effettuata anche una comunicazione diretta agli stessi. Questa trasparenza mira a mitigare i danni e a incentivare le organizzazioni a migliorare continuamente le proprie strategie di cybersecurity. Inoltre, l’articolo 35 prevede l’obbligo di condurre valutazioni d’impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA) per i trattamenti che presentano rischi elevati, contribuendo così a prevenire violazioni e a pianificare adeguate misure di sicurezza.

Il GDPR ha quindi contribuito a elevare la cybersecurity da semplice funzione tecnica a elemento chiave della governance aziendale e della compliance normativa. L’integrazione delle politiche di sicurezza informatica con le disposizioni del regolamento richiede un approccio multidisciplinare, che coinvolga non solo esperti IT, ma anche figure legali, manageriali e di risk management. Nonostante i progressi, molte organizzazioni incontrano difficoltà nell’adeguarsi pienamente alle richieste del GDPR, a causa di risorse limitate, complessità tecniche e mutevoli scenari delle minacce informatiche. Tuttavia, il regolamento rappresenta uno strumento imprescindibile per promuovere una cultura della sicurezza digitale e per rafforzare la fiducia di cittadini, clienti e partner.

In conclusione, la sinergia tra cybersecurity e GDPR è fondamentale per garantire una protezione efficace dei dati personali in un mondo sempre più connesso e vulnerabile, creando un ambiente digitale più sicuro, chiaro e rispettoso dei diritti fondamentali.

2. Le tipologie di attacco cyber più comuni

Gli attacchi informatici rappresentano la principale minaccia alla sicurezza digitale, colpendo ogni giorno aziende, istituzioni e singoli utenti. Le tecniche di attacco sono in continua evoluzione e si adattano alle nuove tecnologie e vulnerabilità, ma alcune tipologie risultano particolarmente diffuse e pericolose. In questo capitolo verranno analizzate due delle forme di attacco più comuni e insidiose: il ransomware e il phishing, entrambe responsabili di ingenti danni economici e violazioni della privacy.

2.1 Il ransomware

Il ransomware è una tipologia di malware che, una volta penetrato in un sistema informatico, blocca o cifra i dati presenti, rendendoli inaccessibili al legittimo proprietario. Per sbloccare i dati, gli attaccanti chiedono un riscatto economico, solitamente in criptovalute, garantendo (o promettendo) la restituzione dell'accesso ai dati una volta effettuato il pagamento. Questo tipo di attacco si è diffuso rapidamente negli ultimi anni per la sua efficacia nel paralizzare aziende, enti pubblici e infrastrutture critiche. I ransomware possono essere veicolati attraverso e-mail di phishing, vulnerabilità non aggiornate nei software o accessi remoti non protetti. Una volta infiltrato nel sistema, il ransomware cifra i file con algoritmi di crittografia avanzata e mostra una schermata con le istruzioni per il pagamento. I ransomware più recenti adottano un approccio chiamato **"**double extortion**"**: oltre a cifrare i dati, minacciano di pubblicarli sul dark web se il pagamento non viene effettuato. Gli effetti di un attacco ransomware possono essere devastanti, causando interruzioni operative, perdite finanziarie ingenti e danni reputazionali. La lotta contro il ransomware richiede non solo strumenti tecnologici di difesa e backup regolari, ma anche una solida preparazione organizzativa e normativa, che includa la notifica tempestiva degli incidenti e la cooperazione tra enti pubblici e privati.

2.2 Il phishing e le sue varianti

Il phishing è una tecnica di ingegneria sociale che mira a ingannare l'utente per fargli fornire informazioni sensibili, come credenziali di accesso, dati bancari o informazioni personali. Gli attaccanti si spacciano per entità affidabili (banche, servizi online, aziende). Il phishing può avvenire tramite: e-mail apparentemente provenienti da mittenti legittimi; SMS (*smishing*) con link fraudolenti; chiamate vocali (*vishing*) in cui il truffatore si finge un operatore bancario; finti siti web identici a quelli ufficiali, usati per carpire credenziali. Negli ultimi anni le varianti del phishing sono diventate sempre più sofisticate. Tra queste si annoverano il *spear phishing*, attacchi mirati a specifiche persone o organizzazioni, e il *whaling*, rivolto a figure di alto profilo come dirigenti

aziendali o politici. Un'altra variante diffusa è il *pharming*, che indirizza gli utenti verso siti web falsi, imitazioni di quelli originali, per sottrarre dati. Il phishing rappresenta una minaccia estremamente diffusa perché sfrutta la vulnerabilità umana più che quella tecnologica, rendendo indispensabile l'educazione digitale e la sensibilizzazione degli utenti per ridurre il rischio. Sebbene tecnologie come l'autenticazione multifattoriale e i filtri anti-phishing siano efficaci, la conoscenza e l'attenzione dell'utente rimangono l'elemento di protezione più importante. Ad oggi, secondo i dati del Rapporto Clusit 2024, il phishing rappresenta oltre il 40% degli attacchi rilevati in Italia, con un aumento costante sia in termini di volume che di successo. Le campagne più comuni includono: finti avvisi di pacchi da corrieri (DHL, Poste, Amazon), comunicazioni bancarie false, messaggi da finti portali (INPS, Agenzia delle Entrate, SPID).

In conclusione, le tipologie di attacco informatico analizzate – ransomware e phishing – evidenziano la natura mutevole e insidiosa delle minacce digitali contemporanee. Queste forme di attacco, seppur differenti nelle modalità e negli obiettivi, sono accomunate dalla capacità di sfruttare le vulnerabilità tecnologiche e, soprattutto, quelle umane. Ransomware e phishing rappresentano oggi le due minacce più pervasive nel panorama cyber. Mentre il ransomware punta a un guadagno immediato tramite estorsione, il phishing agisce spesso come porta d'ingresso per attacchi più complessi. La loro diffusione è favorita dalla scarsa alfabetizzazione digitale e dalla difficoltà, per utenti e organizzazioni, di distinguere il legittimo dal fraudolento. In un contesto normativo sempre più attento, la prevenzione, la formazione e una risposta coordinata tra pubblico e privato sono le armi principali per affrontare queste minacce in modo efficace. A conferma dell'attualità di questi attacchi, nel prossimo capitolo verranno esaminati due casi concreti che hanno avuto un forte impatto sulla società italiana, mettendo in luce le conseguenze reali delle minacce cyber e le risposte messe in atto dalle istituzioni.

3. Analisi di casi di studio

Per comprendere pienamente le implicazioni pratiche della cybersecurity e l'efficacia – o la mancanza – delle misure di prevenzione e risposta, è utile analizzare alcuni casi concreti di attacchi informatici avvenuti in Italia. Gli episodi che seguono permettono di osservare da vicino come si manifestano le minacce cyber più comuni, quali sono le vulnerabilità sfruttate dagli attaccanti e quali conseguenze possono derivarne per cittadini, aziende e istituzioni pubbliche. In particolare, verranno approfonditi due esempi emblematici: l'attacco ransomware che ha colpito il sistema sanitario della Regione Lazio nel 2021, paralizzando servizi fondamentali durante la pandemia da COVID-19, e la diffusione delle truffe tramite falsi messaggi di corrieri, un caso di phishing particolarmente insidioso e diffuso che

ha coinvolto migliaia di utenti. Entrambi i casi evidenziano non solo l'aspetto tecnico degli attacchi, ma anche le criticità organizzative e le lacune in termini di consapevolezza e formazione.

3.1 L'attacco al sistema sanitario della Regione Lazio (2021)

Nel mese di agosto 2021, la Regione Lazio è stata colpita da un attacco informatico di tipo ransomware che ha avuto conseguenze significative sul funzionamento del sistema sanitario regionale, in particolare durante un periodo già critico a causa dell'emergenza sanitaria da COVID-19. L'attacco ha paralizzato il Centro di Elaborazione Dati (CED) della Regione, rendendo temporaneamente inaccessibili diversi servizi digitali essenziali, tra cui il portale per la prenotazione dei vaccini, le agende sanitarie, i sistemi di gestione delle cartelle cliniche elettroniche e le comunicazioni tra medici di base e strutture ospedaliere.

Secondo le ricostruzioni ufficiali, gli hacker sono riusciti ad accedere ai sistemi regionali sfruttando una vulnerabilità legata a credenziali compromesse di un dipendente, probabilmente ottenute attraverso tecniche di phishing o tramite l'abuso di accessi da remoto non adeguatamente protetti (Remote Desktop Protocol - RDP). L'attacco è avvenuto durante il fine settimana, una scelta strategica che ha permesso ai criminali di operare senza essere immediatamente rilevati.

Il malware installato ha provveduto alla cifratura dei dati sensibili, impedendo l'accesso ai file e costringendo gli amministratori di sistema a bloccare l'intera infrastruttura per tentare di contenere la diffusione del danno. Le autorità regionali hanno dichiarato di non aver ricevuto richieste di riscatto formali, ma si è parlato di un'operazione riconducibile a gruppi internazionali attivi nel cybercrime.

Questo attacco ha suscitato profonda preoccupazione nell'opinione pubblica per almeno tre ragioni principali: il bersaglio perché colpire il sistema sanitario significa mettere a rischio non solo l'efficienza amministrativa, ma anche la salute e la sicurezza dei cittadini; la tempistica perché l'attacco si è verificato nel pieno della campagna vaccinale anti-COVID-19, ritardando la gestione degli appuntamenti e complicando le operazioni di tracciamento sanitario; la vulnerabilità del sistema pubblico perché l'evento ha evidenziato come molte infrastrutture digitali della pubblica amministrazione non fossero sufficientemente aggiornate e protette rispetto alle minacce informatiche contemporanee.

In risposta all'incidente, la Regione Lazio ha avviato una serie di azioni correttive, tra cui:

- L'adozione di nuovi sistemi di autenticazione multifattoriale per il personale;
- L'aggiornamento delle misure di backup e disaster recovery;
- La cooperazione con l'Agenzia per la Cybersicurezza Nazionale (ACN) per rafforzare il monitoraggio e la protezione dei sistemi critici.

L'attacco è diventato un caso emblematico di cyberattacco alle infrastrutture critiche e ha contribuito ad accelerare il dibattito politico e giuridico sulla necessità di un sistema nazionale di difesa cibernetica integrata. Inoltre, ha mostrato come il concetto di "sicurezza sanitaria" oggi non possa prescindere dalla sicurezza digitale.

3.2 Il phishing tramite falsi messaggi di corrieri

Il secondo caso analizzato riguarda un fenomeno in costante crescita in Italia e nel mondo: gli attacchi di phishing basati su falsi messaggi di corrieri. Questo tipo di attacco sfrutta il comportamento comune dei consumatori digitali – l'acquisto frequente online – e si serve di tecniche di ingegneria sociale per spingere gli utenti a cliccare su link fraudolenti, scaricare malware o fornire dati personali.
Il modus operandi è semplice ma estremamente efficace: l'utente riceve un SMS o un'e-mail apparentemente proveniente da un corriere noto, come DHL, Amazon, Poste Italiane o UPS. Il messaggio afferma che c'è un pacco in attesa di consegna, o che è necessario pagare una tassa doganale per riceverlo. Il messaggio contiene un link a un sito web contraffatto, visivamente identico all'originale, dove l'utente è invitato a inserire dati bancari, credenziali o addirittura a scaricare un'app (che in realtà è un trojan o uno spyware).
Un caso documentato nel Rapporto Clusit 2024 segnala che nel solo anno 2023, più del 40% degli attacchi registrati in Italia apparteneva a questa categoria. Durante periodi ad alta intensità commerciale – come il Black Friday, il Natale o il Prime Day – si è registrato un vero e proprio boom di questi tentativi fraudolenti, con campagne anche mirate per specifiche aree geografiche.
L'efficacia di questi attacchi è dovuta a vari fattori:

- Il realismo dell'interfaccia grafica: i siti fraudolenti sono creati per essere quasi indistinguibili da quelli originali;
- La fretta dell'utente medio, che tende a cliccare impulsivamente;
- La fiducia nei marchi coinvolti, che rende più difficile riconoscere l'inganno;
- La carenza di educazione digitale, soprattutto tra le fasce meno giovani della popolazione.

In alcuni casi, i link conducono a malware bancari, che registrano le digitazioni (keylogger) o rubano i codici OTP inviati via SMS, svuotando conti correnti o accedendo ad account digitali.
Le forze dell'ordine italiane e le autorità competenti (es. Polizia Postale, Garante Privacy) hanno avviato diverse campagne di sensibilizzazione, e anche le aziende di logistica hanno collaborato inviando alert ai propri clienti. Tuttavia, l'alto grado di automazione di questi attacchi e la possibilità di generare centinaia di migliaia di messaggi in pochi secondi li rendono difficili da contenere.
Questo caso dimostra l'efficacia distruttiva degli attacchi low-tech ma ad alto impatto e la necessità, oggi più che mai, di un'alfabetizzazione digitale diffusa. Anche qui, le normative europee – come il

GDPR e la Direttiva NIS2 – impongono obblighi ai fornitori di servizi digitali per proteggere gli utenti, ma la prima linea di difesa resta il cittadino.

4. Evoluzione della cybersecurity a seguito dell'avvento dell'IA

Negli ultimi anni, l'intelligenza artificiale (IA) si è affermata come una tecnologia chiave nella trasformazione digitale globale, con un impatto sempre più rilevante anche nel campo della cybersecurity. L'IA, intesa come l'insieme di tecniche e algoritmi capaci di simulare alcune capacità cognitive umane (come apprendere, analizzare e prendere decisioni), offre strumenti innovativi sia per rafforzare la sicurezza informatica, sia – paradossalmente – per minacciarla.

4.1 L'IA come strumento di difesa

Dal punto di vista difensivo, l'IA consente un'evoluzione significativa delle strategie di cybersecurity, superando i limiti dei sistemi tradizionali basati su regole fisse e approcci reattivi. I principali ambiti di applicazione includono:

- Rilevamento delle minacce (threat detection): gli algoritmi di machine learning possono analizzare grandi quantità di dati di rete in tempo reale e identificare comportamenti anomali o potenzialmente dannosi, anche se non corrispondono a modelli noti di attacco. Questo approccio si basa su tecniche di analisi comportamentale e modelli predittivi.
- Risposta automatizzata agli incidenti: sistemi di IA possono essere utilizzati per attivare risposte automatiche a incidenti informatici (come l'isolamento di un dispositivo compromesso), riducendo i tempi di reazione e limitando i danni.
- Analisi e gestione delle vulnerabilità: l'IA può essere impiegata per monitorare costantemente le infrastrutture digitali, identificando punti deboli e suggerendo azioni correttive prima che possano essere sfruttate da un attaccante.
- Filtraggio avanzato di e-mail e contenuti dannosi: le soluzioni antiphishing e antimalware basate su IA riescono a riconoscere contenuti malevoli anche quando camuffati o scritti in modo ingannevole, grazie alla comprensione semantica e all'analisi del contesto.
- *Cyber Threat Intelligence (CTI)*: la raccolta e l'analisi automatica di dati da fonti aperte e dal dark web permette di prevedere nuove minacce, identificare gruppi di attacco e migliorare la preparazione delle difese.

Un esempio concreto in questo ambito è rappresentato dalla tecnologia sviluppata da *Darktrace*, un'azienda britannica leader nella cybersecurity. Il suo sistema basato su IA si ispira al sistema immunitario umano e consente di rilevare in tempo reale attività sospette all'interno delle reti

aziendali. Nel 2022, Darktrace ha contribuito a fermare un attacco ransomware contro un ospedale europeo: l'algoritmo ha rilevato l'anomalia e ha isolato il dispositivo compromesso, impedendo la cifratura di oltre 500.000 documenti clinici. Questo caso dimostra il potenziale dell'intelligenza artificiale nel rafforzare la resilienza operativa e nel salvaguardare asset critici come i dati sanitari.

4.2 I rischi dell'IA nella cybersecurity

Nonostante le sue potenzialità, l'IA rappresenta anche una nuova frontiera del rischio informatico. Gli attaccanti stanno già iniziando a sfruttare strumenti di intelligenza artificiale per rendere più sofisticati e mirati i propri attacchi. Tra i principali rischi emergenti vi sono:

- Attacchi automatizzati: l'IA consente la creazione di malware capaci di adattarsi e modificare il proprio comportamento per evitare i sistemi di rilevamento. Questi software possono condurre ricognizioni automatizzate, scegliere le vulnerabilità più efficaci da sfruttare e persino modificare la propria firma digitale.
- Deepfake e manipolazione delle informazioni: le tecnologie di generazione video e audio basate su IA, come i deepfake, possono essere utilizzate per frodi informatiche (es. impersonificazione di dirigenti aziendali) o campagne di disinformazione, con impatti gravi sulla sicurezza economica e democratica.

  Un caso reale risalente al 2023 ha visto un amministratore delegato di un'azienda con sede in Asia cadere vittima di una frode sofisticata: ha partecipato a una videoconferenza apparentemente con il CFO della casa madre, che in realtà era un deepfake generato tramite IA. Convinto della legittimità della richiesta, ha autorizzato un bonifico da oltre 25 milioni di dollari. L'attacco, orchestrato da un gruppo criminale internazionale, ha sfruttato software di generazione video in tempo reale, dimostrando come l'IA possa essere usata per attacchi di alto profilo altamente persuasivi.
- Social engineering automatizzato: strumenti linguistici avanzati, come i modelli di generazione del linguaggio naturale (es. chatbot malevoli), possono generare messaggi di phishing più convincenti e personalizzati, aumentando il tasso di successo degli attacchi.
- IA contro IA: un ulteriore rischio è rappresentato dalla cosiddetta "guerra algoritmica", in cui gli attaccanti sviluppano sistemi IA per eludere o confondere gli algoritmi difensivi, generando una sorta di "corsa agli armamenti" digitale.

Questi scenari impongono una riflessione critica sull'uso dell'IA e sulla necessità di definire limiti etici, normativi e di governance.

4.3 Prospettive future

Il futuro della cybersecurity è sempre più intrecciato con lo sviluppo dell'intelligenza artificiale. Si prospettano scenari in cui la cyber difesa autonoma, basata su sistemi IA che imparano continuamente e si adattano in tempo reale, diventerà la norma. Tuttavia, questo richiede:

- Investimenti significativi in ricerca e innovazione: solo attraverso finanziamenti adeguati (sia nel settore pubblico che in quello privato) si potranno sviluppare algoritmi sempre più sofisticati e sistemi di intelligenza artificiale robusti e affidabili.
- Adozione di standard internazionali comuni: per garantire interoperabilità e sicurezza dei sistemi IA utilizzati per la cybersecurity, evitando così frammentazioni e lacune che potrebbero essere sfruttate dagli attaccanti.
- Formazione di professionisti esperti sia in AI che in diritto digitale: la presenza di figure professionali in grado di comprendere sia gli aspetti tecnologici che normativi permetterà di progettare soluzioni che siano efficaci, ma anche rispettose della privacy e delle normative vigenti.
- Definizione di cornici giuridiche flessibili ma efficaci, capaci di tenere il passo con l'innovazione

In conclusione, l'IA è destinata a trasformare radicalmente il campo della cybersecurity, fungendo sia da alleato che da minaccia. Il bilanciamento tra innovazione tecnologica e tutela dei diritti fondamentali sarà la sfida centrale dei prossimi anni.

Bibliografia

European Commission. (2023). *Proposal for a Cyber Resilience Act*.

European Parliament & Council. (2022). Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

European Parliament & Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council. (2022). Regulation (EU) 2022/2554 (DORA – Digital Operational Resilience Act). *Official Journal of the European Union*.

European Parliament & Council. (2023). Regulation (EU) 2023/xxx (Data Act). *Official Journal of the European Union*.

European Parliament & Council. (2024). Regulation (EU) 2024/xxx (Artificial Intelligence Act – AI Act). *Official Journal of the European Union*.

Italian Agency for Cybersecurity (ACN). (2023). *Relazione annuale sulla cybersecurity in Italia*. https://www.acn.gov.it

Agenzia per la Cybersicurezza Nazionale (ACN). (2021). *Decreto di istituzione e compiti*. https://www.cybersecurity.gov.it

Governo Italiano. (2023). *Piano Nazionale di Cybersecurity (PNC)*.

Clusit. (2024). *Rapporto annuale sulla sicurezza ICT in Italia 2024*. Associazione Italiana per la Sicurezza Informatica. https://www.clusit.it/rapporto-clusit

ENISA (European Union Agency for Cybersecurity). (2023). *Good Practices in Mitigating Ransomware Attacks*.

ACN (Agenzia per la Cybersicurezza Nazionale). (2021). *Rapporto annuale sulla sicurezza informatica in Italia*. Roma: ACN.

CERT-AgID. (2022). *Analisi degli incidenti informatici nelle infrastrutture critiche italiane: il caso Lazio*. Agenzia per l'Italia Digitale.

Garante per la protezione dei dati personali. (2023). *Linee guida sulla sicurezza informatica e privacy*. Roma: Garante Privacy. https://www.garanteprivacy.it/

Darktrace. (2022). *AI-powered cyber defense in healthcare: Case study on ransomware mitigation*. Darktrace Ltd.

NIST. (2021). *Artificial intelligence cybersecurity standards and guidelines*. National Institute of Standards and Technology.


JEAN
MONNET
CHAIR
Erasmus+
FUTURE
SIGHT
TOR VERGATA