Breviario giuridico della cybersicurezza

A cura di
Andrea Simoncini
Marina Pietrangelo

Prefazione di Bruno Frattasi
Direttore Generale Agenzia per la cybersicurezza nazionale

con la collaborazione di
Federico Niccolò Ricotta

edizioni
Consiglio Nazionale delle Ricerche

Breviario giuridico della **cybersicurezza**

A cura di
Andrea Simoncini
Marina Pietrangelo

Prefazione di Bruno Frattasi
Direttore Generale Agenzia per la cybersicurezza nazionale

con la collaborazione di
Federico Niccolò Ricotta

Le voci sono state redatte col contributo di

Davide Baldini (Università di Firenze), Omar Caramaschi (Università di Genova), Ludovica Ciarravano (Scuola IMT Alti Studi e Università di Firenze), Enza Cirone (Università di Firenze), Donatella Curtotti (Università di Foggia), Gaia Fiorinelli (Scuola Superiore Sant'Anna), Onofrio Flore (Università di Firenze), Matteo Giannelli (Università di Firenze), Cecilia Isola (Università di Genova), Maria Vittoria Malinconi (Università di Firenze), Lorenzo Nannipieri (CNR - Istituto di informatica giuridica e sistemi giudiziari), Wanda Nocerino (Università di Foggia), Marina Pietrangelo (CNR - Istituto di informatica giuridica e sistemi giudiziari), Federico Serini (Università di Torino), Giuseppe Sferrazzo (Agenzia per la cybersicurezza nazionale), Federico Ricotta (CNR - Istituto di informatica giuridica e sistemi giudiziari), Stefano Rovelli (Università di Pisa e CNR - Istituto di informatica giuridica e sistemi giudiziari), Maria Vittoria Zucca (Scuola IMT Alti Studi e Scuola Superiore Sant'Anna), Deisy Villalobos (Università di Genova)

Finanziato dall'EU - Next Generation EU nell'ambito di SERICS (Security and Rights in CyberSpace) Spoke 1 – Progetto CYBERIGHTS (Law and regulation for a better-safe Cyberspace)

Realizzato senza l'uso di Intelligenza Artificiale

Consiglio Nazionale delle Ricerche
Istituto di informatica giuridica e sistemi giudiziari

ISBN (ed. stampa/print edition) 978 88 8080 712 4
ISBN (ed. digitale/electronic edition) 978 88 8080 713 1
DOI https://doi.org/10.32091/cybersicurezza-2025

La versione digitale è pubblicata in Open Access su www.edizioni.cnr.it
Il presente lavoro è protetto dalla licenza CC BY-SA 4.0

coordinamento editoriale: Sara Di Marcello, CNR - Unità Editoria
progetto grafico e impaginazione: Fulvia Ciurlia, CNR - Unità Editoria

pubblicato da
©Cnr Edizioni, 2025
Piazzale Aldo Moro, 7
00185 Roma

www.edizioni.cnr.it
bookshop@cnr.it

Indice

Prefazione 7
Introduzione 9
A
Accesso abusivo a sistema informatico o telematico 15
Account 17
Advanced Persistent Threat (APT) 19
Agenzia per la Cybersicurezza Nazionale (ACN) 21
AI (Artificial Intelligence) 23
AI Act (Artificial Intelligence Act) 26
Algoritmo 29
Architettura nazionale di sicurezza cibernetica 31
Avatar 33
B
Backdoor 37
Bug bounty programs 38
C
Centrali di committenza 43
Centro di Valutazione e Certificazione Nazionale (CVCN) 45
Comitato Interministeriale per la Cybersicurezza (CIC) 47
Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR) 49
Common Vulnerabilities and Exposures (CVE) 52
Computer Security Incident Response Team (CSIRT) 54
Cookie 57
Crittografia 59
Cyberattacco (attacco informatico) 62
Cyberbullismo 64
Cybercrime 66
Cyberdefense 68
Cyberjustice 70
Cyberresilienza 72
Cyberspazio 74
Cyberterrorismo 76
D
Data breach (violazione di dati personali) 81
Dati personali 83
Deepfake 86
Digital forensic 88
Digital Services Act (DSA) 90
Doxing 92
Dual use 94

E
E-procurement 99
Eu-CyCLONe (European Cyber Crisis Liaison Organisation Network) 101
European Data Protection Board (EDPB) 103
European Union Agency for Cybersecurity (ENISA) 105
F
Fake news 111
Fattore umano 113
Firewall 115
Firma digitale 116
G
General Data Protection Regulation (GDPR) 123
General Purpose AI (GPAI) 125
Gruppo di cooperazione per le reti e i sistemi informativi 127
H
Hacker 133
Hacker etico 135
I
Identità digitale 141
Incidente informatico 143
Indirizzo IP 145
Ingegneria sociale 147
Internet 149
Interessato (diritti dell') 152
Investigazioni digitali 157
K
Keylogger 163
M
Malware 169
Misure di sicurezza 171
N
NIS (Direttive Nis) 177
O
Oblio (diritto all') 183
P
Perimetro di Sicurezza Nazionale Cibernetica (PSNC) 189
Phishing 191
Polizia postale 193
Pretexting 195
Privacy 196
Punto di contatto NIS 198

R
Ransomware 203
Regulatory sandbox 205
Reputazione 207
Rete di CSIRT 209
Riservatezza 210
Risk-based approach 212
S
Service provider 217
Sextorsion 219
Sicurezza nazionale 220
Sistema Pubblico di Identità Digitale (SPID) 222
Spam 224
Stazioni appaltanti 226
T
Tallin (manuale di) 231
Trojan 234
V
Vulnerabilità 239
Z
Zero-day 245
Zero trust 246

PREFAZIONE

Gli attacchi informatici si fanno sempre più numerosi e pericolosi. Numerosi a causa della trasformazione digitale delle nostre società e del ritmo accelerato dell'innovazione tecnologica. Pericolosi a causa dell'aumentata aggressività di attori che si presentano nello spazio cibernetico agguerriti e motivati sia dal profitto che da intenzioni politiche e ideologiche collegate alle attuali tensioni geopolitiche.

In questo contesto l'Agenzia per la cybersicurezza nazionale, che mi pregio di dirigere, svolge una funzione di presidio tecnologico e di avamposto culturale. Di presidio tecnologico perché garantisce la risposta efficace agli attacchi, onde preservare, in un'ottica di resilienza, la tutela degli interessi nazionali nello spazio cibernetico. Di avamposto culturale, perché è rivolta a favorire una più diffusa coscienza del rischio digitale e della necessità di un approccio responsabile e prudente all'ambiente cibernetico. È in questo contesto che si collocano, ad esempio, le attività di disseminazione di buone pratiche di cybersicurezza, nonché le iniziative di awareness e di formazione orientate a creare, in ultima analisi, una forza lavoro affidabile e compente per contribuire alla difesa del Paese.

L'Agenzia, poi, cura l'aggiornamento costante e continuo del quadro giuridico in materia, secondo principi di coerenza tra le varie disposizioni susseguitesi in questo ambito negli ultimi anni. L'armonico sviluppo del tessuto normativo è infatti fondamentale in un sistema plurale che vede più attori impegnati nella protezione cibernetica del Paese, ciascuno nel proprio ruolo. In ultima analisi, è questa un'attività di "cucitura" che intende valorizzare le diversità nell'unità, promuovendo tra i vari soggetti, pubblici e privati, le necessarie sinergie e collaborazioni.

ACN, inoltre, per sua natura, è un luogo dove le necessità dello sviluppo tecnologico, convergono e dialogano con la pratica diuturna della tutela delle infrastrutture critiche nazionali: dall'uso dei sistemi di Intelligenza artificiale allo studio della crittografia post-quantum fino al supporto alle start-up e alle PMI con iniziative dedicate al trasferimento tecnologico in un'ottica di promozione della sovranità digitale. Si tratta, beninteso, di un concetto che si declina in termini non solo nazionali ma

necessariamente europei alla luce dell'incrementale produzione legislativa unionale. Si pensi alla NIS, alla Dora, alla Cer e, infine, all'IA Act, e alle loro ricadute interne.
Per questo riteniamo di grande valore il Breviario giuridico della cybersicurezza curato dai professori Marina Pietrangelo e Andrea Simoncini. La pregevolezza di questo lavoro sta nell'avvicinare il lettore, con semplicità e linearità espositiva, qualità che tuttavia non tradiscono la tecnicità degli argomenti trattati, a una materia che sembra riservata agli ultraspecialisti e che nasconde insidie e ambiguità spesso fuorvianti. Mi viene allora da concludere con un antico adagio: nella chiarità è la verità.

Bruno Frattasi
Direttore Generale Agenzia per la cybersicurezza nazionale, ACN

INTRODUZIONE

Il *Breviario giuridico della cybersicurezza* nasce nella fucina del progetto CybeRights, che ha riunito esperti e giovani in formazione per lavorare su uno dei più complessi fronti dell'attuale rapporto tra diritto e digitalizzazione: la cybersicurezza.

Nulla è più possibile nello spazio digitale senza un elevato livello di cybersicurezza, concetto che rimanda subito a misure tecniche altamente specializzate; in realtà, fondamentale è il fattore umano.
Le misure di cybersicurezza ci consentono di proteggere le nostre vite online, le nostre attività professionali o personali, senza dovervi rinunciare e anzi rivendicando semmai il diritto di usare e godere di uno "spazio virtuale " che può e deve essere ancora una opportunità per la crescita personale e lo sviluppo sociale.
In questo scenario, se è vero che nessuno può più ignorare le conseguenze di azioni non sicure compiute online, dai rischi di violazione dei propri sistemi personali fino alla interruzione di servizi essenziali per la vita sociale e i bisogni delle persone, è vero anche che tutti dobbiamo fare la nostra parte.
I benefici che possono derivarci dall'uso delle applicazioni IT dipendono anche da noi, dipendono cioè anche dal nostro livello di consapevolezza sui rischi e sulle conseguenze delle azioni che compiamo quando siamo "connessi".

Ma cosa s'intende esattamente per cybersicurezza e soprattutto "cosa prevede la legge"? Quali sono i soggetti che se ne occupano? Quali sono i comportamenti virtuosi e quelli da evitare?
Di qui l'idea di un "breviario". Questo termine, in origine, indicava la sinossi di prescrizioni (di solito, preghiere) raccolte in forma concisa e pronte per l' uso quotidiano.
Abbiamo immaginato così un "Breviario giuridico della cybersicurezza", per dare una prima risposta alle domande di chi abita lo spazio digitale, prime "istruzioni per l'uso" per muoversi in un dedalo tecnico e normativo in cui la richiesta di informazioni cresce al pari della regolazione.
Il volume contiene un'analisi sistematica dei principali concetti giuridico-informatici che ricorrono nella legislazione, da cui sono

tratti. Secondo il modello del vocabolario, i concetti analizzati sono proposti in ordine alfabetico e spiegati con un linguaggio il più possibile piano, in modo da realizzare una vera e propria guida semplificata sulle norme di settore. Per chi desidera approfondire, le voci sono corredate di riferimenti alla principale letteratura scientifica che è alla base del lavoro di sintesi.
L'opera è destinata, infatti, sia agli addetti ai lavori, che vogliono avere sottomano una guida agile con i contenuti essenziali della materia, sia a coloro che intendono documentarsi per la prima volta sui risvolti giuridico-istituzionali delle attività di cybersicurezza.

Infine, una nota sul metodo di lavoro e sulle prospettive. Questo volume è nato come opera collettiva e collaborativa: le voci sono state "proposte" e poi redatte dai collaboratori, in rari casi, assegnate. E su questa via vorremmo proseguire, valorizzando ulteriormente questo modello collaborativo, attraverso la versione online del Breviario che è consultabile sulla piattaforma Osservatorio CybeRights.
Il progetto, infatti, si inserisce nella più ampia attività di ricerca e formazione intrapresa dal Centro interuniversitario CybeRights all'interno della Fondazione Serics (Space and Rights for a Safe Cyberspace) nata dal finanziamento PNRR.
La versione del Breviario resterà quindi aperta alla proposta e alla raccolta di nuove voci (visto che comunque ne mancano) o di nuovi temi che l'evoluzione tecnologica porterà a maggiore evidenza.
Le proposte di nuove voci possono essere inviate alla direzione dell'Osservatorio che ne validerà il contenuto.
Confidiamo così che questa lettura plurale e condivisa di un fenomeno che intreccia gli studi giuridici, connettendo come mai profili di diritto sostanziale e processuale, costituzionale, penale, civile, amministrativo, regionale e più ancora, rafforzi il valore della riflessione *del diritto* e *sui diritti*, che a nostro avviso resta irrinunciabile per comprendere il mondo in cui viviamo.

Per chiudere, molti sono i ringraziamenti dovuti: ai colleghi e alle colleghe che hanno creduto in questa iniziativa; alla preziosa collaborazione di Federico Ricotta; al Direttore dell'ACN, che ci

ha onorati della sua prefazione, confortandoci in qualche modo sulla bontà del lavoro fin qui fatto.

Firenze, settembre 2025
I curatori

a

ACCESSO ABUSIVO A SISTEMA INFORMATICO O TELEMATICO

L'accesso abusivo a sistema informatico o telematico è la fattispecie che punisce le intrusioni nel cd. domicilio informatico ed è prevista dal Codice penale italiano all'art. 615-*ter*.

Il reato corrisponde al modello dell'*Illegal/Unauthorized access* delineato nelle fonti internazionali ed europee relative alla criminalità informatica e cibernetica (es.: art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica; art. 3 della Direttiva europea 2013/40/UE relativa agli attacchi contro i sistemi di informazione).

In termini generali, integra la fattispecie chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà del titolare. La pena prevista per tale delitto è aggravata, ad esempio, nel caso in cui il fatto sia commesso da un pubblico ufficiale, oppure con violenza o minaccia, o ancora se riguardi un sistema informatico o telematico di interesse pubblico. Secondo la giurisprudenza, la fattispecie ricorre anche qualora il soggetto agente sia legittimamente abilitato all'accesso al sistema e tuttavia vìoli le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare o acceda per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita.

Il delitto è collocato tra i reati contro l'inviolabilità del domicilio, sul presupposto che i sistemi informatici o telematici costituiscano ormai una «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione» (v. la relazione al ddl n. 2773, poi legge n. 547/1993). Nella prospettiva internazionale ed europea, il delitto rappresenta un tassello della tutela (penale) della cd. CIA Triad (*Confidentiality, Integrity and Availability*) e garantisce anzitutto la riservatezza informatica, indipendentemente dalle finalità perseguite dall'autore dell'intrusione. Attualmente, la fattispecie di *accesso abusivo a*

sistema informatico o telematico rappresenta presidio penale di rilievo nella complessiva strategia nazionale ed europea per la cybersicurezza e il contrasto agli attacchi informatici, a tutela altresì della sicurezza nazionale e collettiva. Secondo la Raccomandazione n. 1 del GREVIO (*Group of Experts on Action against Violence against Women and Domestic Violence*) la fattispecie costituisce inoltre strumento di tutela della persona, rispetto a ipotesi di *stalking* o violenza in contesto digitale.

APPROFONDIMENTI

- Berghella, Blaiotta, *Diritto penale dell'informatica e beni giuridici*, in *Cassazione penale*, 1995, 2329 ss.
- Pecorella, *Diritto penale dell'informatica*, Padova, 2006.
- Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Picotti, *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 ss.
- Salvadori, *I reati contro la riservatezza informatica*, in Cadoppi, Canestrari, Manna, Papa (a cura di), *Cybercrime*, Milano, 2023, 694 ss.

VOCI CORRELATE

CYBERCRIME
HACKER
HACKER ETICO

ACCOUNT

Nel contesto delle tecnologie dell'informazione e della comunicazione, un account corrisponde a un profilo, ossia a una utenza registrata presso un fornitore di servizi digitali.

Un account è normalmente individuato da un nome utente (o ID) e da una password (cd. credenziali di accesso/autenticazione), che consentono al titolare l'accesso (o *login*) all'area riservata e al servizio. La procedura di autenticazione si definisce «a due fattori» quando affianca all'utilizzo di ID e password anche un secondo fattore di autenticazione (ad es. codice OTP inviato via SMS o mail, impronta digitale, ecc.). I fattori di autenticazione tradizionalmente includono: (i) *something you know* (qualcosa che sai: ad es. una password o un PIN); (ii) *something you have* (qualcosa che hai: ad es. un token, uno smartphone); o (iii) *something you are* (qualcosa che sei: ad es. un dato biometrico, come il volto o l'impronta digitale). In alcuni casi, un account registrato presso un *provider* può consentire di accedere anche ad app e servizi di terze parti, mediante le interfacce cd. API.

I dati identificativi dell'account, che consentono al titolare l'accesso al servizio, possono essere altresì considerati una identità digitale. Con questa accezione, ad esempio, il Codice penale prevede una pena più elevata nel caso in cui il delitto di frode informatica (art. 640-*ter* c.p.) sia commesso con furto o indebito utilizzo dell'identità digitale, in danno di uno o più soggetti: secondo la giurisprudenza costante, tale nozione di "identità digitale" fa riferimento proprio alle credenziali di accesso, necessarie per il *login* presso *provider* informatici privati o pubblici. Integra invece il delitto di sostituzione di persona (art. 494 c.p.) la creazione di un account social con uso (abusivo) delle generalità e dell'immagine di un altro soggetto. Il DPCM del 24/10/2014 (SPID) definisce all'art. 1 lett. o) l'identità digitale come «la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale».
Attualmente assumono particolare rilevanza gli account (o profili) su piattaforme di social media, che consentono agli utenti

di comunicare e condividere contenuti di carattere personale: tali account costituiscono estrinsecazione digitale dell'identità personale, per persone fisiche e giuridiche. La diffusione di account cd. social ha posto la questione, teorica e pratica, della cd. eredità digitale, cioè della sorte di account e profili dopo la morte del titolare: al proposito, molte piattaforme prevedono apposite procedure per la gestione o la cessazione degli account da parte di utenti eredi.

APPROFONDIMENTI

- Abhishek, Roshan, Kumar, Ranjan, *A Comprehensive Study on Multifactor Authentication Schemes*, in Meghanathan, Nagamalai, Chaki (eds.), *Advances in Computing and Information Technology*, Berlin, 2013, 561 ss.
- Flor, *Identità digitale e tutela penale*, in AIPDP e DiPLaP (a cura di), *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP. Atti dei seminari di discussione in collaborazione con il DiPLaP*, Milano, 2023, 573 ss.
- Leanza, *L'identità personale nell'era telematica: l'identità digitale*, in *Diritto di Famiglia e delle Persone (II),* 2023, 1807 ss.
- Marraffino, *La sostituzione di persona mediante furto di identità digitale*, in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, Milano, 2023, 321 ss.
- Resta, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica,* 2007, 511 ss.
- Sullivan, *Digital identity – From emergent legal concept to new reality*, in *Computer Law & Security Review*, 2018, 34, 4, 723 ss.

VOCI CORRELATE

DATI PERSONALI
IDENTITÁ DIGITALE
IDENTITA PERSONALE
INTERNET

ADVANCED PERSISTENT THREAT (APT)

L'*Advanced Persistent Threat* (APT) è una minaccia persistente avanzata cioè una forma di minaccia informatica. Essa è attivata da un avversario dotato di risorse significative e competenze avanzate, in grado di impiegare molteplici vettori di attacco - tra cui il cyberspazio, strumenti fisici e tecniche di inganno - per perseguire obiettivi quali l'esfiltrazione di dati sensibili, l'ostruzione di funzioni critiche o l'infiltrazione prolungata nei sistemi informativi.
La complessità di tali attacchi si manifesta, tra l'altro, nell'abituale condotta di occultamento delle tracce lasciate e nell'impiego di credenziali legittime per accedere a reti esterne rispetto a quella della vittima. L'attaccante utilizza anche le cd. Tecniche di movimento laterale, che gli consentono di estendere la propria presenza all'interno della rete compromessa, infettando ulteriori dispositivi o utenze.
Le APT si distinguono per la loro persistenza temporale, l'adattabilità alle contromisure difensive e la capacità di mantenere un'interazione continuativa con i sistemi violati, sia a fini di spionaggio cibernetico sia per altre forme di intrusione mirata, anche non digitali.
Gli illeciti penalmente rilevanti che si possono configurare in relazione a tali attacchi sono molteplici e variano in base al contesto. Tuttavia, da un punto di vista penalistico, le APT sottendono un disegno criminoso unitario: da una prospettiva teorica, sono riconducibili all'istituto del reato continuato; da un punto di vista tecnico, si concretizzano in una serie di violazioni eterogenee, reiterate, difficili da identificare e da ricondurre a un unico soggetto.
Il *modus operandi* consente di attribuire gli attacchi a determinati gruppi organizzati. Alcuni di essi, come APT31, si contraddistinguono per l'impiego di *botnet* realizzate sfruttando router domestici compromessi; altri, come Mustang Panda, adottano tecniche più convenzionali ma comunque efficaci, tra cui l'uso di dispositivi USB infetti.

APPROFONDIMENTI

- ENISA, *APT: Advanced Persistent Threat, in ENISA Glossary, European Union Agency for Cybersecurity.*
- National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39). U.S. Department of Commerce, 2011.
- The MITRE Corporation, *Enterprise Techniques - Lateral Movement*, MITRE ATT&CK Framework.
- The MITRE Corporation, *Groups MITRE ATT&CK*, MITRE.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERCRIME
HACKER
INCIDENTE INFORMATICO

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)

L'Agenzia per la cybersicurezza nazionale (ACN) è l'ente governativo italiano che coordina e implementa le politiche e le strategie di cybersicurezza del Paese. L'Autorità è stata istituita col d.l.n. 82 del 2021, convertito con modifiche nella legge n. 109/2021, ed è operativa dal 1° settembre dello stesso anno. Essa rappresenta il fulcro dell'architettura istituzionale italiana in materia di sicurezza cibernetica. La sua creazione ha segnato un passaggio di rilievo nella costruzione di una governance centralizzata e coerente del cyberspazio nazionale, superando la precedente frammentazione di competenze tra diversi organi dello Stato.

L'Agenzia opera come soggetto autonomo, dotato di personalità giuridica di diritto pubblico, e risponde funzionalmente alla Presidenza del Consiglio dei ministri. Essa assume un ruolo primario nella definizione e nell'attuazione della strategia nazionale di cybersicurezza, nel coordinamento delle attività degli attori pubblici e privati coinvolti nella protezione delle reti e dei sistemi informativi, nonché nella vigilanza sul rispetto delle misure di sicurezza da parte dei soggetti rientranti nel perimetro nazionale di sicurezza cibernetica o soggetti alle normative di settore (tra queste, la cosiddetta Direttiva NIS 2).

In virtù delle sue attribuzioni, l'ACN svolge funzioni sia regolatorie sia operative. È titolare di competenze in materia di prevenzione, rilevazione, analisi e risposta agli incidenti cibernetici, attraverso il coordinamento del CSIRT Italia, e fornisce supporto tecnico alle infrastrutture critiche, contribuendo alla loro resilienza rispetto a minacce e vulnerabilità informatiche; elabora standard, protocolli e misure di sicurezza, per lo più previsti dalla normativa euronionale; ha poteri ispettivi e sanzionatori nei confronti dei soggetti vigilati.

L'Agenzia promuove, inoltre, politiche industriali, scientifiche e formative orientate a rafforzare la capacità del Paese di dotarsi di soluzioni tecnologiche avanzate, autonome e sicure; sostiene la ricerca nel campo della cybersicurezza; favorisce la crescita di competenze specialistiche; incentiva la collaborazione con

il mondo accademico e con il settore privato, nell'ottica di uno sviluppo sostenibile e sovrano dell'ecosistema digitale nazionale. Nel quadro europeo e internazionale, l'Agenzia funge da punto di contatto per le autorità estere competenti e partecipa attivamente alla definizione di strategie comuni per la tutela dello spazio cibernetico. A livello interno, essa si inserisce in una rete multilivello che comprende, tra gli altri, il Sistema di informazione per la sicurezza della Repubblica, il Ministero della difesa, le forze di polizia e le altre autorità regolatorie di settore.

APPROFONDIMENTI

- Cavelty, Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authori*ty, in *Journal of European Public Policy*, Vol. 30, 2023.
- Colaiacovo (a cura di), *Sicurezza, informazioni, giustizia penale*, Pisa, 2023, 359 ss.
- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277 ss.
- Ricotta, *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in Colaiacovo (a cura di), Sicurezza, informazioni, giustizia penale, Pisa, 2023, 359 e ss.

VOCI CORRELATE

ARCHITETTURA NAZIONALE DI SICUREZZA CIBERNETICA
NIS (DIRETTIVE NIS)
PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

AI (ARTIFICIAL INTELLIGENCE)

AI è l'acronimo di *artificial intelligence* o in italiano intelligenza artificiale (IA). Essa è definibile come il settore della scienza informatica che studia gli agenti informatici o macchine che simulano il comportamento umano ricevendo precetti dall'ambiente circostante. Si tratta di una definizione inevitabilmente molto ampia, che sconta la dimensione assai vasta della materia e la mancanza di accordo nella comunità scientifica sulla definizione di "intelligenza", prima ancora che di "intelligenza artificiale". In concreto, l'espressione "intelligenza artificiale" comprende numerose tecnologie piuttosto differenti tra di loro su un piano tecnico, ma accomunate dalla circostanza di simulare alcuni aspetti generalmente riconducibili all'intelligenza umana.

Negli ultimi anni, e specialmente negli ultimi due decenni, la tecnologia maggiormente promettente in termini di progressi è il cosiddetto *Machine Learning*, incluse le sue varianti come le Reti Neurali (*Neural Networks*) e il *Deep Learning*, risultando essere quella oggi più comunemente associata all'IA.
Un'ulteriore suddivisione può essere individuata tra sistemi di IA specializzati da un lato, ossia i sistemi impiegati per scopi specifici (come la valutazione del merito creditizio, la profilazione delle preferenze di un individuo, il riconoscimento facciale ecc.) e sistemi di IA per scopi generali dall'altro, vale a dire sistemi in grado di svolgere con competenza un'ampia gamma di compiti distinti (ad es., sistemi di IA generativa come ChatGPT).

L'*AI Act* dell'Unione europea (Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio) elude il problema definitorio, dettando una definizione normativa non tanto di intelligenza artificiale, quanto di "Sistema di intelligenza artificiale", definito all'art. 3, lett. a), come segue: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

L'adozione sempre più diffusa di sistemi di IA solleva rilevanti questioni etiche e giuridiche, soprattutto in relazione alla tutela dei diritti fondamentali. Tra i principali rischi vi è quello della discriminazione algoritmica, ossia l'effetto per cui sistemi di IA producono risultati distorti o ingiusti a danno di determinati gruppi o individui, spesso a causa di dati di addestramento incompleti, non rappresentativi o riflessivi di pregiudizi sociali preesistenti. Tali distorsioni possono manifestarsi, ad esempio, nell'ambito del reclutamento del personale, della concessione di prestiti, o del riconoscimento facciale, con effetti discriminatori particolarmente rilevanti per le persone vulnerabili, che possono subire discriminazioni, ad esempio, su base etnica, di genere o socioeconomica. Ulteriori criticità riguardano la trasparenza, la possibilità di contestare decisioni automatizzate e l'attribuzione della responsabilità giuridica per eventuali danni prodotti dai sistemi di IA.

Proprio per affrontare tali rischi, l'*AI Act* prevede misure differenziate in base al livello di rischio associato ai sistemi, con l'obiettivo di assicurare che lo sviluppo e l'utilizzo dell'IA avvengano nel rispetto dei valori e dei diritti fondamentali sanciti dall'ordinamento dell'Unione europea.

La legge italiana 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale) contiene sia disposizioni di principio, che ai sensi dell'art. 1, co. 2, "si interpretano e si applicano conformemente" all'*AI ACT*, sia prescrizioni direttamente applicabili. Tra queste ultime, rilevano in particolare il Capo III che definisce poteri e funzioni delle autorità di settore e i Capi IV e V in tema di diritto d'autore e materia penale.

APPROFONDIMENTI

- Fidanza, *Sulla distinzione tra intelligenza artificiale e algoritmi*, in *Rivista di diritto dell'impresa*, 2024.
- Russell, Norvig, *Artificial intelligence: a modern approach,* 4th ed. Upper Saddle River, NJ, Prentice Hall, 2021.
- Simoncini, *Il linguaggio dell'intelligenza artificiale e la tutela Costituzionale dei diritti*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, 2024.

VOCI CORRELATE

AI ACT (ARTIFICIAL INTELLIGENCE ACT)
ALGORITMO
GENERAL PURPOSE AI (GPAI)
GENERAL DATA PROTECTION REGULATION (GDPR)

AI ACT (ARTIFICIAL INTELLIGENCE ACT)

L'*AI Act* è il Regolamento (UE) 2024/1689 dell'Unione europea che disciplina lo sviluppo e l'utilizzo di sistemi e modelli di intelligenza artificiale (IA), garantendo sicurezza, rispetto dei diritti fondamentali e promuovendo l'innovazione. Uno degli obiettivi principali è evitare che i singoli Stati membri introducano normative nazionali disomogenee, prevedendo invece una normativa unitaria in UE, a supporto del mercato unico e favorendo la certezza del diritto. Ciò dovrebbe facilitare lo sviluppo e l'adozione dell'IA in tutta l'Unione, rendendola competitiva su scala globale.

L'*AI Act* è entrato in vigore il 2 agosto 2024, sebbene la diretta applicabilità del regolamento sia stata differita ai mesi e anni successivi, a seconda dei singoli ambiti regolamentati.
La tecnica normativa dell'*AI Act* si fonda su di un approccio basato sul rischio (*risk-based approach*), classificando i sistemi di IA in base al loro potenziale impatto sui diritti fondamentali e sulla sicurezza. Una prima macro-distinzione viene effettuata tra «sistemi di IA», ossia sistemi software che incorporano elementi di IA (ad es., un software di *credit scoring* bancario, oppure ChatGPT), e «modelli di IA» per finalità generali, ossia i singoli componenti intelligenti dei sistemi di IA (ad es. i *Large Language Models* come GPT-4o).
I sistemi di IA vengono classificati come segue, in base alla finalità di utilizzo:

- rischio inaccettabile (art. 5). Include sistemi di IA che producono rischi considerati inaccettabili e non mitigabili, quali ad esempio sistemi di social scoring, sistemi di riconoscimento delle emozioni utilizzati fuori dall'ambito medico e sistemi biometrici di catalogazione in categorie protette (ad es., sulla base dell'etnia);
- alto rischio (art. 5). Include tecnologie che operano in settori critici come la sanità, l'istruzione, l'occupazione, la biometria e le infrastrutture critiche. Questi sistemi devono rispettare

requisiti rigorosi in termini di sicurezza, trasparenza e supervisione umana;

- rischio limitato (art. 50). Comprende applicazioni come chatbot o deepfake, per cui si richiedono livelli di trasparenza adeguati, ad esempio informando gli utenti che stanno interagendo con un sistema di IA e non con un essere umano;
- rischio minimo, qualsiasi sistema di IA che non rientra nelle precedenti categorie (ad es., filtri antispam, IA utilizzata nei videogiochi) è considerato a rischio minimo e, come tale, non è sottoposto ad alcun obbligo dall'*AI Act*, anche se potrebbe ricadere nell'area di applicazione di altre normative (ad es., GDPR, laddove vi sia un trattamento di dati personali).

I modelli di IA per finalità generali vengono suddivisi come segue, a prescindere dalla finalità di utilizzo (trattandosi per definizione di modelli che possono essere utilizzati per molteplici finalità, ad esempio integrandoli in altri software):

- modelli di IA per finalità generali. Tecnologie come i *Large Language Model* che generano contenuti audio, video e/o testuali, autonomamente. I fornitori di questi modelli devono garantire trasparenza sull'origine del contenuto generato e prevedere misure a tutela del diritto d'autore, in fase di addestramento del sistema;
- modelli di IA per finalità generali con rischio sistemico. Modelli di IA estremamente grandi e che utilizzano vaste quantità di potere computazionale, con impatti su larga scala o in grado di influenzare interi settori economici, sociali o politici (ad es., GPT 4). Per questa categoria sono previsti controlli particolarmente rigorosi e valutazioni d'impatto periodiche.

In caso di non conformità, sono previste sanzioni fino a € 35 milioni o al 7% del fatturato mondiale annuo. Per i sistemi di IA, l'enforcement è delegato ai singoli Stati membri, che dovranno designare una o più autorità di controllo nazionali. Per i modelli di IA per finalità generali, l'enforcement è invece accentrato nell'Ufficio europeo per l'IA (*AI Office*), presso la Commissione europea.

Al di là dell'aspetto strettamente regolatorio, l'*AI Act* prevede strumenti a favore dell'innovazione. Tra questi:

- alfabetizzazione in materia di IA. Iniziative per migliorare la comprensione dell'IA, inclusi rischi e benefici, tra cittadini, imprese e istituzioni;
- spazi di sperimentazione normativa (*AI Regulatory Sandboxes*). Ambienti di test regolamentati per le imprese che possono così sperimentare nuove tecnologie IA senza il rischio immediato di incorrere in sanzioni, favorendo lo sviluppo sicuro e conforme fin dalla progettazione.

APPROFONDIMENTI

- Cirone, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in *Quaderni AISDUE,* fascicolo speciale, 2, 2024.
- Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE,* fascicolo speciale, 2, 2024.
- Smuha, Yeung, *The European Union's AI Act: beyond motherhood and apple pie?*, June 24, 2024.
- Veale, Borgesius, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International,* 4, 2021.

VOCI CORRELATE

AI (ARTIFICIAL INTELLIGENCE)
ALGORITMO
GENERAL PURPOSE AI (GPAI)
REGULATORY SANDBOX

ALGORITMO

L'algoritmo è convenzionalmente definibile come una sequenza finita di istruzioni, ben definita e univoca, tale da poter essere eseguita meccanicamente e tale da produrre un determinato risultato. Questa nozione ha una storia millenaria. Il termine algoritmo pare derivi dal nome del matematico persiano al-Khwarizmi vissuto nel IX secolo, che per primo riuscì a fornire soluzioni esplicite a certi tipi di equazioni. Per secoli quindi questa nozione è stata intuitivamente riferita in diverse aree della matematica a uno specifico stile di dimostrazione per cui la risoluzione del problema matematico avveniva sulla base di un elenco di istruzioni specifiche. Questa definizione tradizionale è, tuttavia, piuttosto generica, poiché ricomprende al suo interno situazioni più disparate e senza alcuna connessione con il settore dell'ICT e dell'IA quali, ad esempio, la ricetta per cucinare una pietanza.

In ambito giuridico nell'ordinamento nazionale una definizione di algoritmo è stata introdotta dal Consiglio di Stato nella sentenza 7891 del 2021, secondo cui l'algoritmo è «una sequenza finita di istruzioni, ben definita univoca, tale da poter essere eseguita meccanicamente con un elevato grado di automazione e tale da produrre un determinato risultato».

APPROFONDIMENTI

- Baldini, De Benedetto, *The open texture of 'algorithm' in legal language*, in AI & Society, 2024.
- Fidanza, *Sulla distinzione tra intelligenza artificiale e algoritmi*, in *Rivista di diritto dell'impresa*, 2024.
- Pietrangelo, Nannipieri, *Intelligenza artificiale e pubbliche amministrazioni, tra incertezze definitorie, usi disomogenei e giudici supplenti*, in Falchi, Giannotti, Monreale et al. (eds.), Ital-IA 2023*, Proceedings Ital-IA 2023: 3rd National Conference on Artificial Intelligence*, 2023.

VOCI CORRELATE

AI ACT (ARTIFICIAL INTELLIGENCE ACT)
AI (ARTIFICIAL INTELLIGENCE)
CRITTOGRAFIA
GENERAL PURPOSE AI (GPAI)

a

ARCHITETTURA NAZIONALE DI SICUREZZA CIBERNETICA

L'architettura nazionale di cybersicurezza è il quadro strutturato e coordinato a livello nazionale che definisce gli organi preposti all'adozione ed attuazione di politiche, strategie, norme e pratiche per proteggere dalle minacce informatiche le infrastrutture critiche, i sistemi informatici, le reti e i dati di un Paese. La base normativa di riferimento è costituita dal d.l. n. 82 del 2021 (convertito con modifiche nella legge n. 109/2021) che ha definito l'architettura nazionale e previsto l'istituzione dell'Agenzia nazionale per la cybersicurezza (ACN). La governance del sistema nazionale di sicurezza cibernetica è così composta: al vertice è posto il Presidente del Consiglio dei ministri a cui sono attribuite l'alta direzione e la responsabilità generale delle "politiche di cybersicurezza". Ad esso spettano l'adozione della relativa strategia nazionale e la nomina dei vertici dell'Agenzia per la cybersicurezza nazionale. Il Presidente del Consiglio dei ministri può delegare alla Autorità delegata per il sistema di informazione per la sicurezza della Repubblica le funzioni che non sono a lui attribuite in via esclusiva. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.
In senso più ampio, l'attuale architettura nazionale di sicurezza cibernetica è stata strutturata su quattro grandi pilastri di competenze tra loro diversificate ma comunicanti: la cybersicurezza e la resilienza nello spazio cibernetico, affidate all'Agenzia per la cybersicurezza nazionale; la raccolta e l'analisi informativa, affidate al Sistema di informazione per la sicurezza della Repubblica; la difesa e la sicurezza militare dello Stato, affidate al Ministero della Difesa; la prevenzione e il contrasto dei reati, di competenza delle forze di polizia e dell'autorità giudiziaria.

APPROFONDIMENTI

- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277 ss.
- Longo, *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in *Rivista italiana di informatica e diritto*, 1, 2024, 65 ss.
- Ricotta, *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in Colaiacovo (a cura di), *Sicurezza, informazioni, giustizia penale*, Pisa, 2023, 359 ss.
- Ricotta, *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in *Diritto penale contemporaneo*, 1, 2023, 97 ss.

VOCI CORRELATE

a

AGENZIA DI CYBERSICUREZZA NAZIONALE (ACN)
MISURE DI SICUREZZA
NIS (DIRETTIVE NIS)
PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

AVATAR

Nel linguaggio informatico l'*avatar* è l'immagine bidimensionale o la rappresentazione grafica tridimensionale scelta dall'utente per raffigurare sé stesso in una realtà virtuale (comunità *online*, app di messagistica, giochi, metaverso ecc.). Il termine avatar deriva dal sanscrito *avatāra*, utilizzato nell'induismo con il significato di "incarnazione".

L'avatar concorre alla definizione dell'identità digitale dell'utente, nonché alla sua esperienza-presenza digitale, in misura variabile a seconda del livello d'integrazione tra realtà virtuale e realtà fisica. L'avatar costituisce, ora, anche il mezzo attraverso il quale gli utenti partecipano al cd. Metaverso: è, infatti, attraverso la propria rappresentazione grafica in corpi digitali che gli utenti interagiscono gli uni con gli altri, in una sorta di dimensione alternativa e digitale dell'esistenza.
La cyber-psicologia ha individuato empiricamente una certa tendenza degli utenti ad attuare per il tramite del proprio avatar comportamenti più "sregolati" e meno inibiti socialmente, rispetto a quelli tenuti nella realtà fisica, in conseguenza della cd. deindividuazione nelle relazioni mediate dalle ICT. Per altro verso, è stato rilevato che, mediante l'avatar, l'utente ha una percezione diretta della realtà virtuale capace di riflettersi sulla sua esperienza reale e sulla sua integrità psico-fisica, ad esempio nel caso di un'aggressione o una molestia subita dall'avatar.

Proprio tale collocazione dell'avatar tra reale e virtuale ha attualmente assunto rilevanza in prospettiva giuridica, rispetto all'esigenza di disciplinare i comportamenti tenuti dagli utenti per il tramite del proprio alter ego digitale: è recente, al proposito, la notizia dell'indagine avviata nel Regno Unito per l'aggressione sessuale ai danni di un avatar di una ragazza, avvenuta in un contesto di realtà virtuale.

APPROFONDIMENTI

- Chalmers, *Reality+. Virtual worlds and the problems of philosophy,* New York, 2022.

- Messinger et al., *On the Relationship between My Avatar and Myself*, in *Journal of Virtual Worlds Research*, 1-2, 2008, 1 ss.
- Nazzaro, *Soggettività dell'avatar tra profilazione e identità personale*, in *Tecnologie e Diritto*, 2024, 1, 135 ss.
- Rigotti, Malgieri, *Human vulnerability in the metaverse*, Brussels, 2023.
- INTERPOL, *Metaverse: A Law Enforcement Perspective. Use Cases, Crime, Forensics, Investigation, and Governance*, White Paper, 2024.
- Saccomani, *Vivere il metaverso mediante il corpo/avatar nella spazialità virtuale*, in *Informazione filosofica*, 8, 2022, 117 ss.

VOCI CORRELATE

ACCOUNT
IDENTITÀ DIGITALE
INTERNET

b

BACKDOOR

Una *backdoor* è un metodo nascosto per bypassare le normali procedure di autenticazione e ottenere l'accesso a un sistema informatico, rete o applicazione.
Letteralmente il termine significa "porta di servizio", alludendo così alle uscite secondarie di un edificio.
La backdoor può essere utilizzata per scopi leciti, fornendo un canale di accesso per svolgere operazioni tecniche, o per scopi illeciti. Le backdoor possono infatti essere inserite nel software da sviluppatori malintenzionati o possono essere create in un tempo successivo rispetto alla creazione del software sfruttando vulnerabilità esistenti. Una volta installata, una backdoor consente agli attaccanti di controllare il sistema da remoto, eseguire comandi e rubare dati senza essere rilevati.

APPROFONDIMENTI

- Chiara, *Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso alcuni diritti di cybersicurezza?*, in *Diritto & Questioni pubbliche*, 1, 2025, 1 ss.
- Ricotta, *Questioni sull'uso della Backdoor a scopo di investigazione*, in *Cassazione penale*, 2, 2019, 28 ss.

VOCI CORRELATE

ACCESSO ABUSIVO A SISTEMA INFORMATICO
CYBERATTACCO (ATTACCO INFORMATICO)
VULNERABILITÀ

BUG BOUNTY PROGRAMS

I *Bug Bounty Programs* consistono nella pratica organizzativa di compensare soggetti esterni, quali ricercatori di sicurezza e cd. hacker etici, con una ricompensa monetaria per l'identificazione e la segnalazione di vulnerabilità (da qui *bug*) nei propri sistemi informatici, applicazioni o siti web, rafforzando così la postura complessiva di sicurezza. Tali programmi rivestono un ruolo fondamentale nell'individuare falle che potrebbero essere potenzialmente sfruttate da attori malevoli. Ogni Bug Bounty Program si fonda su un insieme di regole di ingaggio che svolgono due funzioni: da un lato, definiscono il comportamento atteso dai ricercatori durante l'identificazione delle vulnerabilità e nella trasmissione delle segnalazioni; dall'altro, stabiliscono gli obblighi delle organizzazioni, come la determinazione dell'entità dei compensi per le vulnerabilità rilevate e le tempistiche previste per la loro risoluzione.

In sintesi, i principali elementi che compongono le "regole di ingaggio" dei Bug Bounty Program sono:

- le aree *in-scope* e *out-of-scope*, che delineano con precisione le sezioni del sistema, dell'applicazione o del prodotto che i ricercatori sono autorizzati a esaminare, specificando al contempo le componenti escluse dal programma;
- le vulnerabilità ammissibili e non ammissibili, che definiscono i criteri per considerare valide le segnalazioni, evidenziando le tipologie di vulnerabilità che l'organizzazione intende prioritariamente identificare, in particolare quelle che comportano rischi significativi per la sicurezza;
- le linee guida per la divulgazione, che stabiliscono le modalità e i tempi di eventuale pubblicazione delle vulnerabilità scoperte, solitamente consentita solo dopo l'implementazione della correzione da parte dell'organizzazione;
- le azioni vietate o indesiderate, cioè l'elenco delle pratiche non consentite durante le attività di ricerca, con l'obiettivo di garantire il rispetto di principi etici, leggi vigenti in materia e la tutela dell'integrità dei sistemi analizzati.

La “taglia sulla testa” delle vulnerabilità, pur identificandosi in un esborso economico da parte dell’azienda, non è considerata dall’azienda una perdita. Infatti, se una vulnerabilità venisse individuata (e sfruttata) da attori malevoli prima di essere corretta, le conseguenze economiche e reputazionali per l’organizzazione potrebbero essere di gran lunga più gravi.

APPROFONDIMENTI

- Fiorinelli, Zucca, *Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU* in *Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024),* 2024, vol. 3731, 1 ss.
- Laszka et al., *The rules of engagement for bug bounty programs*, in *Financial Cryptography and Data Security: 22nd International Conference*, Berlin, 2018.
- Malladi, *Bug bounty programs for cybersecurity: Practices, issues, and recommendations*, in *IEEE Software*, vol. 37, 1, 2019.

VOCI CORRELATE

HACKER ETICO
INCIDENTE INFORMATICO
MISURE DI SICUREZZA
VULNERABILITÀ

C

CENTRALI DI COMMITTENZA

Le centrali di committenza operano nel contesto dell'*e-procurement* (acquisizione di beni e sevizi mediante piattaforme digitali). Sono soggetti pubblici che gestiscono la centralizzazione degli acquisti per conto di più stazioni appaltanti, essendo loro delegato il ruolo di stazione appaltante in favore di altri soggetti pubblici, favorendo un notevole risparmio di spesa e un migliore approvvigionamento dei beni richiesti.
L'esigenza di un potenziamento delle centrali di committenza è richiesta dalla Direttiva n. 24/2014 sugli appalti pubblici, secondo cui la forte aggregazione della gestione degli appalti comporta una riduzione dei costi, un miglioramento del servizio e una maggiore professionalità nella conduzione dei contratti (vedi in particolare i Considerando nn. 59 e 69).
Le centrali di committenza nel panorama della commessa pubblica migliorano e rafforzano la capacità di acquisizione e vendita e, per la loro natura polivalente, di azione. Esse, infatti, operano come intermediari aggiudicando appalti, gestiscono sistemi dinamici di acquisizione o concludono accordi quadro ad uso delle amministrazioni aggiudicatrici.
A norma dell'articolo 62 del nuovo Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36), in cui si rintraccia la qualificazione giuridica delle centrali di committenza e le relative funzioni. Esse progettano, aggiudicano e stipulano contratti o accordi quadro per conto delle stazioni appaltanti, qualificate o non qualificate che siano, potendo, da ultimo, affidare convenzioni a cui le stesse possono aderire. Le centrali di committenza hanno anche la facoltà di impostare dei sistemi dinamici di acquisizione, determinare mercati elettronici di negoziazione, dare esecuzione contrattuale per conto delle stazioni appaltanti qualificate o non qualificate e rendere prestazioni di committenza ausiliaria.
Obiettivo del nuovo Codice dei contratti pubblici è la definizione di un nuovo modello di committenza pubblica, lungo la scia di quanto prospettato dal precedente Codice del 2016. Questo modello è pensato come *asset* centrale di aggregazione e centralizzazione, attorno a cui ruotano gli strumenti destinati al soddisfacimento economico di tutti i soggetti attivi nella commessa pubblica. Con questo nuovo approccio, infine, le

stazioni appaltanti sono preparate ad assolvere nel modo migliore possibile al complessivo processo di approvvigionamento.

APPROFONDIMENTI

- Macchia, *La qualificazione delle amministrazioni appaltanti,* in *Giornale di diritto amministrativo* 1, 2017, 50 ss.
- Mattarella*, La centralizzazione delle committenze,* in *Giornale di diritto amministrativo,* 5, 2016, 613 ss.
- Nunziata, *Aggregazione, centralizzazione e qualificazione della committenza*, in Macchia (a cura di) *Costruire e acquistare, Lezioni sul nuovo Codice dei contratti pubblici*, Torino, 2024, 63 ss.

VOCI CORRELATE

E-PROCUREMENT
STAZIONI APPALTANTI

CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE (CVCN)

Il Centro di valutazione e certificazione nazionale (CVCN) è l'organismo cui compete la valutazione e certificazione della cybersicurezza delle risorse informatiche in uso presso soggetti esercenti funzioni o servizi essenziali per lo Stato. Si tratta di una funzione prevista dalla disciplina del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e assegnata al CVCN dal d.l. 105 del 2019 (art. 1, co. 6), convertito con modifiche nella legge n. 133/2019. L'elenco dei soggetti esercenti funzioni o servizi essenziali è contenuto nel decreto attuativo di tale disposizione, cioè il DPCM 15 giugno 2019.
Per le funzioni assegnategli, il CVCN riveste un ruolo centrale nella strategia di cybersicurezza italiana in quanto contribuisce a prevenire rischi legati alla crescente dipendenza da tecnologie digitali, e a proteggere la sovranità tecnologica nazionale.
Si tratta di un ente originariamente istituito presso l'Istituto superiore delle comunicazioni e tecnologie informatiche (ISCTI) del Ministero dello sviluppo economico, che è oggi confluito presso l'Agenzia nazionale per la cybersicurezza.

Oltre alle funzioni operative di valutazione e certificazione della cybersicurezza, il Centro collabora con gli enti europei e internazionali che si occupano di armonizzazione degli standard di cybersicurezza, favorendo così anche lo scambio di informazioni sui caratteri delle minacce emergenti.

Il CVCN supporta mediante la propria attività di valutazione il Gruppo di coordinamento per l'esercizio dei poteri speciali. In particolare, cura l'analisi degli aspetti tecnici di cybersicurezza legati alla tecnologia 5G e, in previsione, si occupa dei settori tecnologici che saranno inclusi nella disciplina Golden Power a seguito delle recenti modifiche normative (cfr. l'art. 1-*bis* del d.l. n. 21 del 2012).
Per le funzioni di monitoraggio si avvale dei Laboratori accreditati di prova (LAP), centri accreditati dallo stesso CVCN (cfr. l'art. 1, co 7 del d.l. n. 105 2019).

APPROFONDIMENTI

- Osservatorio Accredia, *Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata*, 1, 2022.
- Serini, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in Calzolaio (a cura di), *La fine di internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 41 ss.
- Sferrazzo, *La cybersecurity nel nuovo Codice dei contratti pubblici: l'art. 108 co. 4 e le criticità per le stazioni appaltanti*, in *Teoria e critica della regolazione sociale*, 30, 2025, 157 ss.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

COMITATO INTERMINISTERIALE PER LA CYBERSICUREZZA (CIC)

Il Comitato interministeriale per la cybersicurezza (CIC) è l'organismo politico-strategico, istituito presso la Presidenza del Consiglio dei ministri, che ha il compito di indirizzare, coordinare e monitorare le attività rilevanti per cybersicurezza nella Repubblica Italiana. Il Comitato è Presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata per la sicurezza della Repubblica, dai Ministri dell'interno, degli esteri e della cooperazione internazionale, della difesa, della giustizia, dell'economia, delle imprese e del made in Italy, dell'ambiente e della sicurezza energetica, dell'Università e della ricerca, delle infrastrutture e dei trasporti, nonché dal Direttore Generale dell'Agenzia per la cybersicurezza nazionale con funzioni di segretario.

La composizione del Comitato riflette la necessità di un approccio integrato e trasversale alla sicurezza cibernetica nazionale. Il coinvolgimento dei ministri responsabili dei principali settori strategici garantisce, infatti, che le decisioni in materia di cybersicurezza tengano conto delle diverse esigenze e vulnerabilità del Paese, favorendo anche la condivisione di informazioni e la definizione di strategie comuni, evitando frammentazioni e sovrapposizioni tra le diverse amministrazioni. Le funzioni attribuite al Comitato esprimono quindi una supervisione centralizzata per assicurare coerenza nelle politiche e rapidità di risposta alle minacce, che spesso sono trasversali e coinvolgono più settori contemporaneamente. Il CIC ha peraltro un ruolo non meramente consultivo, ma proattivo: il Comitato propone gli indirizzi gli indirizzi generali da perseguire nelle politiche di cybersicurezza nazionale ed esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; coordina e promuove l'adozione di iniziative per favorire la collaborazione tra soggetti istituzionali e operatori privati, sia a livello nazionale che internazionale, nel settore della cybersicurezza. Infine, vigila sull'attuazione delle politiche e strategie di cybersicurezza, assicurando il raccordo tra le diverse amministrazioni coinvolte.

APPROFONDIMENTI

- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277 ss.
- Ricotta, *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in Colaiacovo (a cura di), *Sicurezza, informazioni giustizia penale*, Pisa, 2023, 359 ss.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
ARCHITETTURA NAZIONALE PER LA CYBERSICUREZZA

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA (COPASIR)

Il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) è un organismo parlamentare bicamerale istituito dall'articolo 30 della legge 3 agosto 2007, n. 124, che ha riformato il Sistema di informazione per la sicurezza della Repubblica (i cd. "Servizi") e la disciplina del segreto.

Al COPASIR è assegnata la funzione di verificare, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni.
Dell'organismo, che opera normalmente in condizioni di segretezza o comunque con un regime di pubblicità dei lavori limitato, fanno parte cinque deputati e cinque senatori nominati dai Presidenti delle due Camere in modo da garantire la rappresentanza paritaria della maggioranza e delle opposizioni, che esprimono il Presidente.

Per l'esercizio delle proprie funzioni di controllo, il Comitato dispone di poteri conoscitivi molto ampi. In primo luogo, può procedere all'audizione di una pluralità di soggetti titolari di informazioni e di competenze di interesse, a partire dal Presidente del Consiglio dei ministri e dei responsabili di vertice di Dipartimento delle informazioni per la sicurezza (DIS), Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni e sicurezza interna (AISI), oltre che dell'Agenzia per la cybersicurezza nazionale. Una ulteriore modalità di acquisizione di informazioni utili all'esercizio del controllo parlamentare è costituita dalla facoltà del Comitato di ottenere copie di atti e di documenti relativi a procedimenti e a inchieste in corso presso l'autorità giudiziaria o presso altri organi inquirenti, nonché la documentazione e gli elementi informativi ritenuti di interesse in possesso del Sistema di informazione per la sicurezza o della pubblica amministrazione.

Al Comitato sono, altresì, attribuite rilevanti competenze consultive. In particolare, l'organo è chiamato a esprimere il proprio parere obbligatorio non vincolante su tutti gli schemi di decreto o di regolamento previsti nella legge n. 124 del 2007 e su ogni altro schema di decreto o di regolamento che riguardi l'organizzazione e lo stato del personale degli organismi di informazione e sicurezza.
Il Comitato e il suo presidente sono destinatari di numerose comunicazioni obbligatorie e relazioni periodiche da parte del Governo, degli organismi di *intelligence* e dell'Agenzia per la cybersicurezza (ACN). Tra le informative obbligatorie al Presidente del COPASIR da parte del Presidente del Consiglio dei ministri si evidenziano quelle relative alla nomina dei direttori e dei vicedirettori di DIS, AISE, AISI e Agenzia per la cybersicurezza.

Il Comitato dispone, infine, di rilevanti poteri in materia di conferma della opposizione del segreto di Stato da parte del Presidente del Consiglio dei ministri.
Con specifico riguardo alla cybersicurezza, gli interventi normativi successivi alla legge del 2007 hanno potenziato il ruolo del COPASIR, affidando a esso alcuni poteri specifici: sorvegliare sull'applicazione del Piano nazionale per la sicurezza dello spazio cibernetico; esprimere pareri sulle direttive del Presidente del Consiglio; approvare specifiche linee d'indirizzo per favorire la collaborazione tra soggetti istituzionali e operatori privati interessati alla sicurezza cibernetica; elaborare indirizzi generali e obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza della Repubblica.

APPROFONDIMENTI

- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277 ss.
- Perini, *Evoluzione della forma di governo alla luce della disciplina e della prassi del COPASIR*, in *Rassegna parlamentare*, 1, 2023, 19 ss.
- Ricotta, Il segreto di Stato, in Colaiacovo (a cura di), *Sicurezza, informazioni, giustizia penale*, Pisa, 2023.

VOCI CORRELATE

ARCHITETTURA NAZIONALE DI CYBERSICUREZZA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
SICUREZZA NAZIONALE

COMMON VULNERABILITIES AND EXPOSURES (CVE)

Le *Common Vulnerabilities and Exposures* (CVE) sono un insieme di identificatori univoci assegnati a vulnerabilità di sicurezza note che colpiscono software, hardware o firmware. Si tratta di un sistema di catalogazione pubblica nato per offrire un linguaggio condiviso e standardizzato per descrivere debolezze e difetti informatici che possono essere sfruttati da attori malevoli per compromettere la sicurezza di un sistema. Ogni voce CVE è accompagnata da una breve descrizione del problema, un identificatore univoco (ad esempio, CVE-2023-12345) e, talvolta, riferimenti a database di sicurezza, bollettini dei produttori o strumenti di mitigazione.

Le CVE non vanno confuse con le CWE (*Common Weakness Enumeration*): mentre le CVE rappresentano esempi concreti di vulnerabilità specifiche, le CWE costituiscono una tassonomia delle categorie astratte di debolezze nel design o nell'implementazione del software. Una CWE descrive il tipo di errore che è stato commesso, mentre una CVE individua "dove" quell'errore si è verificato in un prodotto reale. Si può dire quindi che le CWE forniscono il quadro teorico e le CVE la relativa espressione pratica nel mondo reale.

Il sistema CVE è un elemento cruciale per il settore della sicurezza informatica. Esso, infatti, costituisce la base comune per il monitoraggio e la gestione delle vulnerabilità, quindi facilita la comunicazione tra esperti, produttori di software, ricercatori di sicurezza, enti governativi e utenti finali. Le CVE sono utilizzate nei sistemi di gestione delle vulnerabilità (*Vulnerability Management Systems*), nei controlli di conformità normativa (ISO/IEC 27001, ecc.) e nei *penetration test*.

APPROFONDIMENTI

- The MITRE Corporation, *CVE – Common Vulnerabilities and Exposures*, MITRE, 2024.
- The MITRE Corporation. *CWE – Common Weakness Enumeration*, MITRE, 2024.

VOCI CORRELATE

ADVANCED PERSISTENT THREAT (APT)
ARCHITETTURA NAZIONALE DI CYBERSICUREZZA
CYBERCRIME
VULNERABILITÀ

a. COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Il *Computer Security Incident Response Team* (CSIRT) è una unità specializzata nella gestione degli incidenti di sicurezza informatica. La sua funzione principale è monitorare, intercettare e analizzare le minacce di sicurezza informatica, rispondendo così all'esigenza di proteggere aziende e organizzazioni di ogni dimensione dagli attacchi informatici, che sono sempre più avanzati e dannosi. I CSIRT non si limitano alla gestione degli incidenti, ma svolgono un ruolo cruciale anche nella prevenzione. Attraverso la creazione di procedure standardizzate e la diffusione di avvisi e bollettini, essi aiutano le organizzazioni a prepararsi contro le future minacce. Nello specifico, le principali funzioni e responsabilità di un CSIRT includono:

- monitoraggio e rilevamento, monitoraggio continuo delle reti per rilevare qualsiasi attività sospetta o malevola;
- analisi degli incidenti, una volta individuato l'incidente, il CSIRT analizza la natura e l'origine dell'attacco per comprendere come è stato eseguito e quali vulnerabilità sono state sfruttate;
- coordinamento della risposta, dopo l'analisi, il CSIRT coordina la risposta, che può comprendere il contenimento dell'attacco e la mitigazione dei danni;
- ripresa delle operazioni, il team lavora per ripristinare rapidamente le normali operazioni, garantendo la continuità delle funzioni aziendali con il minimo impatto;
- comunicazione, il CSIRT mantiene informati e aggiornati gli stakeholder interni ed esterni, inclusi i clienti, i partner e le autorità, sullo stato delle minacce e sulle azioni di risposta.

Il CSIRT collabora con un Security Operations Center (SOC) e altre entità di sicurezza per garantire una risposta efficace e tempestiva agli incidenti. Questa collaborazione è essenziale per un approccio olistico alla sicurezza informatica, che prevede la condivisione di informazioni e best practices tra diversi team e organizzazioni.

In Italia, il CSIRT nazionale è istituito presso l'Agenzia per la cybersicurezza nazionale (ACN), in attuazione di quanto previsto dal d.l. 14 giugno 2021, n. 82, convertito con modificazioni dalla

legge 4 agosto 2021, n. 109, e svolge un ruolo centrale nella gestione degli incidenti cibernetici a livello statale.
A livello regionale, un'importante innovazione è stata introdotta con la legge regionale della Toscana 9 dicembre 2024, n. 57, recante Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Tale legge, che modifica la L.R. 54/2009, rafforza il quadro normativo regionale in materia di trasformazione digitale e sicurezza informatica, delineando un sistema più integrato di governance tecnologica e tutela dei diritti digitali. In particolare, l'articolo 16 della legge disciplina le funzioni del *Computer Security Incident Response Team* della Toscana (CSIRT Toscana), struttura operativa incaricata della gestione e della prevenzione degli incidenti di sicurezza informatica a livello regionale. Tra le sue principali competenze rientrano il monitoraggio e l'analisi dei rischi e delle minacce cyber che interessano il territorio, l'emissione di preallarmi, allerte e annunci, nonché la divulgazione di informazioni rilevanti agli operatori coinvolti. Il CSIRT riceve notifiche di incidenti informatici, sia obbligatorie sia volontarie, curandone l'eventuale trasmissione alle autorità nazionali competenti e coordinando, ove necessario, le attività di analisi e risposta. In caso di incidente, è previsto un intervento diretto volto a contenere i danni e a garantire il ripristino dei servizi.
Il CSIRT Toscana si occupa inoltre dell'analisi dinamica dei rischi e degli incidenti, della promozione della sensibilizzazione situazionale in materia di sicurezza e resilienza cibernetica e partecipa attivamente alla rete nazionale dei CSIRT italiani. È previsto anche l'esercizio di ulteriori funzioni eventualmente conferite dall'Agenzia per la cybersicurezza nazionale (ACN), nonché lo svolgimento di altri compiti individuati con apposita deliberazione regionale, in conformità alla normativa di settore.

APPROFONDIMENTI

- Giannelli, *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza,* in Fiorinelli, Giannelli (a cura di), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, sezione monografica della *Rivista italiana di informatica e diritto*, 1, 2024, 15 ss.

- Perri, Ziccardi (a cura di), *Dizionario Legal Tech*, Milano, 2020.
- Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in Pietrangelo (a cura di), *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 2024, 13 ss.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA ITALIANA (ACN)
INCIDENTE INFORMATICO
NIS (DIRETTIVE NIS)
RETE DI CSIRT

COOKIE

Il cookie è un piccolo file di testo inviato da un sito web al dispositivo dell'utente durante la navigazione, con lo scopo di memorizzare informazioni che saranno poi ritrasmesse al medesimo sito in occasione degli accessi successivi. I cookies consentono il riconoscimento dell'utente e semplificano l'esperienza online, ad esempio conservando articoli in un carrello in un sito di e-commerce, precompilando moduli o memorizzando preferenze di navigazione.

Dal lato del gestore del sito, i cookies permettono la raccolta e l'elaborazione di dati personali (quali indirizzo IP, identificativi online, credenziali) e non personali (come impostazioni di lingua o tipologia di dispositivo), che possono essere utilizzati per finalità statistiche, di personalizzazione, marketing e profilazione, e talvolta condivisi con soggetti terzi.

L'uso dei cookies è disciplinato a livello dell'Unione europea dall'art. 5, par. 3, della Direttiva 2002/58/CE (cd. Direttiva ePrivacy), come modificata dalla Direttiva 2009/136/CE. Tale norma prevede che l'archiviazione di informazioni o l'accesso a informazioni già archiviate nel terminale dell'utente sia consentita solo previo consenso informato, tranne nel caso di cookie tecnici strettamente necessari. Nell'ordinamento italiano, tale principio è stato recepito dall'art. 122 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101. Le Linee guida del Garante per la protezione dei dati personali del 10 giugno 2021, inoltre, hanno ulteriormente precisato le modalità per la redazione di una corretta informativa, la raccolta del consenso dell'utente, nonchè le modalità per la revoca del consenso che può avvenire in qualsiasi momento.

APPROFONDIMENTI

- Borgobello, *Manuale di diritto della protezione dei dati personali, dei servizi e dei mercati digitali*, Milano, 2023, 279 ss.

- Garofalo, *Cookies and the Passive Role of the Data Subject*, in Bernes, Irti, Senigaglia (eds), *Privacy and Data Protection in Software Services,* Singapore, 2021, 73 ss.
- Leta Jones, *The Character of Consent – The History of Cookies and the Future of Technology Consent*, Cambridge, 2024.
- Markou, *Behavioural advertising and the new 'EU Cookie Law' as a victim of business resistance and a lack of official determination,* in Gutwirth, Leens, De Hert (eds), *Data Protection in the Move*, Dordrecht, 2016, 213 ss.
- Santos, Bielova, Matte, *Are Cookie Banners Indeed Compliant With the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners,* in *Technology and Regulation*, 2020, 91 ss.

VOCI CORRELATE

C

CYBERSPAZIO
INTERESSATO (DIRITTI DELL')
GENERAL DATA PROTECTION REGULATION (GDPR)

CRITTOGRAFIA

La crittografia (o criptografia, dal greco antico kryptós, “nascosto” e graphía, “scrittura”) è la tecnica che permette, con l’aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti (o *plaintext*), in una forma illeggibile per quegli utenti che non possiedono una chiave segreta di decifrazione (*key*).

Fin dall’antichità, i procedimenti di cifratura sono stati utilizzati per proteggere i messaggi da letture non autorizzate. Con l’evoluzione tecnologica, si è resa necessaria anche la garanzia di ulteriori proprietà fondamentali come l’integrità, l’autenticazione e il non ripudio, ottenute attraverso specifiche tecniche crittografiche.
Nella disciplina relativa a nuove forme di documentazione, in particolare il cd. documento informatico (per una definizione, cfr. l’art. 20 del d.lgs. n. 82/2005 recante Codice dell’amministrazione digitale), e alla loro validità ed efficacia probatoria, la crittografia assume un ruolo fondamentale per impedire l’accesso indiscriminato alle informazioni contenute nel documento, imputare il documento ad un soggetto determinato e determinabile (attraverso la cd. firma digitale), nonché tutelare e verificare agevolmente l’integrità del documento stesso.

In Italia, la legge 28 giugno 2024, n. 90 (in particolare, l’art. 10) individua nell’Agenzia per la cybersicurezza nazionale (ACN) l’autorità competente per lo sviluppo e la promozione di standard crittografici avanzati in quanto strumenti di cybersicurezza. Tali standard servono a garantire un elevato livello di sicurezza nei sistemi informatici e di protezione delle informazioni sensibili e strategiche, in ambito non classificato, come previsto dalla Strategia nazionale di cybersicurezza e nella normativa nazionale ed europea.
Dal punto di vista giuridico, si discute sulla liceità di alcune tecniche di sicurezza, in quanto esse potrebbero rientrare tra i divieti di tecniche crittografiche già vietati dalle norme di settore. Il dibattito dottrinale e giurisprudenziale riguarda soprattutto il bilanciamento tra la protezione del diritto fondamentale dell’individuo alla protezione dei suoi dati personali e l’esercizio del

potere/dovere dello Stato di proteggere la cittadinanza e garantire la stabilità del territorio (cfr. Corte Europea dei Diritti dell'Uomo, Terza Sezione, caso Podchasov c. Russia del 13 febbraio 2024). La stessa suscettibilità di qualifica delle tecniche crittografiche, generalmente considerate beni a duplice uso (così qualificate ad esempio nell'Accordo di Wassenaar, 1996, e nel Regolamento (UE) 2021/821), le ha sempre rese difficilmente inquadrabili in un regime giuridico ben definito e, soprattutto, omogeneo a livello internazionale. Nondimeno, esistono linee guida non vincolanti, come quelle elaborate dall'OECD (*Recommendation of the Council concerning Guidelines for Cryptography Policy* e *Inventory of Controls on Use of Cryptography Technologies*) che contengono principi cui ispirarsi per l'adozione, da parte di ogni singolo Governo, di una politica nazionale in materia di crittografia.

Le tecniche di crittografia sono infine al centro di un recente ripensamento dei suoi presupposti e tecniche implementative a causa di nuovi sviluppi tecnologici, come il computer quantistico, che possono minare la sicurezza delle attuali infrastrutture di sicurezza. Quest'ultimo, infatti, potendo risolvere rapidamente problemi matematici complessi, come la fattorizzazione di numeri primi su cui si basano gli algoritmi di crittografia classica come RSA, è in grado di mettere a rischio le attuali tecniche di cifratura. Dagli Stati Uniti (cfr. *Quantum Computing Cybersecurity Preparedness Act 6 U.S.C. § 1526*), all'Unione europea (cfr. European Commission, *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*), viene incoraggiata la migrazione a tecniche crittografiche resilienti anche ai più potenti attacchi informatici, cd. *Quantum-safe Cryptography*.

APPROFONDIMENTI

- ACN, *Linee Guida Funzioni Crittografiche*, 11 luglio 2024.S
- Chiara, *Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso alcuni diritti di cybersicurezza?,* in *Diritto & Questioni pubbliche*, 1, 2025, 1 ss.
- Dizon, Upson, *Laws of encryption: An emerging legal framework*, in *Computer Law & Security Review*, Vol. 43, 2021.

- Musiani, *La crittografia nei sistemi di messaggistica sicura: le libertà digitali tra sviluppo tecnologico e regolazione*, in *Rivista di Digital Politics*, 3, 2022, 423 ss.
- Ziccardi, *Crittografia e diritto. Crittografia, utilizzo e disciplina giuridica documento informatico e firma digitale, segretezza delle informazioni e sorveglianza globale*, Torino, 2003.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
DUAL-USE
FIRMA DIGITALE
VULNERABILITÀ

CYBERATTACCO (ATTACCO INFORMATICO)

Il cyberattacco o attacco informatico è qualsiasi operazione intenzionale e non autorizzata realizzata per compromettere la riservatezza, l'integrità, la disponibilità o il funzionamento di un sistema informatico o telematico, o dei dati in esso contenuti. Rientrano, quindi, nella nozione di cyberattacco i casi di accesso abusivo, interferenza illecita, intercettazione, danneggiamento di dati o sistemi ecc. La crescente informatizzazione di attività pubbliche e private, di rilievo sociale ed economico, rende attualmente i cyber-attacchi una minaccia per la sicurezza nazionale, oltre che per i singoli beni personali o patrimoniali attaccati.

Il fenomeno ha rilevanza giuridica, con alcuni distinguo a seconda dell'origine, della portata, della natura o della finalità dell'attacco, Un cyberattacco, infatti, può costituire un reato, a proiezione offensiva individuale, collettiva o pubblica, nel contesto del diritto penale dell'informatica; può integrare un atto terroristico (cd. cyber-terrorismo); può financo costituire atto di rilevanza militare o bellica e potenzialmente ricadere nell'ambito applicativo del diritto penale internazionale.

A livello europeo, il Regolamento del Consiglio n. 2019/796 e la Decisione del Consiglio n. 2019/797 disciplinano le misure restrittive adottabili contro i cyber-attacchi che minacciano l'Unione o i suoi Stati membri (riferite agli attacchi informatici relativi, tra gli altri, a: infrastrutture critiche, servizi essenziali, funzioni statali), nell'ambito del cd. *Cyber Diplomacy Toolbox*.

Secondo il rapporto ENISA *Threat Landscape* 2024, i cyberattacchi sono in crescita a livello globale ed europeo. Tra le minacce informatiche di maggiore rilievo, si segnalano: *ransomware* (attacchi informatici seguiti da una richiesta di "riscatto" per il rispristino dell'integrità o della funzionalità del sistema); DDoS *(Distributed Denial of Service*, volti a compromettere il funzionamento di un sistema mediante sovraccarico o saturazione delle sue risorse); attacchi lungo la catena di fornitura (*supply-chain attacks*, che sfruttano le vulnerabilità di terze parti).

APPROFONDIMENTI

- Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue, Spiegel, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 100, 817 ss.
- Holt, Chermak, Freilich, Turner, Greene-Colozzi, *An Assessment of the Harms Associated With Ideologically* Iglezakis (a cura di), *The Legal Regulation of Cyber Attacks*, Alphen an den Rijn, 2020.
- Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017.
- Möller, *Cyberattacker Profiles, Cyberattack Models and Scenarios, and Cybersecurity Ontology*, in Id., *Guide to Cybersecurity in Digital Transformation*, Cham, 2023, 181 ss.
- Poli, Sommario, *The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions*, in *German Law Journal*, 2023, 24, 522 ss.
- *Motivated Cyberattacks*, in *Crime & Delinquency*, 2024, 71(3), 624 ss.

VOCI CORRELATE

ACCESSO ABUSIVO A SISTEMA INFORMATICO O TELEMATICO
CYBERCRIME
HACKER
MALWARE

CYBERBULLISMO

Il termine cyberbullismo identifica le manifestazioni di bullismo virtuale compiute mediante la rete telematica: azioni caratterizzate dalla volontà di prevaricazione, reiterata nel tempo e attuata mediante l'uso di strumenti informatici a danno di un singolo o di un gruppo. Tra queste si richiamano: le molestie, il ricatto, la diffamazione, l'aggressione, la manipolazione e l'illecito trattamento dei dati personali in danno di minori.
Al cyberbullismo sono riconosciuti i fattori qualificanti il bullismo "tradizionale": l'asimmetria di potere, la ripetizione e l'intenzionalità, con le peculiarità legate al particolare contesto in cui si realizzano le azioni, cioè il cyberspazio. Anzitutto, il fenomeno rileva per la sua ampiezza. L'uso di strumenti informatici per la realizzazione della condotta, infatti, annichilisce ogni ostacolo legato al tempo e allo spazio: se nel bullismo tradizionale è necessaria un'occasione di contatto tra il bullo e la vittima in un ambiente fisico comune, nel cyberbullismo le potenzialità della rete telematica rendono la condotta del cyberbullo realizzabile in ogni momento e in ogni luogo. Non è da ostacolo la distanza fisica o geografica, il che amplifica il danno e l'offesa. Inoltre, una volta pubblicato in Internet, il materiale diffamatorio resta nella disponibilità del chiunque per un periodo di tempo indefinito. Altra caratteristica focale è l'anonimato: il cyberbullo agisce dietro lo schermo del proprio smartphone o del proprio computer, mediante l'uso di *nickname* o *avatar*, celando così la propria identità. Ciò lo induce a sentirsi non solo protetto dall'ombra dell'anonimato ed essere, così, più disinibito, ma anche meno responsabile e meno in grado di comprendere la portata reale delle sue azioni a causa dell'assenza di contatto fisico con la vittima. Sono molte le tipologie di comportamento in cui può manifestarsi. Tra queste: (a) il *flaming*, invio di messaggi elettronici dal contenuto violento, aggressivo, denigratorio al fine di umiliare e provocare la vittima; (b) la *denigration,* la diffusione di foto, video, informazioni riguardanti la vittima al solo scopo di umiliarla e lederne la propria riservatezza; (c) l'*impersonation*, il furto d'identità digitale da parte del cyberbullo, il quale sarà in grado di inviare messaggi sgradevoli allo scopo di far credere che provengano dal soggetto, in realtà, leso.

In Italia il fenomeno è stato regolato per la prima volta con la legge n. 71 del 2017 (Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo) e più di recente dalla legge n. 70 del 2024 (Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo). Le norme mirano a contrastare il cyberbullismo in tutte le sue manifestazioni, ma soprattutto a prevenirlo attraverso un'opera di collaborazione tra famiglie, scuole e associazioni.

APPROFONDIMENTI

- Del Gaudio, *Tutelare i minori nell'era digitale,* in R. Razzante (a cura di), *Manuale di cybersicurezza,* Pisa, 2023.
- Di Simone, Spata, *Il Cyberbullismo e i reati dell'era digitale,* Rimini, 2024.
- Siani, *Cyberbullismo. Piccolo manuale per proteggere e guidare la generazione digitale,* Roma, 2025.

VOCI CORRELATE

CYBERCRIME
CYBERSPAZIO
DOXING

CYBERCRIME

La nozione di *cybercrime* individua, in termini molto generali, i reati e le attività di natura criminale commessi mediante l'uso di ICT o la rete internet. Non esiste, ad ogni modo, una definizione universalmente valida e accettata del termine, che ha un'accezione più criminologica o politico-criminale che precisamente giuridica. In principio, si faceva riferimento al concetto di *computer crime*, poi superato con l'avvento del web e, dunque, del cd. cyberspazio. Alla luce dell'attuale sviluppo tecnologico, si è anche proposto di sostituire al concetto di *cybercrime* quello di *digital crime*.

La dottrina italiana tendenzialmente distingue tra reati informatici e reati cibernetici per individuare, con la prima nozione, i reati commessi con (o ai danni di) tecnologie informatiche (ad es. accesso abusivo a sistema informatico) e, con la seconda, i reati commessi mediante la (o nella) rete internet (ad es. *cyberstalking*). Si qualificano, inoltre, reati informatici o cibernetici "in senso ampio" i reati che, secondo la formulazione della relativa fattispecie, possono anche - ma non necessariamente - commettersi con ICT o internet (ad es. diffamazione, truffa).

Un'altra distinzione di rilievo, all'interno del concetto di *cybercrime*, è quella tra reati cyber-dipendenti, che possono essere esclusivamente commessi mediante computer o altre ICT (dunque, nuovi rispetto alla criminalità "tradizionale": si pensi, ad esempio, all'accesso abusivo a sistema informatico); e reati cyber-abilitati, cioè reati "tradizionali" che sono facilitati dalle ICT o da internet, che ad esempio ne ampliano la portata offensiva oppure assicurano un relativo anonimato all'autore, rispetto alle modalità di realizzazione offline (tra questi, le truffe online, le violazioni del diritto d'autore, la circolazione di materiale pedopornografico).

L'avvento del fenomeno del *cybercrime* ha richiesto ai legislatori – a livello nazionale, europeo e internazionale – di introdurre nuove disposizioni incriminatrici in diritto penale, ma anche di definire nuovi poteri investigativi e nuove modalità di accertamento

e cooperazione, per lo svolgimento di indagini e la ricerca di prove nello spazio digitale. Il primo e più rilevante trattato internazionale in materia è la Convenzione del Consiglio d'Europa sul *cybercrime*, siglata a Budapest nel 2001. Più recente invece la *United Nations Convention against Cybercrime* adottata dall'Assemblea Generale delle Nazioni Unite il 24 dicembre 2024.

APPROFONDIMENTI

- Gillespie, *Cybercrime. Key Issues and Debates*, New York, 2019.
- Holt, Bossler, Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction*, New York, 2022.
- Morgante, Fiorinelli (a cura di), *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement*, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 2025
- Picotti, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme*, in Cadoppi, Canestrari, Manna, Papa (diretto da), *Cybercrime*, Milano, 2023, 32 ss.
- Powell, Stratton, Cameron, *Digital Criminology. Crime and Justice in Digital Society*, New York, 2018.
- Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, 2024.

VOCI CORRELATE

ACCESSO ABUSIVO A SISTEMA INFORMATICO
CYBERSPAZIO
DIGITAL FORENSICS
INTERNET

CYBERDEFENSE

La *cyberdefense* consiste nell'insieme delle misure di protezione di reti informatiche, infrastrutture critiche e informazioni, finalizzate ad assicurare risposte efficaci ad attacchi o minacce. La *cyberdefense*, quindi, è quindi uno strumento fondamentale per la tutela di dati sensibili e risorse strategiche. Rivolta a organizzazioni, enti pubblici e reti complesse, essa mira a prevenire, rilevare e contrastare tempestivamente azioni dannose, impedendo la compromissione di dati e sistemi mediante strategie difensive basate sull'adozione di misure tecniche e organizzative (riduzione dell'esposizione agli attacchi; individuazione di asset critici e informazioni sensibili; controlli preventivi; rafforzamento delle capacità di rilevamento e risposta agli attacchi).

Con la Cyber Security Strategy del 2013 l'Unione europea ha avviato una politica di rafforzamento della sicurezza digitale dell'Unione in risposta al crescente numero e alla complessità degli attacchi informatici, specialmente in settori e servizi critici come sanità, energia e trasporti. La strategia propone di rafforzare l'autonomia tecnologica dell'Unione, fondata sulla resilienza dei sistemi connessi, favorendo una collaborazione più stretta tra le comunità che si occupano di mercato interno, sicurezza, politica estera e difesa, per affrontare le minacce in modo coordinato. In tale contesto, nel 2022 la Commissione europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una comunicazione congiunta sulla *cyberdefense*, anche in ragione dell'avvenuta aggressione russa contro l'Ucraina, con l'obiettivo di rafforzare la capacità dell'Unione di proteggere i propri cittadini e le infrastrutture critiche.

La politica si articola in quattro pilastri principali che comprendono diverse iniziative per aiutare l'UE e gli Stati membri a identificare, prevenire e difendersi meglio dagli attacchi informatici: agire congiuntamente per rafforzare la difesa informatica dell'Unione; salvaguardare l'intero ecosistema della difesa; investire nello sviluppo delle capacità di difesa informatica; collaborare per affrontare insieme le sfide comuni.

L'Unione europea intende, inoltre, diminuire la sua dipendenza

strategica da tecnologie informatiche critiche, rafforzando la Base Industriale Tecnologica di Difesa Europea (EDTIB). A tal fine, sono numerose le attività di cooperazione in materia di difesa nel cyberspazio affidate a diverse istituzioni, tra cui la Commissione europea, il Servizio europeo per l'azione esterna (SEAE), l'Agenzia europea per la difesa, l'*European Union Agency for Cybersecurity* (ENISA) e l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol).

APPROFONDIMENTI

- Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law,* in *Rivista dell'Associazione Italiana dei Costituzionalisti,* 2022, 1 ss.
- Sciacovelli, *Attività ostili nel ciberspazio: il quadro normativo internazionale e dell'UE e l'importanza di istituire un'Unità congiunta per il ciberspazio,* in Osservatorio SIOI, 2021, 1 ss.
- Tzavara, Vassiliadis, *Tracing the evolution of cyber resilience: a historical and conceptual review,* in *International Journal of Information Security, 23,* 2024.

VOCI CORRELATE

CYBERCRIME
CYBERTERRORISMO
EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)
SICUREZZA NAZIONALE

CYBERJUSTICE

La formula *cyberjustice* è spesso usata come sinonimo di *e-justice* (giustizia digitale). Secondo l'impostazione adottata a livello internazionale, la giustizia digitale è definibile come il risultato del processo di incorporazione delle tecnologie digitali nel sistema dell'amministrazione della giustizia (CEPEJ 2016). Questa definizione ampia, quindi, copre tutte le attività giurisdizionali in cui sono impiegate le applicazioni digitali: re-ingegnerizzazione di processi, raccolta dati e integrazione dei sistemi, risoluzione di controversie online, svolgimento dei processi da remoto, sistemi digitali di accesso alle prove ecc. (UNDP 2022).
La digitalizzazione della giustizia intesa in senso lato coinvolge più d'un aspetto di rilevo costituzionale: l'esercizio della funzione giurisdizionale (es. art. 24 Cost e diritto di difesa esercitato online nelle udienze penali durante la pandemia da covid-19); l'organizzazione degli apparati amministrativi e giudicanti (es. art. 25 Cost. e applicazione automatizzata del principio di precostituzione del giudice naturale); la separazione dei poteri nello Stato costituzionale (ad es. sul ruolo dei Consigli di giustizia nelle decisioni sulla digitalizzazione giudiziaria).
Nell'ambito della giustizia digitale, sono in fase di sperimentazione sistemi di "giustizia predittiva" basati su applicazioni di intelligenza artificiale, capaci di restituire previsioni probabilistiche sugli esiti di una specifica attività giudiziaria (CEPEJ: *European Ethical Charter on the use of Artificial Intelligence in Judicial Systems and their Environment*). Questi sistemi presuppongono un livello avanzato di digitalizzazione dell'organizzazione giudiziaria e, in particolare, dei dataset delle decisione giudiziarie su cui i sistemi predittivi possono essere addestrati. Le cautele al riguardo sono numerose, particolarmente da parte dei giuspubblicisti che considerano irrinunciabili le garanzie previste dall'ordinamento giuridico a tutela dell'autonomia e dell'imparzialità dei magistrati (su cui vedi la decisione del Conseil constitutionnel francese, dec. n. 2019-778, che ha riconosciuto la legittimità della scelta legislativa di proibire la profilazione dei giudici attraverso strumenti di intelligenza artificiale).
La normativa fissa in ogni caso alcuni limiti non superabili. L'art. 22 del Regolamento generale sulla protezione dei dati personali

n. 2016/679 (*General Data Protection Regulation* - GDPR) stabilisce che ogni persona interessata «ha il diritto di non essere sottopost[a] a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che l[a] riguardano o che incida in modo analogo significativamente [su di lei]».
Il Regolamento sull'intelligenza artificiale n. 2024/1689 (*Artificial Intelligence* Act - AI Act) inserisce l'attività giurisdizionale nella categoria delle attività ad alto rischio, per cui l'uso di sistemi vasati su intelligenza artificiale è subordinato a più stringenti obblighi e divieti volti a garantirne la trasparenza, l'affidabilità e il controllo da parte dell'uomo (cfr. gli artt. 8-15 *AI Act*).

APPROFONDIMENTI

- Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *Dpce online*, 2020.
- Garapon, Lassègue, *La giustizia digitale. Determinismo tecnologico e libertà,* Bologna, 2021.
- Longo, *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Milano, 2023.

VOCI CORRELATE

AI ACT (ARTIFICIAL INTELLIGENCE ACT)
DIGITAL FORENSICS
INVESTIGAZIONI DIGITALI
SISTEMA PUBBLICO DI IDENTITÀ DIGITALE (SPID)

CYBERRESILIENZA

La cyberresilienza (*cyber resilience)* è la capacità di un'organizzazione di difendersi dagli attacchi informatici e di assorbire l'impatto di un evento avverso, garantendo la continuità operativa e il rapido ripristino dei servizi essenziali anche durante o subito dopo un incidente. Il termine deriva dal latino *resilire*, che significa "saltare indietro", e indica proprio la capacità di un materiale di piegarsi senza spezzarsi, assorbendo e dissipando l'energia di un impatto.
Il concetto di resilienza va infatti oltre la semplice sicurezza informatica, che si concentra sulla prevenzione e sulla difesa, perché implica una visione più ampia che integra tecnologia, processi organizzativi e cultura aziendale. Essere resilienti in ambito cyber significa abbracciare un approccio adattivo, preparandosi all'eventualità che una violazione possa comunque avvenire, pianificando ogni azione per minimizzare i danni, ripristinare rapidamente i sistemi e imparare dagli incidenti per rafforzare la propria postura di sicurezza nel tempo.
Dunque, non si tratta soltanto di evitare gli attacchi, ma di saperli gestire quando si verificano, contenendo l'impatto, riprendendo il controllo in tempi brevi dei sistemi e assicurare la migliore continuità operativa.

APPROFONDIMENTI

- Björck, Henkel, Stirna, Zdravkovic, *Cyber Resilience. Fundamentals for a Definition,* in Rocha, Correia, Costanzo, Reis (eds.), *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, 353, Berlin, 2015.
- Camisa, Simoncini, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, 2024.
- Tzavara, Vassiliadis, *Tracing the evolution of cyber resilience: a historical and conceptual review,* in *International Journal of Information Security, 23,* 2024.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
FATTORE UMANO
VULNERABILITÀ

CYBERSPAZIO

La parola cyberspazio è spesso usata come sinonimo di Internet. Essa indica lo spazio virtuale in cui si realizza lo scambio di dati e informazioni per mezzo di sistemi di connessione che interagiscono tra loro. In questa dimensione immateriale agiscono istituzioni pubbliche e soggetti privati, individui e gruppi, e dunque la postura di cybersicurezza risulta determinante per proteggere i dati scambiati e i sistemi da rischi che possono avere un impatto sulla società e sull'ordinamento giuridico.
Il termine cyberspazio è entrato nell'uso corrente all'inizio degli anni Ottanta quando Gibson nel romanzo *Neuromancer* usò l'inglese *cyberspace*, ripartendo dal prefisso *cyber* già impiegato nel 1948 dal matematico Wiener per coniare la parola cybernetica (disciplina che studia i processi riguardanti «la comunicazione e il controllo nell'animale e nella macchina»). Nel suo romanzo Gibson definì il cyberspazio come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici. Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano».
Anche sotto il profilo giuridico, il termine cyberspazio conserva una valenza ampia e generalista. Si segnala tuttavia un primo e isolato caso di presenza della parola nella normativa nazionale in materia di sistemi di comunicazione. L'art. 7-*bis* della legge n. 70 del 2020 (di conversione con modifiche del d.l. n. 28/2020) disciplina i «Sistemi di protezione dei minori dai rischi del cyberspazio», cioè i sistemi di controllo parentale o di filtro per contenuti inadatti ai minori che per l'appunto navigano nel cyberspazio.

APPROFONDIMENTI

- Rizzi, Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in Pietrangelo (a cura di), *Lo*

Stato insicuro. Sicurezza e sorveglianza nella cybersocietà, sezione monografica della *Rivista italiana di informatica e diritto,* 2, 2024.

- Ursi (a cura di), in *La sicurezza nel cyberspazio*, Milano, 2023.

VOCI CORRELATE

CYBERBULLISMO
CYBERRESILIENZA
FATTORE UMANO
INTERNET

CYBERTERRORISMO

Per cyberterrorismo s'intende, in senso ampio, l'uso delle tecnologie informatiche e del cyberspazio per il compimento, la propaganda o la facilitazione di atti di terrorismo (da intendersi, secondo la definizione comunemente accolta, come atti di violenza, commessi per motivazioni di carattere politico, ideologico o religioso, allo scopo di ingenerare terrore nella popolazione, con ricadute sull'ordine pubblico e la sicurezza).

Diverse sono le classificazioni di atti di cyberterrorismo proposte in letteratura: (a) esclusivamente gli atti di violenza fisica realizzati per il tramite delle ICT (ad es. attacchi informatici a infrastrutture critiche con una diretta ripercussione sull'integrità fisica delle persone interessate); (b) anche gli atti di propaganda o reclutamento, rispetto ad attività o associazioni terroristiche, realizzati sfruttando le potenzialità diffusive delle ICT (ad es. i social network); (c) anche attacchi informatici capaci di determinare paura nella popolazione (ad es. mediante condotte di intrusione, controllo, ecc.), pure in assenza di un'effettiva violenza fisica.

Secondo la Guidance Note # 11 (Terrorism) accessoria alla Convenzione del Consiglio d'Europea sul *cybercrime* (Budapest, 2001) i *cybercrime* previsti dalla Convenzione medesima possano anche coincidere con atti di terrorismo. In tal senso anche la Direttiva europea 2017/541/UE sulla lotta contro il terrorismo che annovera nella nozione di "reati di terrorismo" anche la distruzione di infrastrutture informatiche, o il danneggiamento/interferenza ai danni di dati o sistemi, quando siano cagionati danni gravi o siano commessi ai danni di un sistema di informazione di un'infrastruttura critica.

APPROFONDIMENTI

- Baker-Beall, Mott, *Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis*, in *Journal of Common Market Studies*, 2022, 60, 1086 ss.

- Brenner, *Cybercrime, cyberterrorism and cyberwarfare*, in *Revue internationale de droit pénal*, 2006, 77(3), 453 ss.
- Flor, *Cyber-terrorismo e diritto penale in Italia*, in Wenin, Fornasari (a cura di), *Diritto Penale e Modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Trento, 2017, 325 ss.
- Gori, *Cyberterroristi e cybercriminali: le invisibili minacce alla sicurezza*, in *Il Politico*, 2007, LXXII, 3, 292 ss.
- Marsili, *The War on Cyberterrorism*, in *Democracy and Security*, 2018, 15(2), 172 ss.
- Tehrani, Manap, Taji, *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime*, in *Computer Law & Security Review*, 2013, 29, 3, 207 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERCRIME
CYBERDEFENCE

d

DATA BREACH (VIOLAZIONE DI DATI PERSONALI)

La *data breach* (in italiano "violazione di dati personali") è una violazione della sicurezza informatica che causa distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o, comunque, trattati. Tale violazione può essere determinata da una condotta umana, illecita e intenzionale o riconducibile a errore e disattenzione; ma può anche essere indipendente dalla volontà umana.
Le cause che determinano una *data breach* sono molto eterogenee: dalla perdita involontaria di dati personali, ai più sofisticati attacchi cibernetici, fino alle calamità naturali. In ogni caso, si tratta di una violazione da cui possono derivare danni fisici, materiali o immateriali, alle persone cui sono riferibili i dati violati. Sotto il profilo giuridico, vengono in rilievo diverse fattispecie, tra cui le condotte discriminatorie, il furto d'identità, la lesione della riservatezza, la sottrazione di segreti commerciali ecc. Particolarmente a rischio sono poi i diritti fondamentali della persona coinvolta nella violazione dei suoi dati in molti casi sensibili (si pensi al caso della violazione di un sistema informativo di ambito sanitario).
La normativa di riferimento che regola la gestione dei *data breach* è il GDPR (*General Data Protection Regulation*) o Regolamento generale sulla protezione dei dati n. 2016/679, che disciplina nel dettaglio la notifica e la gestione delle violazioni (cfr. gli articoli 33 e 34). In particolare, l'art. 33 stabilisce che il titolare del trattamento notifichi all'autorità di controllo (in Italia il Garante per la protezione dei dati personali) la violazione dei dati «senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che la violazione non sia suscettibile di creare un rischio per i diritti e le libertà delle persone fisiche».

APPROFONDIMENTI

- Calzolaio, *Protezione dei dati personali (voce*), in Digesto delle discipline pubblicistiche, 2017.

- Giordano, Lanzo, «*Data breach*» *e privacy. Quando la sicurezza dei dati personali viene compromessa. I casi decisi dal garante privacy,* Milano, 2020.
- Iaselli, *Guida alla nuova procedura di data breach*, Milano, 2021.
- Resta, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in Pietrangelo (a cura di), *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* sezione monografica della Rivista italiana di informatica e diritto, 2, 2024, 67 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)

DATI PERSONALI

I dati personali sono informazioni che permettono di identificare o rendono identificabile la persona, anche indirettamente. La nozione giuridica di dato personale richiede la compresenza di quattro elementi costitutivi:

- l'informazione, cioè il contenuto informativo del dato;
- la persona fisica, che è il soggetto cui viene collegato il contenuto informativo;
- il collegamento, inteso come operazione logica che permette di riferire l'informazione a un soggetto almeno identificabile;
- l'identificazione/identificabilità, basata su un attributo o una condizione specifica della persona fisica che assicuri il processo di identificazione (non è sufficiente un collegamento solo in astratto).

A titolo esemplificativo, sono qualificabili come dati personali: il nome e il cognome, il codice fiscale, i dati relativi all'ubicazione ecc.

In forza della diversa rilevanza giuridica per la sfera personale del soggetto cui si riferiscono, il legislatore distingue i dati personali in dati particolari e i dati giudiziari.
I dati particolari (detti anche dati sensibili) sono dati personali particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali. I dati giudiziari sono le informazioni contenute nei sistemi informativi giudiziari da cui può dedursi la qualità di imputato o indagato.
I dati non particolari (come categoria residuale rispetto ai dati particolari o sensibili e ai dati giudiziari) sono qualificati dati comuni.
I dati personali possono essere oggetto di "trattamento". Con questa espressione s'intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. A titolo d'esempio, costituiscono trattamento di dati personali: la raccolta, la registrazione, la modifica, la diffusione e l'utilizzo.

Il trattamento dei dati personali è regolato dagli artt. 6.1 e 9.2 del Regolamento generale sulla protezione dei dati n. 2016/679 (*General Data Protection Regulation* - GDPR), che stabilisce un divieto generale di trattamento, salvo i casi in esso indicati che devono rispettare le cosiddette sei "condizioni di liceità". Tra queste, rileva in particolare il consenso dell'interessato.
L'interessato è la persona fisica alla quale si riferiscono i dati personali.
Nei casi di trattamento dei dati, il titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione ecc. che adotta le decisioni sugli scopi e sulle modalità del trattamento; mentre il responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo.
I dati particolari (detti anche dati sensibili) sono dati personali particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali. Essi ineriscono ad aspetti costitutivi o strutturali dell'identità personale della persona cui si riferiscono e, quindi, necessitano di un più elevato grado di protezione giuridica. Il trattamento di tali potrebbe porre cioè rischi significativi in termini di lesione dei diritti e delle libertà fondamentali dell'interessato.

d

Il legislatore nazionale (come pure la letteratura giuridica) utilizza la formula "dati sensibili" per indicare la categoria di dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Il GDPR include in questa categoria anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
Il GDPR e la normativa nazionale vietano il trattamento di dati particolari o sensibili, perché esso può avere un impatto significativo sulla dignità. Fanno eccezione i soli casi espressamente previsti dalla stessa, tra cui il consenso esplicito dell'interessato; l'esercizio di un diritto in sede giudiziaria; la sussistenza di motivi d'interesse pubblico e la necessarietà di tutelare un interesse vitale.

APPROFONDIMENTI

- Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello,* Napoli, 2018.
- D'Orazio, Finocchiaro, Pollicino, Resta (a cura di), *Codice della privacy e data protection, Milano,* 2021.
- Finocchiaro, *Privacy e protezione dei dati personali,* Bologna, 2012.
- Rodotà, *Intervista su privacy e libertà,* Roma-Bari, 2005.

VOCI CORRELATE

DATA BREACH (VIOLAZIONE DI DATI PERSONALI)
GENERAL DATA PROTECTION REGULATION (GDPR)
INTERESSATO (DIRITTI DELL')

DEEPFAKE

Il *deepfake* è un file multimediale generato dall'intelligenza artificiale (IA), appartenente alla più ampia categoria dei *synthetic-media*, cioè contenuti sintetici. Si tratta di un contenuto falso generati tramite il *deep-learning* (specifica tecnica di "apprendimento profondo", distinta dal *machine learning,* che, utilizzando reti neurali multilivello, imita il funzionamento del cervello umano).
Il termine *deepfake* venne utilizzato per la prima volta nel 2017 sulla piattaforma Reddit da un utente che era solito pubblicare video falsificati in cui volti di donne di fama mondiale apparivano sovrapposti a corpi di attrici in film pornografici. Il neologismo è nato dall'unione delle parole inglesi "deep (learning)" e "fake (content)".

d

Il *deepfake* è quindi una foto, un video, un audio o altro contenuto multimediale generato dall'IA che, manipolando digitalmente contenuti veri, produce falsi iperrealistici. Per esempio, in un video *deepfake* una persona identificabile nella realtà pronuncia parole o compie azioni mai pronunciate o compiute.
In passato, i *deepfake* erano poco diffusi per via dell'alto costo delle tecnologie necessarie per produrli. Oggi invece sono molto diffusi, perché sono state sviluppate app e software a basso costo che rendono possibile realizzare deepfake – anche di buona qualità – comodamente dal proprio smartphone.
Dal punto di vista giuridico, un *deepfake* è un contenuto che lede i diritti fondamentali delle persone coinvolte, specie in ragione dell'estrema rapidità e facilità con cui esso può essere creato e diffuso tramite i social media a un numero indefinito di destinatari. Se utilizzate con intento malevolo, infatti, rappresentano una fonte di pericolo sia per il soggetto rappresentato nel deepfake sia per il soggetto a cui giunge il contenuto stesso.
Si consideri per esempio il *deepnude*, che è una specifica categoria di *deepfake* in cui i soggetti prescelti vengono denudati artificialmente oppure sovrapposti a volti o corpi di altri soggetti impegnati in pose o azioni a carattere esplicitamente sessuale.
Oggi il ricorso ai *deepfake* travolge tutti. Se in origine il *deep-nude* veniva utilizzato per causare un danno a personaggi noti

per screditarne la reputazione, negli ultimi tempi si assiste all'utilizzo di tale pratica anche a danno di persone le quali si scoprono vittime di azioni psicologicamente e socialmente dannose (come il cd. *revenge porn*). I *deepfake* sono impiegati per screditare l'immagine di esponenti politici, influenzando il dibattito pubblico e pilotando le campagne elettorali.
L'uso di questi strumenti ha un impatto enorme sulle democrazie contemporanee, può alimenta la sfiducia nelle istituzioni pubbliche e nelle fonti di informazione. Il *deepfake* può privare le persone della cosiddetta autodeterminazione informativa (ciò che voglio far sapere di me, lo decido io) e incidere sulla propria libertà decisionale (quello che penso e faccio è una scelta su cui gli altri non possono interferire).

APPROFONDIMENTI

- Cazzinga, *Una nuova tecnica(anche) per veicolare disinformazione: le risposte europee ai deepfakes*,* in *Media Laws,* 1, 2023, 170 ss.
- Helmus,*Artificial Intelligence, Deepfakes and Disinformation. A Primer,* RAND Corp., 6 luglio 2022, in RAND.org
- Meskys, Liaudanskas, Kalpokiene, Jurcys, *Regulating deep fakes: legal and ethical considerations,* in *Journal of Intellectual Property Law & Practice*, 15, 2020, 24 ss.
- Orlando, *La regolamentazione del deepfake in Europa, Stati Uniti e Cina, in Media Laws*, 1, 2024, 307 ss.
- Pollicino, Dunn, *Disinformazione e intelligenza artifciale nell'anno delle global election: rischi (ed opportunità),* in *Federalismi.it*, 12, 2024.

VOCI CORRELATE

AI (ARTIFICIAL INTELLIGENCE)
CYBERBULLISMO
CYBERSPAZIO
FAKE NEWS

DIGITAL FORENSIC

L'espressione *digital forensics* (in italiano letteralmente "investigazioni informatiche") allude in via generale all'uso degli strumenti digitali per finalità investigative. Gran parte delle informazioni necessarie per l'accertamento di un reato, informatico o comune, transitano nel mondo digitale ed è perciò di fondamentale importanza adeguare le tecniche investigative alle "nuove fonti" di prova, alla luce dei nuovi caratteri (immaterialità, fragilità e rischio di contaminazione) che esse presentano. Nell'ordinamento nazionale la materia è regolata dalla legge 18 marzo 2008, n. 48, di ratifica della Convenzione del Consiglio d'Europa del 2001 sulla criminalità informatica, che si prefigge di assicurare la conservazione senza alterazioni, anche successive, del dato informatico originale, la formazione di una copia conforme non modificabile dell'elemento acquisito, e l'installazione di sigilli informatici sui documenti appresi. In particolare, la modalità per preservare il dato informatico e garantirne l'autenticità consiste nel tracciare la procedura di repertamento e analisi, così da escludere alterazioni delle tracce informatiche intervenute successivamente alla creazione, trasmissione o allocazione in altro supporto (cosiddetta "catena di custodia"). Più nel dettaglio, è necessario assicurare che:

- nessuna azione sia svolta se idonea ad altera i dati direttamente o indirettamente;
- non si acceda mai direttamente ai dati sulla scena del crimine e che se una azione simile sia indispensabile per scongiurare il rischio di una perdita definitiva, chi vi accede possieda le competenze tecniche e le conoscenze giuridiche necessarie per svolgere le operazioni e, successivamente, illustrare i passaggi seguiti nelle attività informatiche;
- tutte le azioni sulla scena del crimine siano ritualmente e adeguatamente documentate, in modo tale da consentire al giudice e alle parti del processo di valutarne la correttezza e di poterle utilizzare a fini di prova;
- colui che conduce le indagini sia responsabile del rispetto di tali prescrizioni e risponda delle eventuali violazioni.

Una volta acquisito il dato informatico, è necessario garantire la sua corretta conservazione. Poiché nella dimensione digitale non esiste ovvero è sfumata la distinzione tra originale e copia, molto spesso la conservazione della prova avviene attraverso una attività di riversamento dei dati su supporti di memoria particolarmente affidabili (cosiddetta copia forense). Anche la procedura di copia dei dati deve seguire tassativamente le procedure necessarie al fine di garantire la genuinità e l'affidabilità del compendio acquisito.

APPROFONDIMENTI

- Aterno, *Digital forensics (investigazioni informatiche), voce,* in *Digesto delle discipline penalistiche,* Aggiornamento, Torino, 2009, 217 ss.
- Aterno, Cajani, Costabile, *Curtotti, Cyber forensics e indagini digitali, Torino,* 2021.
- Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa, Torino,* 2018.

VOCI CORRELATE

CYBERCRIME
CYBERJUSTICE
INVESTIGAZIONI DIGITALI
TROJAN

DIGITAL SERVICES ACT (DSA)

Il *Digital Services Act* (DSA) o Regolamento sui servizi digitali (Regolamento (UE) 2022/2065) introduce un quadro giuridico uniforme per i fornitori di servizi intermediari online — tra cui piattaforme digitali, motori di ricerca e servizi di *hosting* —, armonizzando le norme applicabili negli Stati membri. Il DSA si colloca all'interno della più ampia strategia digitale dell'Unione europea, avviata nel 2015, che comprende anche il Digital Markets Act (DMA) o Regolamento sui mercati digitali (Regolamento (UE) 2022/1925) nell'ambito del pacchetto sui servizi digitali (*Digital Services Act Package*).

L'obiettivo principale del DSA è aggiornare e ampliare il quadro normativo introdotto dalla Direttiva 2000/31/CE (Direttiva sul commercio elettronico), delineando un assetto giuridico più adeguato alle sfide poste dall'economia digitale. Il Regolamento mira a garantire un ecosistema online più sicuro per utenti e imprese, rafforzando al contempo la tutela dei diritti fondamentali nello spazio digitale.

Pur mantenendo elementi di continuità con la precedente Direttiva e-Commerce, tra cui il regime di esenzione di responsabilità per i fornitori di mera condotta, caching e hosting, seppur con alcune modifiche, il DSA introduce significative innovazioni in materia di obblighi di diligenza per i fornitori di servizi online.
Adottando un approccio asimmetrico, il nuovo regolamento stabilisce un regime di *due diligence* differenziato, in cui gli obblighi variano in base alla natura, alla dimensione e all'impatto economico del fornitore e del servizio offerto. Tra questi rientrano la trasparenza delle condizioni di utilizzo, l'implementazione di meccanismi di segnalazione e rimozione dei contenuti illegali, la tracciabilità dei venditori nei marketplace digitali e la protezione dei consumatori rispetto a prodotti o servizi illeciti.
Le piattaforme e i motori di ricerca di dimensioni molto grandi (*Very Large Online Platforms - VLOPs* e *Very Large Online Search Engines - VLOSEs*), che cioè contano almeno 45 milioni di utenti attivi mensili nell'UE, sono soggetti ad obblighi aggiuntivi, tra

cui audit indipendenti annuali, valutazioni di rischio sistemico e misure specifiche per mitigare fenomeni quali la disinformazione e la diffusione di contenuti dannosi per la salute pubblica.

APPROFONDIMENTI

- Bolognini, Pelino, Scialdone, *Digital Services Act e Digital Markets Act: definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano, 2023.
- Husovec, Roche Laguna, *Digital Services Act: A Short Primer*, in Husovec, Roche Laguna (eds), *Principles of the Digital Services Act*, Oxford, 2024.
- Wilman, Kalėda, Loewenthal, *The EU Digital Services Act*, Oxford, 2024.

VOCI CORRELATE

CYBERSPAZIO
INTERNET
SERVICE PROVIDER

DOXING

Il termine *doxing* (o *doxxing*) è un neologismo. “Dox” riprende il concetto di *dropping documents* (“divulgazione di documenti”) utilizzato a partire dagli anni Novanta dagli hacker per qualificare un’azione di vendetta nei confronti di hacker rivali. La vendetta consisteva nella raccolta e pubblicazione di informazioni allo scopo di rivelare la reale identità degli esponenti dei gruppi rivali, di solito coperta da anonimato. Dal gergo di nicchia ha poi trovato utilizzo nel più ampio contesto della criminalità informatica.

Il *doxing* non è definito a livello legislativo, né dal legislatore UE né dal legislatore nazionale. Non mancano tuttavia definizioni del fenomeno che lo inquadrano dal punto di vista giuridico, anche se si tratta di definizioni non univoche ricavabili dalle elaborazioni dottrinali. Volendo ricavare dalle molteplici definizioni proposte una definizione condivisa, si può qualificare il *doxing* come l’insieme delle azioni messe in pratica dal cd. *doxer* e finalizzate alla ricerca, raccolta e diffusione online di informazioni personali – anche sensibili – riferite ad un individuo e senza il suo consenso. Così definito, il *doxing* è una pratica diffusa soprattutto sui social media per schernire, molestare, minacciare o recare danno alla vittima e tipicamente motivata da vendette personali, conflitti ideologici o dalla volontà di offendere la vittima minandone la reputazione.

Le condotte riferibili a tale fenomeno, benché eterogenee soprattutto nel diverso grado di offesa arrecabile, sostanziano generalmente lesioni al diritto alla privacy del soggetto colpito. E così, gli attacchi di *doxing* potranno essere realizzati mediante la pubblicazione di un numero di telefono senza autorizzazione o l’invio di una lettera o di un pacco da parte di uno sconosciuto, ma potranno anche configurare gravi reati come il furto d’identità, la frode, finanche il reato di molestie. Ancora, potranno essere strumentali al compimento di atti riconducibili al fenomeno del cyberbullismo.

APPROFONDIMENTI

- Chen, Cheung, Chan, *Doxing: What Adolescents Look for and Their Intentions,* in *Int. J. Environ. Res. Public Health,* 16(2), 2019, 218 ss.
- Douglas*, Doxing: a conceptual analysis* in *Ethics Inf Technol*, 2016 (18), 199 ss.
- Kukul, *Personal data and personal safety: re-examining the limits of public data in the context of doxing* in *International Data Privacy Law*, 13 (3), 2023, 182 ss.

VOCI CORRELATE

CYBERBULLISMO
CYBERCRIME
CYBERSPAZIO
DATI PERSONALI

DUAL USE

Si definiscono *dual use* i beni suscettibili di essere utilizzati per applicazioni sia civili sia militari. Tra i beni *dual use* rientrano anche le tecnologie digitali e, in particolare, i software utilizzabili ad es. per realizzare attacchi di carattere distruttivo o intrusivo.

A livello europeo, la più recente disciplina dei prodotti *dual use* si rinviene nel Regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce un regime di controllo dell'esportazione, del transito e del trasferimento di prodotti *dual use*.

Nell'elenco dei prodotti *dual use* (Allegato I al Regolmento), la cui esportazione è soggetta ad autorizzazione, rientrano anche alcuni beni cyber, riconducibili alle categorie dei "Calcolatori" (Categoria 4: ad es. calcolatori progettati per funzionare a determinate temperature, molto basse o molto elevate) e "Telecomunicazioni e sicurezza dell'informazione" (Categoria 5: ad es. sistemi di crittografia con determinate caratteristiche).

Tra i beni espressamente disciplinati dal Regolamento, rientrano in particolare i prodotti di sorveglianza informatica (*cyber-surveillance*), definiti come prodotti «appositamente progettati per consentire la sorveglianza dissimulata di persone fisiche mediante il monitoraggio, l'estrazione, la raccolta o l'analisi di dati provenienti da sistemi di informazione e telecomunicazione». L'esportazione di questi prodotti è soggetta ad autorizzazione nel caso in cui essi siano o possano essere destinati, in tutto o in parte, a un uso connesso alla repressione interna o all'attuazione di gravi violazioni dei diritti umani o del diritto umanitario internazionale.

APPROFONDIMENTI

- Du Bois, Tapia Reyes, *Dual-use and cyber-surveillance: EU policies and current practices*, 2023.

- Grinbaum, Adomaitis, Dual use concerns of generative AI and large language models, in *Journal of Responsible Innovation*, 2024, 11(1).
- Passaglia (a cura di), *Le due facce della rivoluzione digitale, tra emergenze e tecnologie dual-use*, sezione monografica della *Rivista italiana di informatica e diritto,* 2, 2025.
- Ramella, Irlando, *Normativa dell'Ue inerente i beni a duplice uso e prodotti cyber*, in *GeoTrade: Rivista di geopolitica e commercio estero*, 2023, 7, 8 ss.
- Riebe, Reuter, *Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment*, in Reuter (a cura di), *Information Technology for Peace and Security*, Wiesbaden, 2019, 165 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERDEFENCE
CYBERTERRORISMO
MALWARE

E-PROCUREMENT

L'*e-procurement* (*electronic procurement*) è un sistema digitalizzato impiegato per le procedure di acquisto di beni e sevizi in modo più efficiente. Utilizzano questi sistemi sia i soggetti privati che le amministrazioni pubbliche. In particolare, per il settore degli appalti e delle concessioni pubbiche, la normativa prescrive la completa digitalizzazione delle procedure, dall'acquisto fino all'esecuzione finale del contratto.
Il nuovo Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36) ha disciplina alcuni profili critici della digitalizzazione della commessa pubblica, legati alla riduzione e certezza dei tempi delle procedure di gara, alla stipula dei contratti e all'esecuzione degli appalti. Per supportare questo percorso, il Codice dispone che sia data piena attuazione alla *Banca dati nazionale dei contratti pubblici* gestita dall'Autorità nazionale anticorruzione (ANAC) e al *Fascicolo virtuale dell'operatore economico*. Secondo la nuova normativa, inoltre, le stazioni appaltanti possono utilizzare procedure automatizzate anche nella valutazione delle offerte.
Il sistema di *e-procurement* definito nel Codice dei contratti pubblici è un sistema *end-to-end* , che si basa sulla integrazione e interoperabilità tra piattaforme digitali, col fine di ridurre tempi e costi delle attività e la partecipazione di nuovi operatori economici. La nuova disciplina codicistica (Parte II del Libro I, artt. 19-29) segue gli indirizzi già definiti col Piano Nazionale di Ripresa e Resilienza (PNRR) ed è conforme agli orientamenti eurounionali, che sono riassumibili in alcuni principi generali: il principio *digital by defaul*t (i servizi pubblici sono erogati in modalità digitale); il principio *interoperability by default* (i servizi pubblici sono progettati per funzionare in tutto il mercato unico); il principio *once only* (i cittadini e le imprese forniscano informazioni alle pubbliche amministrazioni "una sola volta"); il principio *cross-border by default* (i servizi pubblici digitali pertinenti a livello transfrontaliero sono accessibili e disponibili, per supportare la mobilità all'interno del mercato unico).

APPROFONDIMENTI

- Carlotti, *I principi nel Codice dei contratti pubblici: la digitalizzazione,* in *Giustizia amministrativa.it,* 2023.
- Clarizia, *La digitalizzazione dell'intero ciclo di vita dell'appalto*, in Macchia (a cura di) *Costruire e acquistare. Lezioni sul nuovo Codice dei contratti pubblici*, Torino, 2024, 77 ss.
- Tallaro*, La digitalizzazione del ciclo dei contratti pubblici,* in *Giustizia amministrativa.it,* 2023.

VOCI CORRELATE

CENTRALI DI COMMITTENZA
STAZIONI APPALTANTI

e

EU-CYCLONE (EUROPEAN CYBER CRISIS LIAISON ORGANISATION NETWORK)

L'*European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe) è la rete europea delle organizzazioni di collegamento per le crisi informatiche cui che gestisce le emergenze causate da incidenti informatici su vasta scala. L'"incidente di cybersicurezza su vasta scala" è definito nella Direttiva 2022/2555 (NIS 2) quale «incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi, o che ha un impatto significativo su almeno due Stati membri» (art. 6, n. 7, Direttiva NIS 2).
L'EU-CyCLONe è stata istituita gestire in modo coordinato gli incidenti e le crisi di cybersicurezza su vasta scala, garantendo il regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'Unione nonché sostenendo il processo decisionale politico in merito a tali incidenti o crisi (art. 16, Direttiva NIS 2).
La Rete, il cui segretariato è svolto dall'*European Union Agency for Cybersecurity* (ENISA), è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri (ad es. per l'Italia l'Agenzia per la cybersicurezza nazionale e il *Computer Security Incident Response Team Italia*). Il funzionamento interno della Rete è disciplinato da un apposito Regolamento adottato dalla stessa.
La Commissione europea può partecipare alle attività della Rete come osservatore, salvo acquisire la qualità di membro effettivo nei casi in cui un incidente di cybersicurezza su vasta scala potenziale o in corso abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nel campo applicativo della disciplina NIS (ad es. pubbliche amministrazioni, settore bancario, sanitario, idrico ecc.). L'EU-CyCLONe può invitare anche i rappresentanti dei pertinenti portatori di interessi a partecipare ai suoi lavori in qualità di osservatori.
L'EU-CyCLONe è sottoposta al controllo di Parlamento europeo e Consiglio, ai quali ogni 18 mesi presenta una relazione sulle proprie attività.

APPROFONDIMENTI

- Bendiek, The EU as a force for peace in international cyber diplomacy, in *Stiftung Wissenschaft und Politik*, 19, 2018.
- Fysarakis, Mavroeidis, Athanatos, Spanoudakis, Ioannidis, *A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint*, in *IEEE International Conference on Big Data (Big Data)*, 2022.
- Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, 4, 2022.
- Serini, *Collective cyber situational awareness in EU. A political project of difficult legal realisation?*, in *Computer Law & Security Review*, vol. 55, 2024.

VOCI CORRELATE

e

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)
GRUPPO DI COOPERAZIONE PER LE RETI E I SISTEMI INFORMATIVI
NIS (DIRETTIVE NIS)

EUROPEAN DATA PROTECTION BOARD (EDPB)

L'*European Data Protection Board* (EDPB) è il Comitato europeo per la protezione dei dati. Si tratta di un organismo indipendente dell'Unione europea, dotato di personalità giuridica, istituito con il Regolamento generale sulla protezione dei dati n. 2016/679 (*General Data Protection Regulation* - GDPR), artt. 68 e 76, in sostituzione del precedente Working Party 29 (WP29), ossia il Gruppo di lavoro istituito con l'art. 29 della previgente disciplina europea sulla protezione dei dati personali (la Direttiva 45/95/CE).

L'EDPB è composto dai rappresentanti delle autorità di protezione dei dati di ciascun Paese dell'UE (ad es. per l'Italia è il Garante per la protezione dei dati personali), insieme al Garante europeo della protezione dei dati (EDPS) che partecipa con diritto di voto. Il Comitato è guidato da un presidente eletto, coadiuvato da un segretariato che gestisce i compiti amministrativi e operativi.

Il principale compito del Comitato è quello di garantire l'applicazione uniforme del GDPR in tutti gli Stati membri promuovendo la cooperazione tra le Autorità garanti nazionali. A tal fine l'EDPB emana linee guida, raccomandazioni e buone pratiche che aiutano le autorità nazionali e le organizzazioni private a comprendere e applicare correttamente il GDPR. Questi documenti sono particolarmente importanti per affrontare questioni interpretative complesse e per tenere il passo con l'evoluzione tecnologica.
Il Comitato ha anche il compito di risolvere le controversie che possono sorgere tra le autorità di protezione dei dati nazionali, specialmente nel caso di traffico transfrontaliero di dati.
Attraverso il suo ruolo di supervisione, garantisce che le decisioni prese in questi contesti siano coerenti e rispettino i principi del GDPR.
Un'altra funzione chiave è quella di fornire consulenza alla Commissione europea e ad altre istituzioni dell'UE su proposte legislative e accordi internazionali che riguardano la protezione dei dati personali. Infine, l'EDPB monitora costantemente le

nuove tecnologie e i cambiamenti sociali per valutare il loro impatto sulla protezione dei dati personali. Questo gli permette di rimanere aggiornato e di adattare le sue indicazioni alle nuove sfide, come l'intelligenza artificiale, la biometria e la profilazione.

Il Comitato è inoltre competente circa la corretta applicazione e nell'emanazione di linee guida per il trattamento dei dati personali da parte delle forze di polizia nell'Unione (Dir. (UE) 2016/680).

Esercitano una forma di controllo sull'operato dell'EDPB la Corte di giustizia dell'Unione europea (CGUE), che garantisce la conformità al diritto UE delle decisioni dell'EDPB; il Parlamento europeo, che monitora l'efficacia delle attività dell'EPDB e può chiedere relazioni o chiarimenti; e la Corte dei conti europea, per la verifica sull'uso delle risorse finanziarie assegnate al Comitato.

Il Comitato, come gli altri organismi UE, è soggetto alla disciplina europea sul trattamento dei dati personali da parte delle istituzioni dell'Unione (Regolamento (UE) 2018/1725).

APPROFONDIMENTI

- Calzolaio, Longo, Iannuzzi, Orofino, *La regolazione europea della società digitale*, Torino, 2024.
- Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il regolamento europeo 2016/679,* Torino, 2016.
- Solove, Schwartz, *EU Data Protection and the GDPR*, Aspen Publishing, 2023.

VOCI CORRELATE

DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
INTERESSATO (DIRITTI DELL')

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

L'*European Union Agency for Cybersecurity* (ENISA) è l'Agenzia dell'Unione europea per la cybersicurezza con sede principale ad Atene (altri uffici sono a Heraklion e Bruxelles). Si tratta di un organismo indipendente dell'Unione dotato di personalità giuridica. Istituita nel 2004 sulla base di un mandato temporaneo (Reg. (CE) n. 460/2004), via via esteso nel tempo (Reg. (UE) n. 1007/2008; Reg. (UE) n. 580/2011; Reg. (UE) n. 526/2013), l'Agenzia ha acquisito natura permanente solo nel 2019 con il Regolamento (UE) 2019/889 (*Cybersecurity Act*).
Circa la sua struttura amministrativa, l'Agenzia è composta dal consiglio di amministrazione; dal comitato esecutivo; dal direttore esecutivo, che risponde al consiglio di amministrazione; da una rete di funzionari nazionali di collegamento e dal gruppo consultivo ENISA, composto da esperti riconosciuti che rappresentano i diversi portatori di interessi.

Il *Cybersecurity Act* del 2019 ha rafforzato il potere e incrementato le funzioni dell'ENISA, prevedendo anche lo stanziamento di maggiori risorse per il bilancio dell'Agenzia a fronte delle crescenti minacce informatiche in Europa. La missione dell'ENISA è quella creare un clima di fiducia verso l'utilizzo delle tecnologie dell'informazione e della comunicazione e di assicurare un elevato livello di cybersicurezza in tutta l'Unione, contribuendo in tal modo al buon funzionamento del mercato interno. A tal proposito, l'ENISA fornisce supporto tecnico e operativo agli Stati membri e alle istituzioni europee, promuove la collaborazione tra i vari attori del settore e favorisce l'adozione di normative e standard comuni per affrontare le minacce cibernetiche. Con riguardo alla normazione tecnica, spetta all'ENISA promuovere l'uso della certificazione europea di cybersicurezza e contribuire all'istituzione e al mantenimento di un apposito quadro europeo di certificazione in materia (EUCC).

All'Agenzia sono assegnati anche funzioni di assistenza e consulenza per la promozione, lo sviluppo e la revisione delle

politiche e delle normative europee di cybersicurezza, nonché di assistenza agli Stati membri nell'attuazione uniforme di tali atti, mediante pareri, orientamenti e consigli.
L'ENISA svolge, inoltre, attività di formazione, ricerca e sensibilizzazione per migliorare le capacità di prevenzione, rilevamento e risposta agli attacchi informatici.

Con l'evoluzione del quadro legislativo europeo in materia di cybersicurezza nuovi e ulteriori sono i compiti assegnati all'ENISA. Ai sensi della Direttiva NIS 2 (artt. 14 e 16 Direttiva (UE) 2022/2555), l'ENISA è parte del Gruppo di cooperazione, la cui funzione è quella di agevolare la cooperazione strategica e lo scambio di informazioni, svolge la funzione di segretaria della Rete europea delle organizzazioni di collegamento per le crisi informatiche, ed inoltre è responsabile della tenuta e della sicurezza della banca dati europea delle vulnerabilità.
Il *Cyber Resilience Act* (Regolamento (UE) 2024/2847, artt. 14 e 15) prevede che l'Agenzia sia destinataria delle notifiche da parte di fabbricanti di prodotti ICT relativamente alle "vulnerabilità attivamente sfruttate" contenute nei prodotti con elementi digitali, oppure delle vulnerabilità dei prodotti (non attivamente strutturate) notificate su base volontaria.
Il *Cyber Solidarity Act* (Regolamento (UE) 2025/38) attribuisce all'ENISA il compito di svolgere analisi di valutazione degli incidenti di cybersicurezza significativi e su vasta scala al termine del quale è tenuta a redigere il relativo rapporto di revisione dell'incidente, in collaborazione con le parti interessate, compresi i rappresentanti del settore privato, degli Stati membri, della Commissione e di altre istituzioni, organi e agenzie pertinenti dell'UE.
Avendo un ruolo di coordinamento e di assistenza, è presumibile che il quadro normativo in materia di cybersicurezza assegni all'Agenzia ulteriori funzioni oltre quelle qui sintetizzate.

APPROFONDIMENTI

- Calzolaio, *Autorità indipendenti e di governo della società digitale*, in Calzolaio, Longo, Iannuzzi, Orofino, Torino, *La regolazione europea della società digitale*, 2024, 83 ss.

- Cavelty, Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authorit*y, in *Journal of European Public Policy*, Vol. 30, 2023.

VOCI CORRELATE

EU-CYCLONE (EUROPEAN CYBER CRISIS LIAISON ORGANISATION NETWORK)
GRUPPO DI COOPERAZIONE PER LE RETI E I SISTEMI INFORMATIVI
NIS (DIRETTIVE NIS)

f

FAKE NEWS

Locuzione inglese (lett. notizie false o informazioni false, fasulle, inventate, manipolate, quindi come sinonimo di disinformazione) con la quale si indica un'informazione o una notizia parzialmente o interamente non corrispondente al vero che viene diffusa, in maniera più o meno intenzionale, attraverso il web, i media o le tecnologie digitali di comunicazione come i social network.

Le fake news si caratterizzano per un'apparente credibilità che viene incrementata dalle aspettative alterate dell'opinione pubblica e dai pregiudizi costitutivi della stessa notizia falsa, con ciò determinandosi una significativa facilità di condivisione e diffusione in assenza di qualunque verifica della fondatezza e delle fonti.
Questo neologismo ha conosciuto una rapida diffusione specialmente in ambito politico a partire dal 2016 (vedi il referendum sulla Brexit nel Regno Unito del 23 giugno o l'elezione di Trump alla Casa Bianca l'8 novembre), rappresentando uno dei riflessi più importanti del tema della postverità, da intendersi come pseudoverità costruita su scelte individuali e collettive basate essenzialmente sull'emotività e sulle convinzioni condivise dall'opinione pubblica, quindi prescindendo (parzialmente o del tutto) dalla conformità con il reale.

Sotto il profilo giuridico, è bene precisare che una fake news non costituisce di per sé illecito penale. Perché rilevi come fattispecie penale (reati di diffamazione, turbativa dell'ordine pubblico, procurato allarme) è necessario un nesso causale tra la fake news e l'illecito sanzionato dalla legge. Infatti, un elemento essenziale del rapporto tra fake news e diritto (penale in particolare) è dato dalla necessità di un corretto bilanciamento tra il diritto di manifestare liberamente il proprio pensiero (protetto dall'art 21 della Costituzione e dall'art. 10 della Convenzione europea dei diritti dell'uomo) e altri diritti fondamentali della persona come, ad esempio, l'onore.
Risulta così necessario valutare adeguatamente quando l'espressione del pensiero oltrepassi i confini del diritto alla libera manifestazione dello stesso prevista dalla Costituzione e

determini un illecito penale, vale a dire in quali casi non si tratti più soltanto di formulare opinioni personali, convinzioni o giudizi, bensì ci si trovi di fronte a notizie false che possono assumere conseguenze giuridiche proprio laddove l'affermazione di una falsità integri alcune fattispecie penali.
Per alcuni reati cioè la diffusione di fake news rappresenta la condotta tipica della fattispecie penale, ad esempio nel caso di disfattismo politico (art. 265 c.p.) o di pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico (art. 656 c.p.) o ancora di procurato allarme presso l'Autorità (art 658 c.p.). In latri casi, la divulgazione di notizie false può integrare la condotta tipica, ma non ne costituisce l'unica configurazione, come nel reato di diffamazione (art. 595 c.p.).

APPROFONDIMENTI

- Califano, *La libertà di manifestazione del pensiero... in rete; nuove frontiere di esercizio di un diritto antico. Fake news, hate speech e profili di responsabilità dei social network*, in *Federalismi.it*, 26, 2021.
- Flaminio, *Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act*, in *Rivista italiana di informatica e diritto*, 2, 2022.
- Guerini, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, 2020.
- Magnani, *Libertà di espressione e fake news, il difficile rapporto tra verità a diritto. Una prospettiva teorica*, in *Costituzionalismo.it*, 3, 2018.
- Pinelli, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto pubblico*, 1, 2022.

VOCI CORRELATE

CYBERSPAZIO
DIGITALE SERVICE ACT (DSA)
INTERNET
REPUTAZIONE

FATTORE UMANO

Il termine fattore umano si riferisce al ruolo che le dinamiche comportamentali e decisionali umane rivestono nell'ambito della sicurezza informatica. Nel settore della cybersicurezza, infatti, alla centralità della tecnologia deve necessariamente affiancarsi la responsabilità degli utenti nel suo concreto utilizzo. Le vulnerabilità legate al fattore umano - come l'utilizzo di password deboli, il clic imprudente su link dannosi o la condivisione inconsapevole di dati sensibili - possono facilmente essere sfruttate da attori malevoli.
Tuttavia, il fattore umano non è soltanto una fonte di rischio: se adeguatamente formato e sensibilizzato, può trasformarsi in una risorsa strategica per la sicurezza. Attraverso programmi di formazione mirati, campagne di *awareness* efficaci e la promozione di una solida cultura della cybersicurezza, gli utenti possono diventare una vera e propria "linea di difesa", contribuendo in modo attivo alla prevenzione degli attacchi e alla protezione delle risorse digitali. La cybersicurezza, dunque, non può affidarsi unicamente a soluzioni tecnologiche, ma richiede un costante investimento nella crescita della consapevolezza e delle competenze degli individui.
Per mitigare i rischi associati al fattore umano risulta indispensabile riconoscere come il dominio della sicurezza informatica non si limiti all'ambito puramente tecnico, ma richieda una consapevolezza proattiva ed una assunzione di responsabilità sui rischi connessi all'uso degli strumenti informatici.

APPROFONDIMENTI

- Camisa, Simoncini, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, 2024.
- Corradini, *Il fattore umano nella sicurezza informatica: il ruolo chiave della consapevolezza*, in *Rivista di scienze dell'educazione*, 56(2), 2018.
- Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in Pietrangelo (a cura di), *Lo Stato insicuro. Sicurezza e sorveglianza nella*

cyber società, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 2024,13 ss.

- Sotira, *Il fattore umano nella cybersecurity: valori e strategie da costruire insieme*, Milano, 2020.

VOCI CORRELATE

INGEGNERIA SOCIALE
INTERNET
PHISHING

f

FIREWALL

Il termine inglese *firewall* qualifica un sistema di sicurezza informatica perimetrale in grado di stabilire quali dati possono o non possono passare dalla rete internet esterna alla rete interna del singolo dispositivo. Tradotto in italiano con "muro tagliafuoco" (una parete costruita all'interno di un edificio al fine di evitare la propagazione di un incendio), i *firewall* informatici svolgono una funzione simile nel loro contesto di applicazione: come fossero un filtro, se ben configurati, sono in grado di mantenere la rete interna sicura controllando il traffico dati in uscita e in entrata, facendo passare solo i dati che rispettano determinate regole e bloccando i dati o i file potenzialmente dannosi.

I *firewall* possono essere: (a) software, programma informatico installabile su ogni dispositivo elettronico (quasi tutti i sistemi operativi comprendono già al loro interno un *firewall*); (b) hardware, dispositivo fisico e autonomo, come un router, dotato di porte a cui i dispositivi di una rete possono essere direttamente connessi.

APPROFONDIMENTI

- Aterno, *Sicurezza informatica: aspetti giuridici e tecnici,* Pisa, 2022.
- Cheswick, Bellovin, Rubin, *Firewall e sicurezza in rete*, Milano, 2003.
- Stewart, Kinsey, *Network Security, Firewalls, and VPNs*, Burlington, 2020.

VOCI CORRELATE

CYBERSPAZIO
MALWARE
MISURE DI SICUREZZA

FIRMA DIGITALE

La firma digitale è un tipo di firma elettronica qualificata basata su una particolare tecnologia: il metodo di crittografia a doppia chiave.
La normativa di riferimento colloca la firma digitale tra le firme elettroniche insieme alla firma elettronica semplice, alla firma elettronica avanzata e alla firma elettronica qualificata. In generale, il termine firma elettronica identifica una sequenza binaria riconducibile al soggetto solo per mezzo di una procedura informatica che permette di certificare la paternità del documento informatico sottoscritto. È legata al contenuto del documento in modo indissolubile, valutabile solo attraverso strumenti informatici ed ha validità temporale limitata.
Secondo il d.lgs n. 82/2005 (Codice dell'amministrazione digitale) la firma elettronica è un insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica.
In particolare, per generare una firma digitale è necessario l'utilizzo di una coppia di chiavi asimmetriche fornite al titolare della firma: la cd. *chiave privata* è usata dal soggetto titolare e permette di apporre la firma digitale; e la cd. *chiave pubblica* utilizzata per la verifica dell'autenticità della firma digitale stessa, chiave che è destinata ad essere resa pubblica. Le due chiavi sono correlate, ma allo stesso tempo indipendenti, perché la chiave pubblica corrispondente permette di decifrare la chiave privata, ma essa - la chiave pubblica, conoscibile da chiunque - non permette di risalire alla chiave privata, che è nota solo al titolare. Questo meccanismo rende particolarmente sicura la sottoscrizione con firma digitale.
La crittografia asimmetrica utilizzata per la creazione di una firma digitale, infatti, assicura: (a) integrità, e quindi la certezza che il documento non sia stato manomesso o modificato dopo la sottoscrizione; (b) paternità, garanzia dell'identità del firmatario; (c) non ripudio, poiché il documento informatico sottoscritto ha piena validità legale e non può essere ripudiato dal firmatario; (d) autenticazione e identificazione della provenienza del documento sottoscritto.
La firma digitale, inoltre, si basa su un certificato qualificato rilasciato da un soggetto terzo garante – il cd. prestatore di

servizi fiduciari qualificato – che certifica l'identità del firmatario, assicurando un'attività di controllo a valle. Si tratta di funzioni svolte da soggetti che per legge sono essi stessi sottoposti a tutta una serie di obblighi di qualità e sicurezza e a specifiche responsabilità.
Il Regolamento eIDAS (*electronic IDentification and trust Services for electronic transactions in the internal market*) n. 910/2014 ha previsto l'obbligo di riconoscere le firme elettroniche qualificate negli Stati membri, così stabilendo la piena interoperabilità nell'Unione europea di particolari tipologie di firme elettroniche, tra cui in Italia la firma digitale. L'art. 25, co. 3 di tale regolamento prevede, infatti, che «Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri».
Dal punto di vista dell'efficacia probatoria, a norma del d.lgs. n. 82/2005 (art. 21) e del Regolamento eIDAS la firma digitale garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del Codice civile. Inoltre, l'uso del dispositivo di firma digitale si presume riconducibile al titolare, salvo prova contraria.

APPROFONDIMENTI

- Finocchiaro, *Firma digitale e firme elettroniche. Profili privatistici*, Milano, 2003.
- Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014* (cd. "Eidas"): identificazione "on line", firme elettroniche e servizi fiduciari (reg. UE n. 910/2014), in *Le Nuove leggi civili commentate*, 3, 2015, 419 ss.
- Ortalda, Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Rivista italiana di informatica e diritto*, 1, 2022, 145 ss.
- Rizzo, *Le firme elettroniche nel Regolamento eIDAS 2. La falsità della firma digitale*, in *Contratto e impresa*, 1, 2025, 95 ss.

VOCI CORRELATE

CRITTOGRAFIA
IDENTITÀ DIGITALE
SISTEMA PUBBLICO DI IDENTITÀ DIGITALE (SPID)

f

g

GENERAL DATA PROTECTION REGULATION (GDPR)

Il *General Data Protection Regulation* (GDPR) o Regolamento generale per la protezione dei dati personali n. 2016/679 è la principale normativa di diritto dell'UE in materia di protezione dei dati personali. Questo regolamento rappresenta un significativo passo in avanti nella tutela della protezione dei dati dei diritti degli individui all'interno dell'Unione europea, diritto fondamentale altresì sancito all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea.

Il GDPR è stato adottato il 27 aprile 2016 e pubblicato nella Gazzetta ufficiale dell'Unione europea il 4 maggio 2016. È entrato in vigore il 24 maggio 2016, con l'obbligo di attuazione da parte degli Stati membri a partire dal 25 maggio 2018. Il regolamento è composto da 99 articoli, che stabiliscono diritti e obblighi in materia di protezione dei dati personali, e da 173 considerando, che forniscono il contesto e le motivazioni alla base delle disposizioni normative, pur avendo solo un valore interpretativo. Essendo un regolamento, il GDPR è direttamente applicabile in tutti gli Stati membri dell'Unione europea senza necessità di recepimento tramite legislazioni nazionali. Ciò garantisce una uniformità della tutela dei dati personali in tutta l'Unione europea e l'eliminazione delle discrepanze che esistevano precedentemente tra le varie legislazioni nazionali. Ciononostante, il regolamento prevede alcune aree in cui sono lasciati margini di discrezionalità agli Stati membri che consentono deroghe e adattamenti specifici alle proprie normative nazionali.

Il GDPR introduce importanti principi e requisiti per la protezione dei dati personali, tra cui la liceità, la correttezza e la trasparenza del trattamento dei dati, la limitazione delle finalità, la minimizzazione dei dati, l'accuratezza, la limitazione della conservazione e l'integrità e riservatezza dei dati. Inoltre, il regolamento stabilisce nuovi diritti per i soggetti interessati, come il diritto all'oblio, il diritto alla portabilità dei dati e il diritto di opporsi al trattamento dei propri dati personali.

L'obiettivo principale del GDPR è rafforzare e armonizzare la protezione dei dati personali per tutti gli individui all'interno dell'Unione europea. Il GDPR mira a garantire che i dati personali siano trattati in modo lecito, equo e trasparente, proteggendo così i diritti e le libertà individuali. Inoltre, esso impone rigorosi obblighi a chi intende trattare i dati personali, come ad esempio la predisposizione di misure di sicurezza, la notifica delle violazioni dei dati, la valutazione d'impatto sulla protezione dei dati e la nomina di un responsabile della protezione dei dati (DPO) in determinate circostanze.
Le sanzioni per la non conformità possono essere severe, includendo multe fino a 20 milioni di euro o il 4% del fatturato globale annuo dell'organizzazione, a seconda di quale sia l'importo maggiore.

APPROFONDIMENTI

- Cirone, *La dimensione extraterritoriale della protezione dei dati nella recente giurisprudenza della Corte di giustizia: uno strumento di promozione dei valori dell'Unione?*, in Nascimbene, Greco (a cura di), *I grands arrêts della Corte di giustizia dell'Unione europea negli ultimi dieci anni: attualità e problemi aperti*, Milano, 2025, 47 ss.
- Riccio, Scorza, Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2022.
- Sciaudone (a cura di), *Commentario al codice della privacy,* Pisa, 2023.
- Voigt, Von dem Bussche, *The EU General Data Protection Regulation*, Berlin, 2024.

VOCI CORRELATE

DATA BREACH (VIOLAZIONE DI DATI PERSONALI)
DATI PERSONALI
EUROPEAN DATA PROTECTION BOARD (EDPB)
INTERESSATO (DIRITTI DELL')
OBLIO (DIRITTO ALL')

GENERAL PURPOSE AI (GPAI)

Il *General Purpose AI Model* (GPAI) è un *foundation model* di intelligenza artificiale (IA), in italiano identificabile come modello di IA per finalità generali.
Esso è attualmente definito nell'*AI Act* (Regolamento UE 2024/1689) come «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato» (art. 3, n. 63).
In termini più semplici, i modelli GPAI sono modelli di intelligenza artificiale che, grazie all'addestramento basato su grandi quantità di dati, sono capaci di affrontare diversi tipi di compiti. Tali modelli possono essere utilizzati da soli oppure come componenti inseriti all'interno di altri sistemi di IA. Non rientrano in questa definizione i modelli che sono ancora in fase di ricerca, sviluppo o prototipazione, purché non siano ancora stati immessi sul mercato.
L'*AI Act* distingue due categorie all'interno dei modelli GPAI: da una parte vi sono i modelli generici, dall'altra quelli che presentano rischi sistemici. Questi ultimi, a causa della loro potenziale incidenza su scala europea, sono sottoposti a una regolamentazione più rigorosa rispetto ai primi.
In linea generale, tutti i modelli GPAI sono soggetti ad alcuni obblighi comuni. In particolare, è richiesta la garanzia di un adeguato livello di trasparenza, la nomina di un rappresentante stabilito nell'Unione europea che possa fungere da interlocutore ufficiale con le autorità competenti, l'assicurazione del rispetto delle norme in materia di diritto d'autore.
Per quanto riguarda i modelli GPAI considerati a rischio sistemico, il quadro regolatorio si intensifica. Questi modelli devono adempiere non solo agli obblighi previsti per i modelli generici, ma anche a ulteriori doveri sostanziali. In particolare,

devono effettuare una valutazione tecnica del modello seguendo protocolli e strumenti standardizzati che riflettano lo stato dell'arte. Per questi modelli è necessario analizzare e mitigare i potenziali rischi sistemici a livello dell'Unione, individuando anche le fonti di tali rischi. In caso di incidenti gravi, è previsto l'obbligo di raccogliere, documentare e trasmettere senza indebito ritardo tutte le informazioni rilevanti all'AI Office o, in alternativa, alle autorità nazionali competenti, indicando anche le eventuali misure correttive adottate. Infine, tali modelli devono essere progettati in modo da assicurare un livello adeguato di protezione in materia di cybersicurezza, sia per quanto riguarda il modello stesso che per l'infrastruttura fisica che ne consente il funzionamento.

APPROFONDIMENTI

- Cosentini, Pollicino *et al.*, *Assessing the Impact of Artificial Intelligence Systems on Fundamental Rights, Medialaws,* 2025, 1 ss.
- Mantelero, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template*, in *Computer Law & Security Review*, 2024, 1 ss.
- Orofino, *La regolazione dei modelli di IA per finalità generali,* in Calzolaio, Iannuzzi, Longo, Orofino, Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale,* Torino 2025, 95 ss.

VOCI CORRELATE

AI (ARTIFICIAL INTELLIGENCE)
AI ACT (ARTIFICIAL INTELLIGENCE ACT)
REGULATORY SANDBOX
RISK BASED APPROACH

GRUPPO DI COOPERAZIONE PER LE RETI E I SISTEMI INFORMATIVI

Il Gruppo di cooperazione per le reti e i sistemi informativi è stato istituito con la Direttiva NIS 1 e poi riconfermato dall'art. 14 della successiva NIS 2 (Direttiva 2022/2555). Esso garantisce la cooperazione e lo scambio di informazioni tra gli Stati membri e fornisce orientamenti strategici alla rete di CSIRT e a EU–CyCLONe.

Il Gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione (che svolge il ruolo di segretariato) e dell'*European Union Agency for Cybersecurity* (ENISA). Alle sue attività partecipano altri soggetti istituzionali: il Servizio europeo per l'azione esterna (SEAE) con funzioni di osservatore; le Autorità europee di vigilanza (AEV) e le Autorità competenti DORA per le sole questioni relative alla vigilanza sulle entità finanziarie (come previsto dall'art. 47, par. 1, del Regolamento (UE) 2022/2554 sulla resilienza operativa digitale per il settore finanziario (DORA); se ritenuto opportuno, il Parlamento europeo e i rappresentanti dei pertinenti portatori di interessi.

Per quanto riguarda i profili di funzionamento interno, la Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del Gruppo, mentre circa i profili di controllo, il Gruppo presenta relazioni alla Commissione, al Parlamento europeo e al Consiglio sull'esperienza acquisita a livello strategico.

APPROFONDIMENTI

- Bendiek, *The EU as a force for peace in international cyber diplomacy*, in *Stiftung Wissenschaft und Politik*, 19, 2018.
- Fysarakis, Mavroeidis, Athanatos, Spanoudakis, Ioannidis, *A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness,* in *IEEE International Conference on Big Data (Big Data)*, 2022.

- Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, 4, 2022.
- Serini, *Collective cyber situational awareness in EU. A political project of difficult legal realisation?*, in *Computer Law & Security Review*, 55, 2024.

VOCI CORRELATE

EU-CYCLONE (EUROPEAN CYBER CRISIS LIAISON ORGANISATION NETWORK)
EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)
NIS (DIRETTIVE NIS)

h

HACKER

Il termine hacker ha subito una progressiva evoluzione nel tempo, riflettendo i cambiamenti tecnologici e culturali nel mondo dell'informatica. Le sue origini risalgono agli anni Sessanta, all'interno del Massachusetts Institute of Technology (MIT), dove veniva impiegato con una connotazione positiva per descrivere studenti dotati di elevate competenze tecniche, capaci di "padroneggiare" la tecnologia e di esplorarne ogni potenzialità con creatività e ingegno. Con il passare dei decenni, tuttavia, il significato del termine ha iniziato a trasformarsi, acquisendo nuove sfumature. A partire dagli anni Settanta e Ottanta, alcuni individui hanno iniziato a utilizzare le proprie competenze per accedere ai sistemi informatici senza autorizzazione, inizialmente per curiosità o sfida personale, e successivamente anche con finalità di lucro. La crescente attenzione mediatica verso questi episodi ha progressivamente associato il termine hacker a un'accezione negativa, facendolo diventare sinonimo di trasgressore digitale: una figura che sfrutta le proprie abilità per violare, danneggiare o trarre vantaggio illecito dai sistemi informatici.

Secondo la letteratura criminologica, la figura dell'hacker può essere ad oggi classificata in tre categorie.

I *black hat* (hacker con il cappello nero) sono i criminali informatici, cioè sfruttano le proprie competenze in modo illecito, accedendo a sistemi informatici senza autorizzazione, spesso con l'obiettivo di causare danni, sottrarre dati sensibili o perpetrare frodi.

I *white hat* (hacker con il cappello bianco anche detti hacker etici) sono professionisti della sicurezza informatica che utilizzano le proprie capacità per scopi puramente legittimi. Lavorano a fianco di aziende, organizzazioni o governi, per testare la sicurezza dei sistemi, identificare vulnerabilità e risolvere eventuali falle prima che possano essere scoperte (e sfruttate) da hacker malintenzionati.

I *gray hat* (hacker con il cappello grigio) si collocano in una zona intermedia tra i *white hat* e i *black hat*. Pur non agendo con intenzioni malevole, operano in un contesto etico e giuridico ambiguo. In genere, accedono a sistemi informatici senza autorizzazione con l'obiettivo di individuare vulnerabilità, senza

tuttavia arrecare danni o trarne un vantaggio personale diretto. Spesso segnalano le falle scoperte all'organizzazione interessata, talvolta chiedendo un compenso per la loro scoperta oppure decidendo di rendere pubblica la vulnerabilità.
In conclusione, l'evoluzione del termine hacker — da simbolo di abilità tecnica e spirito innovativo a figura associata a comportamenti illeciti — riflette i mutamenti che hanno interessato il mondo digitale e la crescente complessità delle minacce nel cyberspazio. Oggi la distinzione tra *black hat*, *white hat* e *gray hat* è fondamentale per interpretare le motivazioni che guidano le azioni degli hacker e per valutarne l'effettivo impatto sulla sicurezza informatica.

APPROFONDIMENTI

- Pomante, *Hacker e computer crimes*, 41/15, Napoli, 2000.
- Sterling, *Giro di vite contro gli hacker* (The hacker crackdown), Shake Edizioni Underground, Milano, 1996.
- Strano, *Computer crime*, Manuale di criminologia informatica. Milano, 2000.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
HACKER ETICO

HACKER ETICO

L' hacker etico (anche detto *white hat* hacker) è un professionista della sicurezza informatica che utilizza le proprie competenze per identificare, analizzare e correggere le vulnerabilità presenti in reti, applicazioni e infrastrutture informatiche.
A differenza degli hacker malintenzionati (noti anche come *black hat* hacker), che violano illecitamente i sistemi con scopi dannosi o per profitto personale, gli hacker etici operano con il consenso esplicito delle organizzazioni coinvolte. Tra le principali attività svolte rientrano i test di penetrazione (cosiddetti *penetration testing*), che sono simulazioni controllate di attacchi informatici finalizzate a identificare e correggere vulnerabilità prima che possano essere sfruttate da attori malevoli.

Nel panorama normativo attuale si sta progressivamente affermando la necessità di una regolamentazione giuridica chiara e condivisa per definire ruolo, limiti e responsabilità degli hacker etici. Organizzazioni di rilevanza internazionale, come l'International Council of E-Commerce Consultants, che si occupano della formazione e certificazione degli hacker etici, hanno elaborato codici di condotta volti a orientare l'attività di questi professionisti. Tra i principi fondamentali previsti da questi codici si annoverano: ottenere il permesso esplicito dall'azienda prima di avviare qualsiasi attività di *hacking*; evitare qualsiasi danno ai sistemi oggetto di test; mantenere la massima riservatezza sulle informazioni raccolte; e operare nel pieno rispetto delle normative vigenti in materia, con particolare attenzione alla privacy e alla sicurezza informatica.

Gli hacker etici lavorano a stretto contatto con le aziende per individuare e correggere le vulnerabilità nei sistemi, contribuendo in modo determinante alla tutela dei dati sensibili e delle risorse aziendali. Il loro ruolo, autentica prima linea di difesa contro le minacce informatiche, può risultare fondamentale per rafforzare la sicurezza e l'integrità delle infrastrutture digitali, proteggendo le informazioni critiche e prevenendo attacchi.

APPROFONDIMENTI

- Engebretson, *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*, Amsterdam, 2013.
- Farsole et al., *Ethical hacking*, in *International Journal of Computer Applications*, vol. 1, 10, 2010.

VOCI CORRELATE

BUG BOUNTY PROGRAMS
HACKER

h

IDENTITÀ DIGITALE

L'identità digitale è un concetto che nasce in ambito informatico per identificare tutti i sistemi configurabili come credenziali di accesso a risorse informatiche.

Dal punto di vista giuridico, l'identità digitale è definibile come «la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale» (art. 1, lett. o), DPCM 24 ottobre 2014, cd. Decreto SPID).

La Corte di cassazione si è occupata del tema in alcune decisioni (da ultimo v. Cassazione penale, seconda sezione, sentenze nn. 38027 del 18 settembre 2023 e 13559 del 13 marzo 2024), nelle quali ha richiamato il contributo definitorio dell'Ufficio del Massimario e del Ruolo nella relazione del 16 ottobre (Rel. n. III/03/2013) alla legge 15 ottobre 2013, n.119. Partendo dalla definizione elaborata nel Codice dell'amministrazione digitale, l'Ufficio del Massimario ha sostenuto che l'identità digitale è «comunemente intesa come l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione, che consiste (per come definito dall'art. 1 lett. u-*ter*) del d. lgs. 7 marzo 2005 n. 82) per l'appunto nella validazione dell'insieme di dati attribuiti in modo esclusivo e univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso».

L'identità digitale quindi si realizza mediante la coesistenza di più elementi: un soggetto fisico, proiettato online, l'insieme di dati e codici elettronici (ad es. le credenziali di accesso ai dispositivi) che identificano la persona attraverso il collegamento di tali dati alla sua identità.

APPROFONDIMENTI

- Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 3, 2017, 723 ss.

- Nastri, *Identità digitale e identità personale: un percorso di sintesi*, in Aa.Vv., *Il diritto nell'era digitale*, Milano, 2022, 3 ss.
- Resta, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 2007, 511 ss.
- Scagliarini, *Identità digitale e tutela della privacy*, in Aa.Vv., *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, 335 ss.

VOCI CORRELATE

DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
SISTEMA PUBBLICO DI IDENTITÀ DIGITALE (SPID)

INCIDENTE INFORMATICO

Nelle norme tecniche internazionali di sicurezza informatica e delle informazioni, con il concetto di incidente informatico si fa generalmente riferimento a un singolo evento, o a una serie di eventi, indesiderati o inaspettati, che possono compromettere le reti e i sistemi di un'organizzazione, nonché minacciare la riservatezza, integrità e disponibilità (cd. RID) delle informazioni e dei dati personali.
Si tratta pertanto di eventi che non necessariamente producono danni. Tra le fonti di normazione tecnica internazionale, si segnalano il Punto 3.1.1.5, ISO/IEC 27002:2022 che così definisce l'incidente per la sicurezza delle informazioni: «uno o più eventi di sicurezza delle informazioni correlati e identificati (3.1.14) che possono danneggiare gli asset di un'organizzazione (3.1.2) o comprometterne le operazioni»; e la norma NISTIR 8183 - NIST *Cybersecurity Framework Version* 1.1, secondo cui l'incidente informatico è «un evento che mette effettivamente o potenzialmente a rischio la riservatezza, l'integrità o la disponibilità di un sistema informativo o delle informazioni che il sistema elabora, memorizza o trasmette o che costituisce una violazione o una minaccia imminente di violazione delle politiche di sicurezza, delle procedure di sicurezza o delle politiche di utilizzo accettabile».

Diversamente, nelle norme giuridiche di diritto europeo e nazionali, l'incidente informatico è un evento che compromette le reti e i sistemi di un'organizzazione, nonché il RID delle informazioni e dei dati personali, un evento cioè che ha già prodotto un danno.
Per le definizioni, si vedano le seguenti fonti normative:

- la Direttiva (UE) 2022/2555 (NIS 2), secondo cui l'incidente informatico è «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi» (art. 6, n. 6);
- il Regolamento (UE) 2022/2554 (DORA), per cui il concetto di incidente connesso alle TIC è «un singolo evento, o una serie

di eventi collegati non programmati dall'entità finanziaria, che *compromette* la sicurezza dei sistemi informatici e di rete e ha un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza dei dati o sui servizi forniti dall'entità finanziaria» (art. 3, n. 8);

- il DPCM 30 luglio 2020, n. 131, a tenore del quale che l'incidente è «ogni evento di natura accidentale o intenzionale che *determina* il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici» (art. 1, co. 1, lett. h).

La compromissione delle reti e dei sistemi, oltre a causare un danno per il corretto funzionamento dell'apparato informatico o dei suoi servizi, può determinare una violazione dei dati personali (o data breach), definita dal Regolamento generale sulla protezione dei dati (*General Data Protection Regulation* - GDPR) n. 2016/279 come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4, n. 12).

APPROFONDIMENTI

- Gallotti, *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione. La norma ISO/IEC 27001:2022*.
- Serini, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in Calzolaio (a cura di), *La fine di internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 41 ss.

VOCI CORRELATE

DATA BREACH
GENERAL DATA PROTECTION REGULATION (GDPR)
MISURE DI SICUREZZA
NIS (DIRETTIVE NIS)

INDIRIZZO IP

L'indirizzo IP è l'*Internet Protocol Address* (indirizzo di protocollo Internet), identificabile come una sequenza numerica assegnata a computer collegati alla rete Internet che consente di metterli in comunicazione tra loro.

Gli indirizzi IP sono nati con lo sviluppo delle prime reti di computer, in particolare nel contesto del progetto ARPANET degli anni Settanta, da cui si è evoluta l'attuale rete Internet. La funzione principale di un indirizzo IP è quella di identificare in modo univoco ogni dispositivo connesso a una rete che utilizza il protocollo Internet, permettendo così l'instradamento corretto dei dati tra mittente e destinatario. In altre parole, l'indirizzo IP svolge un ruolo analogo a quello di un indirizzo postale nel mondo fisico, garantendo che le informazioni trasmesse tramite la rete raggiungano esattamente il destinatario previsto.
Gli indirizzi IP possono essere statici (quando restano invariati nel tempo) oppure dinamici (quando variano ad ogni connessione o dopo un certo periodo), a seconda delle modalità di assegnazione da parte del fornitore di accesso a Internet (ISP).

Esistono due principali versioni del protocollo IP:

- IPv4 (Internet Protocol version 4), che utilizza indirizzi composti da quattro numeri separati da punti (es. 192.168.0.1), ognuno compreso tra 0 e 255;
- IPv6 (Internet Protocol version 6), introdotto per far fronte all'esaurimento degli indirizzi IPv4, che impiega una sequenza alfanumerica più lunga (es. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Il trattamento degli indirizzi IP è in linea di principio soggetto al Regolamento generale sulla protezione dei dati (*General Data Protection Regulation* - GDPR) n. 2016/279, come deciso nella sentenza Breyer, C-582/14 della Corte di giustizia dell'Unione europea, secondo cui l'indirizzo IP è un dato personale se riferibile, direttamente o indirettamente, a una persona fisica identificata o identificabile.

APPROFONDIMENTI

- Abba, Lazzaroni, Pietrangelo (a cura di), *La Internet governance e le sfide della trasformazione digitale*, Napoli, 2022.
- Merla, *L'indirizzo IP dinamico quale dato personale*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2017, 360 ss.

VOCI CORRELATE

CYBERSPAZIO
DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
INTERNET

i

INGEGNERIA SOCIALE

L'ingegneria sociale (più comune l'inglese *social engineering)* è una delle tattiche più utilizzate per sfruttare le vulnerabilità di una rete o di un sistema informatico. Il termine qualifica tutta una serie di meccanismi di manipolazione dell'utente attraverso l'interazione umana e, nello specifico, attraverso la costruzione di un rapporto di fiducia e confidenzialità tra l'aggressore e l'utente-vittima. Si tratta di una strategia in cui il malintenzionato, da solo o in gruppo, manipola l'utente al fine di carpire informazioni sensibili o far compiere alla vittima stessa azioni che siano tali da compromettere la sicurezza del sistema informatico nel mirino dell'aggressore.

Le tattiche utilizzate sono varie; il *phishing*, l'impersonificazione, il *vishing*, lo *spear phishing* sono le più frequenti. Sono accomunate dallo sfruttamento intenzionale delle vulnerabilità umane per conseguire obiettivi illeciti, come il furto d'identità o password o denaro.

Gli attacchi di ingegneria sociale sono molto più complessi da contrastare e da prevenire proprio perché si basano sulla psicologia, sui comportamenti e sul coinvolgimento delle emozioni umane.

APPROFONDIMENTI

- Aterno, *Sicurezza informatica: aspetti giuridici e tecnici,* Pisa, 2022.
- Borghini, Garzia, *Psicologia dell'ingegneria sociale (PIS). L'arte dell'inganno. Strategie psicologiche di attacco e di difesa della privacy nel mondo reale e virtuale*, Napoli, 2010.
- Hadnagy, *Human hacking. Influenzare e manipolare il comportamento umano con l'ingegneria sociale,* Milano, 2019.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
FATTORE UMANO
PHISHING

i

INTERNET

Con l'espressione Internet (contrazione di *interconnected networks*, in italiano reti interconnesse) si fa riferimento alle cd. reti di comunicazione elettronica, cioè ad un sistema complesso di apparecchi in origine coincidenti coi soli computer, che attualmente invece include apparecchiature di diverso tipo come televisioni, smartphone o consolle per videogiochi, distribuiti in maniera disomogenea sulla superficie del Pianeta. Sistemi diversi che comunicano tra loro mediante un segnale elettrico trasmesso da mezzi differenti come i cavi originariamente posati per le comunicazioni telefoniche, le fibre ottiche, o anche via etere. Con la medesima espressione si fa anche riferimento all'insieme di dati complessivamente conservati su tutte le macchine connesse tra loro mediante la Rete.
Internet, dunque, è un mezzo di comunicazione che è nato come protocollo per scambiare files tra reti di computer collegate, che utilizzano un linguaggio standardizzato (il cd. Protocollo TCP/IP) e che si è evoluto consentendo di scambiare messaggi elettronici, fino alla nascita del web, ovvero alla possibilità di accedere e connettere in maniera grafica ipertesti.
Si tratta di un mezzo capace non solo di immagazzinare dati precostituiti, ma anche di manipolare e costruire informazioni. Proprio a partire dalla considerazione che qualsiasi dato inserito può essere letto da chiunque sia in rete in cerca di informazioni, si potrebbe sostenere che Internet è un servizio informativo diffuso e permanente, più che un mero mezzo di comunicazione. Seppure mediante strumenti differenti, infatti, è un mezzo che costituisce un unico ambiente, conosciuto come cyberspazio, che rappresenta un reticolo di contatti, uno spazio senza collocazione geografica e privo di costruzione gerarchica.
La vocazione di Internet alla diffusione delle notizie e alla comunicazione, alla costruzione di relazioni pari ordinate e decentrate, alla costituzione di una comunità (virtuale), svela il rilievo "materialmente costituzionale" di questo *fenomeno*.
Una delle implicazioni politico-istituzionali di questo spazio di libertà è la cd. democrazia elettronica (*e-democracy)* rappresentata come modello di decisione politica che procede dal basso, dalla base (*bottom-up*).

Le trasformazioni radicali indotte dall'avvento di Internet sono avversate da quanti guardano invece ad esso, al pari di ogni altro dispositivo o strumento nell'età della tecnica, come una concreta minaccia per il pluralismo, la democrazia e la pace sociale.
Si è osservato, innanzitutto, che il paradigma tecnologico può convertirsi da fattore di liberazione della persona a forza irresistibile e costrittiva della libertà. In questa prospettiva, non è più l'individuo ad esser sovrano ma la tecnologia stessa, che oppone l'automazione all'autonomia, in termini di capacità di autodeterminazione dell'individuo.
Si tratta, ad esempio, dei rischi di controllo e sorveglianza, cui i dispositivi della rete possono condurre, e a tutte le inedite e non trasparenti interazioni tra forme di sapere e potere cui la rete inevitabilmente si presta.
La questione più importante diventa quella della regolamentazione del cyberspazio, come spazio di agibilità sociale, economica e politica: è il tema dell'*Internet Governance*, il governo di internet, inteso come l'adozione da parte dei poteri pubblici, ma anche dei poteri privati, nei loro rispettivi ambiti, di principi, norme, regole, che disciplinano (e condizionano) l'evoluzione e l'uso di internet.
La *Internet Governance* prevede l'inclusione delle parti interessate nel processo decisionale e nella fase di implementazione di politiche. Dal 1998 la regolazione dei servizi di accesso alla rete è rimessa all'*Internet Corporation for Assigned Names and Number* (ICANN), un ente no profit di diritto privato, registrato nello Stato della California negli Stati Uniti. Mediante il potere di assegnazione degli indirizzi IP, di identificazione di protocollo e di gestione del sistema dei nomi a dominio di primo livello generico, del codice internazionale e del sistema di *root server*, svolge la funzione di garantire il funzionamento dei sistemi di identificazione unica di internet, assicurandone la stabilità e la sicurezza; promuove la competizione e la rappresentanza delle comunità globali di internet. È dunque un ente dotato di poteri capaci di incidere unilateralmente sui diritti e sulle libertà che si esercitano a attraverso Internet.

APPROFONDIMENTI

- Abba, Lazzaroni, Pietrangelo (a cura di), *La Internet governance e le sfide della trasformazione digitale*, Napoli, 2022.
- Albanesi, Valastro, Zaccaria, *Diritto dell'informazione e della comunicazione*, Milano, 2023.
- Caretti, Cardone, *Diritto dell'informazione e della comunicazione nell'era dell'intelligenza artificiale*, Bologna, 2024.
- Donati, *Internet (diritto costituzionale)*, in *Enciclopedia del Diritto*, 2014, 545 ss.
- Ruotolo, *Internet (diritto internazionale)*, in *Enciclopedia del Diritto*, 2014, 545 ss.

VOCI CORRELATE

CYBERSPAZIO
DIGITAL SERVICE ACT (DSA)
INDIRIZZO IP
SERVICE PROVIDER

INTERESSATO (DIRITTI DELL’)

Il Regolamento europeo generale sulla protezione dei dati (*General Data Protection Regulation* - GDPR) n. 2016/679 definisce l’interessato come la persona fisica a cui si riferiscono i dati personali oggetto di trattamento. Il Regolamento (Capo III) riconosce espressamente all’interessato una serie di diritti. In particolare:

a. Diritto di accesso dell’interessato (art. 15, Cons. 63, 64 GDPR)
Questo diritto consente all’interessato di ottenere dal titolare del trattamento - senza alcun obbligo di motivazione a sostegno della richiesta - la conferma che sia in corso un trattamento dei propri dati personali. In caso affermativo, l’interessato ha il diritto di accedere a tali dati e ricevere informazioni relative a: le finalità del trattamento; le categorie di dati trattati; i destinatari o le categorie di destinatari a cui i dati sono stati o saranno comunicati (in particolare se destinatari di Paesi extra-Ue o organizzazioni internazionali); il periodo di conservazione dei dati o i criteri utilizzati per determinarlo; l’esistenza di eventuali processi decisionali automatizzati, compresa la profilazione. L’interessato può anche richiedere copia dei dati personali oggetto di trattamento, generalmente fornita gratuitamente, salvo il caso in cui la richiesta sia manifestamente infondata o eccessiva. Tale diritto di ottenere copia dei propri dati può tuttavia subire limitazioni anche se tale azione è lesiva di diritti e libertà altrui. Indicazioni dettagliate sull’esercizio di questo diritto sono nelle le Linee guida 1/2022 sui diritti degli interessati - Diritto di accesso, ver. 2.1dall’European Data Protection Board (EDPB).

b. Diritto di rettifica (art. 16, Cons. 65 GDPR)
Il diritto di rettifica consente all’interessato di ottenere dal titolare del trattamento la correzione dei dati personali inesatti che lo riguardano. L’interessato può anche richiedere l’integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa se necessario. Il titolare deve provvedere alla rettifica senza ingiustificato ritardo, generalmente a titolo gratuito, garantendo così che i dati trattati siano sempre aggiornati, accurati e completi.

c. Diritto alla cancellazione e diritto all'oblio (art. 17, Cons. 65, 66 GDPR)
Il diritto alla cancellazione e il diritto all'oblio sono diritti distinti mediante il cui esercizio si perviene allo stesso risultato: la cancellazione dei dati personali su richiesta dell'interessato. Sui tratti distintivi dei due diritti è intervenuta in più occasioni la Corte di giustizia dell'Unione europea (CGUE), che ha così definire i contorni del diritto all'oblio: un diritto riconosciuto all'interessato per ottenere la rimozione dei propri dati personali resi pubblici (ad es. notizie di cronaca, motori di ricerca, social, ecc.) quando risultino "affievoliti" - a seguito di una valutazione *logico-funzionale* - alcuni indici tra cui, le finalità del trattamento, il contesto all'interno del quale sono stati utilizzati tali dati, il peso e l'attualità, nonché l'interesse pubblico sulla notizia/informazione (CGUE, Case C131/12, *Google Spain*). Il diritto alla cancellazione consente invece all'interessato di ottenere la cancellazione dei propri dati personali senza ingiustificato ritardo, quando: i dati non sono più necessari per le finalità per cui sono stati raccolti o trattati; il consenso sia stato revocato e non esistono altri fondamenti giuridici per il trattamento; i dati sono stati trattati illecitamente; la cancellazione è necessaria per adempiere a un obbligo legale; l'interessato si oppone al trattamento e non prevalgono motivi legittimi per proseguirlo. Entrambi tali diritti non sono assoluti, possono cioè essere limitati, per esempio, per garantire l'esercizio della libertà di espressione, o l'adempimento di obblighi legali o per motivi di interesse pubblico.

d. Diritto alla limitazione del trattamento (art. 18, Cons. 67 GDPR)
Il diritto alla limitazione del trattamento consente all'interessato di richiedere al titolare di limitare l'uso dei propri dati personali in determinati casi, senza richiederne la cancellazione. La limitazione può essere esercitata quando: l'interessato contesta l'esattezza dei dati, per il periodo necessario al titolare per verificarli; il trattamento è illecito, ma l'interessato si oppone alla cancellazione e richiede invece la limitazione; il titolare non necessita più dei dati, ma l'interessato li richiede per accertare, esercitare o difendere un diritto in sede giudiziaria; l'interessato si è opposto al trattamento, in attesa della verifica di prevalenza dei legittimi motivi del titolare. Durante la limitazione, i dati

possono essere solo conservati e trattati in casi specifici, come con il consenso dell'interessato o per ragioni legali.

e. Diritto alla (obbligo di) notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19, Cons. 31 GDPR)
Questo diritto dell'interessato è speculare rispetto alla previsione dell'obbligo a carico del titolare del trattamento di informare l'interessato, e tutti i destinatari a cui sono stati comunicati i dati personali, di eventuali rettifiche, cancellazioni o limitazioni del trattamento. L'obbligo di notifica garantisce trasparenza e permette agli altri soggetti interessati (ad esempio altre organizzazioni) di aggiornare o eliminare i dati nei loro sistemi.
Il titolare non è tenuto alla notifica solo se ciò risulta impossibile o comporta uno sforzo sproporzionato. Su richiesta dell'interessato, il titolare deve anche fornire informazioni sui destinatari che hanno ricevuto i dati.

f. Diritto alla portabilità dei dati (art. 20, Cons. 68 GDPR)
Il diritto alla portabilità dei dati consente all'interessato di ricevere dal titolare del trattamento i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico. L'interessato può inoltre richiedere che i dati siano trasmessi direttamente a un altro titolare, se tecnicamente fattibile. Si tratta di un diritto che tutela i dati personali, favorendone al contempo la circolazione. Il diritto alla portabilità si applica solo quando il trattamento è basato sul consenso o su un contratto; o quando il trattamento è effettuato con mezzi automatizzati. Esso non si applica ai trattamenti non automatizzati o necessari per l'interesse pubblico.

g. Diritto di opposizione (art. 21, Cons. 69, 70 GDPR)
Il diritto di opposizione consente all'interessato di opporsi in qualsiasi momento al trattamento dei propri dati personali, per ragioni di interesse pubblico o per legittimo interesse del titolare (compresa la profilazione), ma anche per evitare il trattamento per finalità di marketing diretto (in questo caso, il diritto è assoluto).
Il titolare deve interrompere il trattamento, salvo che dimostri

l'esistenza di motivi legittimi cogenti che prevalgano sui diritti e le libertà dell'interessato o per l'accertamento, esercizio o difesa di un diritto in sede giudiziaria. L'opposizione al marketing diretto, inclusa la profilazione correlata, implica l'immediata cessazione del trattamento per tali finalità.

h. Diritto di non essere sottoposto a una decisione che sia basata unicamente su un trattamento automatizzato (art. 22, Cons. 71, 72 GDPR)
Questo diritto tutela l'interessato nel caso di decisioni che lo riguardano in modo significativo (ad es. rifiuto di credito o selezione per un lavoro) prese esclusivamente tramite processi automatizzati (ad es. utilizzando l'intelligenza artificiale), anche per finalità di profilazione. In particolare, questo diritto trova applicazione quando le decisioni producono effetti giuridici sull'interessato o influiscono in modo analogo e significativo sulla sua vita. Il trattamento automatizzato è consentito solo se necessario per la conclusione o esecuzione di un contratto; autorizzato dal diritto europeo o degli Stati membri; basato sul consenso esplicito dell'interessato. Tuttavia, in tali casi, il titolare è tenuto ad adottare adeguate misure di salvaguardia, come il diritto dell'interessato di ottenere l'intervento umano sul contenuto della decisione automatizzata, di esprimere la propria opinione e di contestare la decisione.

Oltre ai diritti elencati espressamente previsti dal GDPR, all'interessato sono riconosciuti altri diritti deducibili in via interpretativa dall'analisi di altre disposizioni dello stesso Regolamento. Si tratta del diritto al trattamento in forma concisa, trasparente e intellegibile (art. 12 GDPR) e del diritto alla revoca del consenso (art. 7 GDPR).
Il primo discende dall'obbligo per il titolare del trattamento di adottare adeguate misure di trasparenza (ad es. l'informativa del trattamento) per rendere edotto l'interessato sulle caratteristiche e condizioni del trattamento e sui suoi diritti. L'adeguatezza delle misure comunicative variano a seconda del contesto e soprattutto dell'età dell'interessato: particolari cautele sono infatti poste nel caso in cui il trattamento abbia ad oggetto i dati personali dei minori. Il secondo consente all'interessato di

revocare il consenso in qualsiasi momento e con la stessa facilità con cui è stato accordato, senza che ciò pregiudichi la liceità del trattamento basato sul consenso prima della revoca.
Il titolare del trattamento non può rifiutare di soddisfare le richieste degli interessati circa l'esercizio dei propri diritti, salvo i limiti e le restrizioni indicate in precedenza. Se l'interessato ritenga che i diritti di cui gode sono stati violati, può proporre reclamo all'Autorità garante per la protezione dei dati personali o proporre ricorso davanti al giudice (art. 79, Cons 141, 145, 147 GDPR; artt. 140-*bis* e ss.; d.lgs. 101/2018).

APPROFONDIMENTI

- Bolognini, Pelino (diretto da), *Codice della disciplina privacy*, Milano, 2024.
- D' Orazio, Finocchiaro, Pollicino, Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021.
- Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021.
- Riccio, Scorza, Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2022.

VOCI CORRELATE

DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
OBLIO (DIRITTO ALL')

INVESTIGAZIONI DIGITALI

La legge 18 marzo 2008, n. 48, che ratifica la Convenzione del Consiglio d'Europa sulla criminalità informatica, disciplina l'attività di acquisizione degli elementi di prova digitali per consentire accertamenti urgenti di polizia giudiziaria, ispezioni, perquisizioni e sequestri, anche in relazione ai programmi informatici o ai sistemi informatici ancorché protetti da misure di sicurezza. L'attività tipica dell'*inspicere* si sostanzia in un'attività volta all'osservazione di persone, luoghi, cose e volta all'accertamento di tracce o altri effetti materiali del reato; di contro, il *perquirere* si caratterizza per essere volto alla ricerca del corpo del reato o delle cose ad esso pertinenti, spesso qualificandosi come attività prodromica rispetto al sequestro probatorio.
La perquisizione informatica prevista dal codice di procedura penale non deve confondersi con la cd. perquisizione occulta da remoto effettuata per mezzo del captatore informatico.
Si tratta di un mezzo di indagine che consente di effettuare un insieme di operazioni all'insaputa dell'interessato, volte sia ad esplorare un sistema informatico per trarne utili elementi probatori, sia a monitorarlo con costanza e, più precisamente, di un'attività investigativa che assomma le caratteristiche e le funzioni di diversi mezzi di ricerca della prova tipici, pur non essendo riconducibile ad alcuno di essi, e che presenta altresì caratteri di originalità. Questi strumenti processuali, arricchiti delle disposizioni sul bisogno di integrità dei dati digitali acquisiti, assicura possibili e future prove al procedimento penale garantendo, lì dove possibile, anche la loro conservazione in una forma che consente di mantenere immutate le caratteristiche della cosa e del suo contenuto.

APPROFONDIMENTI

- Aterno, Cajani, Costabile, Curtotti (a cura di), *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici,* Torino, 2021.
- Curtotti, Saravo, *Manuale delle investigazioni sulla scena del crimine*, Torino, 2022.

- Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Torino, 2018.

VOCI CORRELATE

CYBERCRIME
CYBERJUSTICE
DIGITAL FORENCICS
TROJAN

i

k

KEYLOGGER

Un *keylogger* è uno strumento (software o hardware) progettato per registrare ogni tasto premuto su una tastiera, spesso a insaputa dell'utente. Il termine deriva dall'inglese *keystroke logger*, cioè registratore di battute di tastiera. Questo tipo di tecnologia è utilizzata per intercettare e memorizzare tutto ciò che viene digitato, inclusi nomi utente, password, messaggi e altri dati sensibili.
I *keylogger* software sono programmi che operano in background nel sistema operativo e possono essere installati in modo occulto, talvolta come parte di un *malware*, con lo scopo di spiare le attività dell'utente. In alcuni casi, possono persino inviare le informazioni raccolte a un server remoto, consentendo a chi li ha installati di accedere da lontano ai dati digitati.
Esistono anche *keylogger* hardware, piccoli dispositivi fisici che si collegano tra la tastiera e il computer o si integrano direttamente nella tastiera stessa. Questi dispositivi sono spesso usati in attacchi mirati o in contesti in cui l'accesso fisico alla macchina è possibile. Sebbene possano essere utilizzati in ambiti leciti, ad esempio per motivi di controllo parentale, per monitoraggio aziendale (previo consenso), o in test di sicurezza informatica, nella maggior parte dei casi i *keylogger* sono strumenti associati a scopi malevoli, come il furto di identità, lo spionaggio informatico o la violazione della privacy. Essi possono quindi risultare lesivi di diverse disposizioni del Codice penale in relazione, tra gli altri, ai reati di accesso abuso a sistema informatico, frode informatica o diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. Per questo motivo, il loro utilizzo solleva importanti questioni etiche e giuridiche, ed è fondamentale adottare misure di sicurezza per proteggersi da questo tipo di minacce.

APPROFONDIMENTI

- Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla cd. Online Durchsuschung*, in *Rivista trimestrale di diritto penale dell'economia*, 3, 2009, 695 ss.

- Salvadori, *I reati contro la riservatezza informatica*, in Cadoppi, Canestrari, Manna, Papa, *Cybercrime*, Milano, 2023, 694 ss.
- Scerbo, *Equilibrio tra esigenze di tutela della sicurezza collettiva e tutela delle libertà fondamentali. Nuove tecnologie nella giustizia penale? A.I. (artificial intelligence), Trojan horse (captatore infomatico) e gestione dei dati da parte dell'autorità come case studies*, in *Archivio penale*, 1, 2024.
- Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali,* Milano, 2017.

VOCI CORRELATE

ACCESSO ABUSIVO A SISTEMA INFORMATICO
CYBERATTACCO (ATTACCO INFORMATICO)
CYBERCRIME
MALWARE

m

MALWARE

Il *malware* – dall'inglese *malicious* software – è un programma informatico malevolo, progettato per arrecare danno al contenuto di dispositivo informatico o all'attività di chi lo utilizza. Il termine *malware* nasce nel 1990 su iniziativa di Yisrael Radai per identificare la categoria dei software malevoli in precedenza definite virus. In ambito informatico si distinguono virus e *malware* non sono oggi sinonimi: tutti i virus sono *malware*; ma non tutti i tipi di *malware* sono virus.
Oggi alla categoria dei *malware* sono ricondotti tutti i programmi informatici creato con l'intenzione di provocare un danno; tra questi sono censiti i *trojan, worm, spyware, ransomware*.
Il danno prodotto dal *malware* cambia a seconda del tipo di programma, che può provocare il rallentamento del singolo device o l'apertura di finestre indesiderate, o cyber attacchi contro singoli o aziende per sottrarre dati sensibili, segreti aziendali o informazioni riservate.

I *malware* più diffusi sono:

- *ransomware*, blocca il dispositivo o ne cifra i contenuti sino al pagamento di un riscatto in criptovaluta;
- *spyware*, spiano i movimenti della vittima sulla rete internet e inviano i relativi dati a server remoti;
- *botnet*, colpiscono un'intera rete informatica (come quella di una scuola, un'azienda, un ufficio), permettendo all'aggressore di controllare tutti i dispositivi ad essa connessi;
- virus, parti di codici in grado autoreplicarsi e diffondersi all'interno di altri programmi e file di un dispositivo;
- *trojan horse*, assumono le sembianze di software benevoli, nascondono *malware* in file video, audio, oppure in allegati a mail in apparenza innocue.

Nonostante le diversità tra tipi di *malware*, comuni sono gli indici che segnalano un'infezione da *malware*: file bloccati o cancellati; annunci popup; arresto di sistema improvviso; messaggi anomali

ricevuti dai propri contatti; richieste di riscatto. Sono simili anche i canali attraverso cui l'aggressore riesce a diffondere il *malware* all'interno del dispositivo che intende colpire: sono utilizzate, spesso, tecniche di ingegneria sociale, come e-mail di *phishing*, compromissione delle app di messaggistica, exploit, annunci infetti.

Una strategia decisiva per prevenire attacchi da *malware* consiste nel ricorso costante a programmi informatici antivirus, che analizzano i file contenuti nei dispositivi, intercettano i *malware*, li eliminano o suggeriscono procedure per il ripristino dei file infetti. Nonostante nessun antivirus garantisca assoluta protezione, se ben configurato e aggiornato costantemente renderà quantomeno improbabile che un *malware* possa introdursi nel dispositivo.

APPROFONDIMENTI

- Abbate, *Man in the browser. I malware che hanno fatto tremare le banche,* Esculapio, 2023.
- Aterno, *Sicurezza informatica: aspetti giuridici e tecnici,* Pisa, 2022.
- European Network and Information Security Agency (ENISA), *Malicious software: Train the trainer reference guide*, 2010.
- NIST, *Data Integrity: Recovering from a destructive malware attack*, 2016.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
INCIDENTE INFORMATICO
INGEGNERIA SOCIALE
RANSOMWARE

MISURE DI SICUREZZA

Nel contesto della cybersicurezza, una misura di sicurezza è un insieme di controlli, procedure e strumenti organizzativi e tecnici adottati per proteggere le reti, i sistemi informativi e i dati da rischi e minacce informatiche. Le misure sono finalizzate a garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei servizi essenziali, prevenendo incidenti e minimizzando l'impatto di attività malevole. Le misure di sicurezza previste dalla normativa italiana sono mutuate dal NIST *Cybersecurity Framework* (CSF), uno standard ampiamente riconosciuto e adottato a livello internazionale, e in particolare dal Framework Nazionale per la Cybersecurity e la Data Protection, sviluppato e adottato in Italia, che riprende la struttura e la logica del NIST CSF ma adattandolo al contesto normativo e operativo italiano.
Nella loro dimensione massimalista, le misure di sicurezza non sono meri adempimenti prescrittivi, ma rappresentano obiettivi di sicurezza: risultati desiderati che ogni organizzazione deve raggiungere, adattando le modalità di attuazione al proprio contesto, alla valutazione del rischio e alle specificità operative.
Questo approccio per obiettivi permette flessibilità e personalizzazione, pur garantendo un livello minimo di sicurezza uniforme per tutti i soggetti obbligati.
Il NIST *Cybersecurity Framework* (versione 2.0) e il Framework Nazionale italiano suddividono le misure in sei classi principali (*Functions*), ciascuna articolata in categorie e sottocategorie:

- *Govern* (GV), ha come obiettivo la definizione di strategie, politiche, ruoli e responsabilità per la gestione del rischio cyber;
- *Identify* (ID), richiede la mappatura e comprensione degli asset, dei rischi e delle vulnerabilità per dare priorità agli interventi;
- *Protect* (PR), per l'implementazione di controlli per prevenire o limitare l'impatto degli incidenti;
- *Detect* (DE), ha lo scopo di sviluppare capacità di rilevare tempestivamente eventi e anomalie che indicano possibili incidenti cyber;

- *Respond* (RS), pone come obiettivo la gestione ed il contenimento degli incidenti, la comunicazione e l'analisi degli eventi;
- *Infine Recover* (RC), sul ripristino delle attività e delle operazioni dopo un incidente, nonché il miglioramento continuo delle capacità di risposta.

Tutte queste classi di misure sono strutturare per coprire l'intero ciclo di vita della sicurezza informatica, dalla governance alla risposta e recupero, e sono declinate in requisiti specifici sia di tipo tecnico che organizzativo.

APPROFONDIMENTI

- Gallotti, *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione. La norma ISO/IEC 27001:2022*.
- *Serini, La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana,* in Calzolaio (a cura di), *La fine di internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale, sezione monografica della Rivista italiana di informatica e diritto, 2, 41 ss.*

VOCI CORRELATE

CYBERRESILIENZA
INCIDENTE INFORMATICO
NIS (DIRETTIVE NIS)

n

NIS (DIRETTIVE NIS)

Le Direttive NIS sono atti normativi dell'Unione europea che disciplinano la *Network and Information Security*, da cui l'acronimo NIS.
La Direttiva NIS 1 (Direttiva 2016/1148) è stata adottata nel 2016 e rappresenta la prima misura legislativa a livello europeo volta a migliorare la cooperazione tra gli Stati membri e creare un primo livello di armonizzazione in materia di sicurezza cibernetica. Nel 2022 è intervenuta sulla stessa materia la Direttiva NIS 2 (Direttiva (UE) 2022/2555), che ha aggiornando il quadro regolatorio e abrogato la NIS 1.

L'obiettivo principale della direttiva NIS 2 è aumentare la resilienza delle infrastrutture critiche e migliorare la gestione dei rischi di sicurezza informatica, alla luce di un panorama digitale sempre più complesso e vulnerabile agli attacchi cyber. Gli Stati membri dell'UE erano tenuti a recepire la direttiva nei rispettivi ordinamenti nazionali entro il 17 ottobre 2024. In Italia, la direttiva è stata recepita dal d.lgs. 138/2024, cd. Decreto NIS.

Tra le principali novità della Direttiva NIS 2 si segnala, innanzitutto, l'ampliamento dell'ambito di applicazione: vengono ricompresi più settori considerati critici, che si affiancano a quelli già coperti dalla NIS 1, come energia, trasporti e sanità. In particolare, la NIS 2 estende la propria portata anche a settori quali i servizi postali e di corriere, la gestione dei rifiuti, l'industria chimica, alimentare e manifatturiera, includendo automaticamente tutte le imprese di medie e grandi dimensioni che operano in tali ambiti.

La nuova normativa prevede anche più stringenti requisiti di sicurezza. Le organizzazioni che rientrano nel campo di applicazione della direttiva sono tenute ad adottare misure tecniche e organizzative adeguate alla gestione dei rischi informatici, tra cui l'implementazione di sistemi di prevenzione, rilevamento e risposta agli incidenti, lo sviluppo di piani di continuità operativa per garantire la resilienza dei servizi essenziali, nonché la valutazione e mitigazione dei rischi derivanti dalla supply chain e dai fornitori terzi.

Sono, inoltre, introdotti obblighi più rigorosi in materia di notifica degli incidenti: le organizzazioni devono segnalare gli incidenti significativi entro 24 ore dalla loro individuazione, e fornire una relazione dettagliata entro 72 ore, specificando le misure adottate e l'impatto complessivo dell'evento.

Dal punto di vista istituzionale, la NIS 2 rafforza anche i meccanismi di cooperazione tra Stati membri, promuovendo un maggiore coordinamento a livello europeo attraverso la creazione di un Gruppo di Cooperazione e il potenziamento della rete CSIRTs (*Computer Security Incident Response Teams*), al fine di facilitare lo scambio di informazioni e la gestione coordinata delle crisi cyber.

Infine, viene definito un quadro sanzionatorio più incisivo, che impone agli Stati membri di prevedere sanzioni efficaci, proporzionate e dissuasive in caso di violazione degli obblighi previsti dalla direttiva. Le sanzioni possono arrivare fino a 10 milioni di euro o al 2% del fatturato globale annuo dell'impresa, a seconda di quale dei due importi risulti maggiore.

APPROFONDIMENTI

- Fiorinelli, Giannelli (a cura di), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, sezione monografica della *Rivista italiana di informatica e diritto*, 1, 2024.
- Karathanasis, *Cybersecurity and EU Law*, Taylor & Francis, 2024.
- Longo, *La disciplina della cybersecurity nell'Unione europea e in Italia*, in Calzolaio, Longo, Iannuzzi, Orofino, Torino, *La regolazione europea della società digitale*, 2024, 203 ss.
- Razzante, Spanò, *La NIS 2 e il decreto cybersicurezza*, Milano, 2025.
- Salvi, *La Cybersecurity fra obblighi e opportunità. Compendio e correlazione di NIS2 e D.Lgs 138/2024, PSNC, PNRR, L. 90/2024*, Milano, 2025.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
CYBERRESILIENZA
PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)
RETE DI CSIRT
VULNERABILITÀ

OBLIO (DIRITTO ALL')

L'espressione diritto all'oblio non è recente né univoca. Tradizionalmente si fa risalire, nelle sue prime formulazioni, alla seconda metà del Novecento in Francia. Ma solo da alcuni decenni il diritto all'oblio diventa centrale nel dibattito giuridico a livello nazionale e sovranazionale, in cui si ravvisano tre diverse accezioni.

b. Diritto di essere dimenticati

In origine concepito dalla dottrina e dalla giurisprudenza come il diritto di "essere dimenticati", il diritto all'oblio era il diritto del singolo di non vedere ripubblicate a distanza di tempo notizie in passato diffuse lecitamente. In questa prima accezione, dunque, il diritto all'oblio attiene alle ragioni del diritto alla riservatezza: si tratta di capire se fatti o eventi personali, in passato legittimamente pubblicizzati, possano essere oggetto di nuova pubblicazione o, al contrario, se il trascorrere del tempo e il mutamento delle situazioni renda tale successiva diffusione illecita per violazione del diritto alla riservatezza configurando a favore dell'interessato un vero e proprio diritto all'oblio. Secondo la giurisprudenza, il diritto all'oblio è riconosciuto quando nella notizia oggetto di nuova pubblicazione la menzione degli elementi che identificano il soggetto protagonista dei fatti non costituisce più interesse pubblico, concreto ed attuale.

c. Diritto di essere correttamente ricordati

Con la digitalizzazione il diritto all'oblio acquista una nuova accezione. Cambiano i presupposti in relazione sia al fattore temporale sia all'esigenza da soddisfare. Il concetto di "ripubblicazione" nel nuovo spazio cibernetico diviene obsoleto: quando una notizia viene pubblicata è astrattamente disponibile in modo permanente. E così, la questione problematica non è più la ripubblicazione di una notizia resa nota in passato; l'esigenza da soddisfare non è più evitare la nuova diffusione della stessa; il "fattore tempo" non è più considerabile in termini tradizionali perché proprio la costruzione stessa della Rete ci pone di fronte ad un continuum temporale che rende la notizia – diffusa in passato in modo lecito – potenzialmente disponibile per sempre.

A ciò si aggiunge il rischio che le informazioni reperibili e diffuse in Rete siano anche non veritiere o, comunque, non aggiornate. Seguendo tale ragionamento, il diritto all'oblio non è tanto il diritto di essere dimenticati, ma piuttosto il diritto ad essere correttamente ricordati. In questa seconda accezione, il diritto all'oblio attiene alla sfera del diritto all'identità personale. Sulla base di recenti orientamenti giurisprudenziali, si può rilevare che il trattamento lecito dei dati personali discende dal bilanciamento di diritti e interessi contrapposti, all'interno del quale è possibile configurare un diritto all'oblio a favore del soggetto come diritto alla contestualizzazione delle informazioni teso a evitare il travisamento del proprio patrimonio e della propria immagine – tra le altre – professionale, intellettuale, politica e sociale in un preciso contesto storico.

d. Diritto alla cancellazione dei dati personali

La terza accezione del diritto all'oblio è sancita nell'articolo 17 del Regolamento generale sulla protezione dei dati n. 2016/679 come diritto alla cancellazione dei dati personali qualora ricorrano circostanze determinate e specifiche previste dalla normativa europea. In questa terza declinazione quindi il diritto all'oblio come diritto di essere dimenticati in relazione a dati diffusi online attiene al diritto alla protezione dei dati personali. Poiché è tecnicamente impossibile cancellare dal web in via definitiva e assoluta i dati, la disciplina normativa prevede l'attivazione di misure ragionevoli e proporzionate, anche di natura tecnica, mediante cui il diritto possa essere comunque garantito. Tali misure sono finalizzate ad assicurare che gli ulteriori titolari che stanno trattando quei dati personali cancellino qualsiasi link, copia o riproduzione degli stessi; e che i dati vengano deindicizzati dai principali motori di ricerca, in modo da renderli quantomeno difficile da raggiungere.

Vista la sua natura multiforme e i legami con altri diritti fondamentali della persona, il diritto all'oblio non è propriamente configurabile come diritto autonomo, ma piuttosto esso è un diritto strumentale alla realizzazione di uno dei diritti della personalità già ricordati.

APPROFONDIMENTI

- European Data Protection Board (EDPB*), Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, definite in base alle previsioni del Regolamento (UE) 2016/679 (parte I)»*, 7 luglio 2020.
- Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità,* in *Diritto dell'informazione e dell'informatica,* 2014, 591 ss.
- Finocchiaro, *Diritto di internet,* Bologna, 2020.
- Resta, Zeno-Zencovich, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015.

VOCI CORRELATE

DATI PERSONALI
EUROPEAN DATA PROTECTION BOARD (EDPB)
GENERAL DATA PROTECTION REGULATION (GDPR)
RISERVATEZZA

p

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è un articolato sistema di misure, regole e procedure istituito per assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dal cui funzionamento dipende l'esercizio di funzioni e servizi essenziali dello Stato e il cui malfunzionamento, interruzione, anche parziali, ovvero l'utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Il PSNC è stato istituito dal decreto-legge 21 settembre 2019, n. 105 (convertito nella n. 133 del 2019).

Le regole del Perimetro si applicano solo a taluni soggetti selezionati all'esito di una procedura che si articola su tre fasi: per prima cosa, le amministrazioni individuano quali sono le funzioni essenziali (per esempio governo, sicurezza, difesa, giustizia, trasporti) e i servizi essenziali (attività che consentono l'esercizio delle funzioni essenziali o che presentano particolare rilievo economico e sociale); dopodiché, vengono identificati i soggetti pubblici o privati che assicurano o esercitano queste funzioni; infine, vengono individuati i Beni ICT (reti, sistemi informativi e servizi informatici) dal cui regolare funzionamento dipende l'esercizio continui delle funzioni e dei servizi identificati come essenziali.

Dunque, le regole del PSNC si rivolgono in particolare alla tutela dei beni ICT: i soggetti inclusi nel Perimetro sono tenuti a individuare e mantenere aggiornato l'elenco dei beni ICT considerati strategici per l'erogazione delle funzioni e dei servizi essenziali. Su tali beni si applicano rigorose misure di sicurezza, definite da specifici decreti attuativi, che comprendono la valutazione e gestione del rischio, l'adozione di piani di sicurezza, il monitoraggio continuo delle infrastrutture e la predisposizione di procedure per la gestione degli incidenti cibernetici allo scopo di assicurare la sicurezza delle funzioni e dei servizi essenziali dello Stato e, con esse, tutelare la sicurezza nazionale.

Per evitare la compromissione dei beni ICT, è previsto che ogni acquisizione di beni, sistemi e servizi destinati agli asset strategici sia sottoposta a una comunicazione preventiva al

Centro di valutazione e certificazione nazionale, che ne verifica la conformità agli standard di sicurezza richiesti. Inoltre, ogni incidente che impatti su questi beni deve essere notificato tempestivamente al CSIRT Italia, consentendo così una risposta coordinata e tempestiva agli eventi che potrebbero mettere a rischio la continuità operativa. Il quadro di tutela si completa con l'obbligo di sottoporre i beni ICT a valutazioni tecniche e verifiche periodiche, assicurando che le misure adottate siano sempre adeguate rispetto all'evoluzione delle minacce cibernetiche.
In questo modo, la protezione dei beni ICT si traduce in un insieme di azioni preventive e reattive che riducono la probabilità di compromissione e rafforzano la resilienza delle infrastrutture digitali critiche del Paese.
L'Autorità che regola e vigila sul Perimetro è l'Agenzia per la cybersicurezza nazionale (ACN), alla quale la legge affida il ruolo centrale nel coordinare le attività di prevenzione, monitoraggio e risposta agli incidenti, nonché nell'aggiornamento periodico delle misure di sicurezza e nella promozione della cooperazione tra pubblico e privato.

APPROFONDIMENTI

- Cavelty, Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authori*ty, in *Journal of European Public Policy*, Vol. 30, 2023.
- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277 ss.
- Ricotta, *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in Colaiacovo (a cura di), *Sicurezza, informazioni, giustizia penale*, Pisa, 2023, 359 ss.

VOCI CORRELATE

AGENZIA DI CYBERSICUREZZA NAZIONALE (ACN)
ARCHITETTURA NAZIONALE DI CYBERSICUREZZA
MISURE DI SICUREZZA
NIS (DIRETTIVE NIS)

PHISHING

Il *phishing* è un'attività illecita condotta con l'inganno a danno degli utenti della rete Internet. Essa consiste nella sottrazione di dati o informazioni sensibili (dati finanziari, codici di accesso bancari, passwords) e di norma avviene mediante l'invio di messaggi di posta elettronica ingannevoli a cui la vittima "abbocca". Il termine *phishing* deriva, infatti, dalla crasi dei termini inglesi *phreaking* (strumento hardware di pirataggio telefonico) e *fishing* (pescare). Il malintenzionato invia una specifica esca elettronica, mail con allegati o sms contenenti link diretti a risorse web fasulle, con l'intendo di indurre la vittima del *phishing* a rivelare dati sensibili. Le esche elettroniche sono sempre più raffinate, tanto da sembrare comunicazioni veritiere provenienti da banche o società di servizi Internet (ad es. *PayPal* o siti di eCommerce). Esse rinviano invece a pagine web contraffatte ad arte, cioè simili sia nella grafica, sia nel tenore linguistico e lessicale a quella legittima, in cui la vittima inserire le proprie credenziali che, invece di seguire una strada protetta da protocolli di sicurezza, imboccheranno una trasmissione in chiaro registrata dal malintenzionato.

Così, a titolo d'esempio, le credenziali di accesso al proprio account di home banking potranno permettere all'aggressore di disporre a proprio favore bonifici online in frode al titolare del conto concorrente.

La qualificazione giuridica di un atto di *phishing* richiede un'analisi dettagliata della condotta dell'agente cioè del *phisher*, la quale può manifestarsi in modi diversi e, quindi, può integrare diverse fattispecie diversamente sanzionabili. Essa può configurare un trattamento illecito di dati, in violazione dell'art. 167 del Codice privacy, e diversi reati previsti dal Codice penale, come: la truffa, la frode informatica, l'accesso abusivo ad un sistema informatico, finanche la sostituzione di persona.

APPROFONDIMENTI

- Cajani, *Profili penali del phishing,* in *Cassazione penale,* 2007, 2294 ss.

- Cocchi, *Phishing e nuovi attacchi informatici. Modalità operative e strategie difensive,* Ivrea, 2022.
- Costabile, Mazzaraco, Cajani, *Phishing e furto d'identità digitale: indagini informatiche e sicurezza bancaria,* Milano, 2008.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERCRIME
FATTORE UMANO
INGEGNERIA SOCIALE

POLIZIA POSTALE

La Polizia postale e delle comunicazioni è una specialità della Polizia di Stato. Istituita nel 1981, essa si occupa del contrasto alla criminalità informatica e ai reati contro l'inviolabilità e la libertà delle comunicazioni. È articolata in venti compartimenti regionali e ottanta sezioni territoriali, che fanno capo al Servizio centrale, con sede a Roma. Dal 2022 gli uffici periferici sono denominati COSC (Centro operativo sicurezza cibernetica) e SOSC (Sezione operativa sicurezza cibernetica). È coordinata a livello centrale dal Servizio polizia postale e per la sicurezza cibernetica, attivo anche nella cooperazione europea e internazionale sulla cyber-criminalità. Le aree d'intervento della Polizia postale e delle comunicazioni includono: pedopornografia, cyberterrorismo, diritto d'autore, attacchi informatici, tutela delle infrastrutture critiche, frodi commerciali online. Nell'ambito della Polizia postale opera il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) che si incaricato della prevenzione e del contrasto dei reati informatici diretti contro le infrastrutture critiche nazionali.
Alla Polizia postale e delle comunicazioni può rivolgersi chiunque intenda segnalare o denunciare fatti in materia di criminalità informatica, telecomunicazioni e internet.

APPROFONDIMENTI

- Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2024, 2, 277 ss.
- Polizia postale e per la sicurezza cibernetica, *Report Annuale 2024,* 2024.
- Ricotta, *Agenzia per la* cybersicurezza *nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in *Rivista trimestrale di diritto penale contemporaneo*, 2023, 1, 97 ss.
- Trombetta, *Ministero dell'interno e cybersecurity*, in Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023, 85 ss.
- Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023.

VOCI CORRELATE

ACCESSO ABUSIVO A SISTEMA INFORMATICO
CYBERATTACCO (ATTACCO INFORMATICO)
CYBERCRIME

p

PRETEXTING

Il *pretexting* è un tipo di cyberattacco di ingegneria sociale, basato su un pretesto, cioè su una storia inventata, attraverso cui l'agente manipola la vittima. Il pretesto serve per conquistare la fiducia della persona attaccata, che è manipolata e indotta a condividere informazioni sensibili, scaricare *malware*, inviare denaro a persone criminali o danneggiare in altro modo sé stessa o l'organizzazione per cui lavora.
Rientrano nella modalità del *pretexting* gli attacchi mirati come lo *spear phishing* (diretto a una persona specifica) o il *whale phishing* (mirato a dirigenti o utente con accesso privilegiato a informazioni o sistemi sensibili) o ancora il *Business Email Compromise* (BEC), cioè la compromissione di e-mail aziendali.
Il *pretexting* è impiegato anche per attacchi non mirati, come gli *spray-and-pray* inviati via e-mail, il *vishing* (*phishing* vocale) o lo *smishing* (*phishing* tramite SMS).

Al *pretexting* può essere associato lo *spoofing*, cioè la falsificazione di indirizzi e-mail e numeri di telefono per far sembrare che un messaggio provenga da un'altra fonte.

APPROFONDIMENTI

- Steinmetz, *The Identification of a Model Victim for Social Engineering: A Qualitative Analysis*, in *Victims & Offenders*, vol. 16, 4, 2021, 540 ss.
- Watson, Mason, Ackroyd, *Social Engineering Penetration Testing*, 2014.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
INGEGNERIA SOCIALE
PHISHING

PRIVACY

Il termine inglese privacy, reso in italiano con riservatezza o privatezza, è utilizzato nel linguaggio comune per identificare la dimensione della vita privata della persona. In questa sfera riservata quindi rientrano i dati e le informazioni su fatti personali o su cui la persona desidera mantenere la segretezza.
Dal punto di vista giuridico la privacy diventa un diritto tutelabile come «right to be let alone» (USA 1890), cioè «diritto ad essere lasciati soli». Su questa linea, nel 1975 la Corte di Cassazione italiana riconosce per la prima volta il diritto alla privacy come il diritto del singolo alla riservatezza o alla «tutela dell'intimità privata» rispetto a fatti o vicende che siano tali da non essere oggetto di interesse «socialmente apprezzabile» per i terzi.
Nel nuovo conteso della società digitalizzata, il primo diritto alla privacy è evoluto: esso non riguarda più *solo* la protezione della vita privata da ingerenze esterne, ma anche la protezione da potenziali lesioni a diritti fondamentali, conseguenti alla circolazione online di dati e informazioni personali.
Cambia la natura del diritto, da libertà negativa (libertà da ingerenze esterne) a libertà positiva come «diritto all'autodeterminazione informativa della persona», cioè il diritto del soggetto cui le informazioni personali si riferiscono di esercitare legittimamente un controllo su di esse.
Col fine di definire un livello comune di protezione del diritto alla privacy, l'Unione europea adotta prima la Direttiva 95/46/CE, poi il Regolamento (UE) 2017/679 (Regolamento generale sulla protezione dei dati personali o *General Data Protection Regulation* - GDPR). Il diritto alla protezione dei dati personali è anche un diritto fondamentale riconosciuto nella Carta dei diritti fondamentali dell'Unione europea (art. 8).

APPROFONDIMENTI

- Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello,* Napoli, 2018.
- Flor, *Riservatezza informatica*, in *Enciclopedia Treccani online*, 2017.

- Frosini, *La protezione della riservatezza nella società informatica*, in Matteucci (a cura di), *Privacy e banche dei dati*, Bologna, 1981, 37 ss.
- Rodotà, *Repertorio di fine secolo,* Roma-Bari, 1999.

VOCI CORRELATE

DATA BREACH
DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
RISERVATEZZA

PUNTO DI CONTATTO NIS

Le Direttive NIS (NIS 1 e NIS 2) impongono agli Stati membri dell'Unione europea di designare un Punto di contatto unico con il compito di garantire la cooperazione transfrontaliera delle autorità di uno Stato membro con quelle degli altri Stati membri, e, ove opportuno, con la Commissione europea e con l'European Union Agency for Cybersecurity (ENISA). Il Punto di contatto deve garantire anche la cooperazione intersettoriale con altre autorità competenti all'interno dello stesso Stato membro (art. 8, co. 3, 4 e 6, Direttiva (UE) 2022/2555; art. 8, co. 3, 4 e 6, Direttiva (UE) 2016/1148).

Il Punto di contatto unico può coincidere con l'autorità competente per la cybersicurezza istituita dallo Stato membro.

In Italia, l'Agenzia per la cybersicurezza nazionale (ACN) è l'autorità nazionale per la cybersicurezza ed è anche Punto di contatto unico tramite l'azione del *Computer Security Incident Response Team* (CSIRT) Italia, che è una sua articolazione interna (art. 7, co. 1, let. *d)*, d.l. 82 del 2021 convertito con modificazioni dalla legge n. 109 del 2021).

APPROFONDIMENTI

- Cavelty, Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authori*ty, in *Journal of European Public Policy*, Vol. 30, 2023.
- Ricotta, *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in Colaiacovo (a cura di), *Sicurezza, informazioni, giustizia penale*, Pisa, 2023, 359 ss.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)
EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)
NIS (DIRETTIVE NIS)

r

RANSOMWARE

Il *ransomware* (dalla crasi dei termini *ransom*, riscatto, e *malware,* software dannoso) è un programma informatico malevolo, in grado di infettare una rete, un sistema informatico, un computer, uno smartphone o qualunque altro dispositivo elettronico. Il *ransomware* impedisce alla vittima di accedere al sistema informatico e quindi ai suoi dati.
Si distinguono due tipi di ransomware: i *cryptor* che criptano i file contenuti in un dispositivo; e i *blocker* che rendono impossibile l'accesso al dispositivo infettato. In ogni caso, l'indisponibilità dei dati o del sistema avviene attraverso un complesso sistema di cifratura messo in atto dall'aggressore. Per poter accedere nuovamente al dispositivo e ai dati originali è necessario ottenere una chiave di decrittazione, posseduta dall'aggressore, che la mette a disposizione della vittima dietro pagamento di un riscatto. Il riscatto — estorto mediante un messaggio sullo schermo del dispositivo infettato — dovrà essere corrisposto in cripto valuta (ad es. bitcoin). Col *ransomware* l'attaccante si muove su due fronti, realizzando una doppia estorsione (*double extorsion)*. Se cioè la vittima non paga il riscatto, l'aggressore minaccia di diffondere i suoi dati su canali non autorizzati – di comunicazione o sul *dark web* –, rendendoli così visibili a terzi. La seconda minaccia costituisce un ulteriore elemento di pressione sulla vittima. I principali vettori di infezione del *ransomware* sono: la ricezione di e-mail contenenti allegati infetti o collegamenti diretti a software malevoli; la navigazione su siti web compromessi da hacker per essere veicoli di contagio da *ransomware*; cliccare su link o banner su siti web o social network non sicuri; usare reti aziendali vulnerabili. Inoltre, un dispositivo infettato può essere esso stesso un veicolo di infezione: può diffondere il *ransomware* anche ad altri dispositivi connessi sulla rete, sfruttando ad esempio le sincronizzazioni tra dispositivi.
Infine, è importante sapere che le principali linee guida e migliori pratiche a livello internazionale sconsigliano il pagamento del riscatto, perché non è certo che il criminale consegni effettivamente la chiave di decifratura. È preferibile denunciare l'attacco *ransomware* alla polizia postale e contattare centri tecnici specializzati per sbloccare l'accesso al APPRO.

APPROFONDIMENTI

- ENISA, Threat Landscape for Ransomware Attacks, 2022.
- Fiorinelli, *Il ransomware nel DDL Cybersicurezza: dalla fattispecie di estorsione informatica al coordinamento tra indagini e incident response,* in Fiorinelli, Giannelli (a cura di), *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2*, sezione monografica della Rivista italiana di informatica e diritto, 1, 2024, 35 ss.
- Liska, Gallo, Viscardi, *Ransomware. Come difendersi dalle estorsioni digitali,* Milano, 2017.
- Proscia, *Security awareness,* in Razzante (a cura di), *Manuale di cybersicurezza,* Pisa, 2023, 285 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
MALWARE
POLIZIA POSTALE

REGULATORY SANDBOX

Le *regulatory sandboxes* — in italiano spazi di sperimentazione normativa — consentono agli operatori economici di testare prodotti e servizi innovativi in un ambiente di prova controllato, secondo un piano specifico sviluppato e concordato assieme a una o più autorità competenti, con la guida e la supervisione di queste ultime.
Di norma, con le *regulatory sandboxes* per il caso oggetto di sperimentazione si prevedono una temporanea sospensione dell'applicazione di alcune norme di settore, ferma restando l'applicazione di clausole di salvaguardia per la tutela di obiettivi normativi generali (ad es. protezione dei dati personali, sicurezza e protezione dei consumatori ecc.).

Per l'operatore economico, l'accesso alla *regulatory sandbox* garantisce migliori condizioni per sviluppare prodotti e servizi in maniera conforme alla legge fin dalla fase della progettazione. Questo procedimento è infatti guidato e supervisionato delle autorità competenti, che sono generalmente tenute a dare indicazioni sulle proprie aspettative. Per l'autorità, il vantaggio consiste nel poter venire a conoscenza di nuovi sviluppi tecnologici, prima che gli stessi vengano immessi nel mercato (cd. *regulatory learning*).

Dal punto di vista giuridico e in particolare della tecnica normativa, la *regulatory sandbox* è forma innovativa di co-regolazione particolarmente promettente nell'ambito della regolamentazione dei nuovi prodotti e fenomeni tecnologici. Negli ultimi anni, le *regulatory sandboxes* stanno infatti prendendo spazio soprattutto nell'ambito del FinTech e, più in generale, dell'intelligenza artificiale e della cybersicurezza.

Le *regulatory sandboxes* sono ad esempio previste dall'*AI Act* (Regolamento (UE) 2024/1689, al Capo IV "Misure a Sostegno dell'Innovazione") e dal *Cyber Resilience Act* (Regolamento (UE) 2024/2847, all'art. 33 "Misure di sostegno per le microimprese e le piccole e medie imprese, comprese le start-up").

APPROFONDIMENTI

- Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista italiana di informatica e diritto*, 2, 2023, 201 ss.
- Bagni, Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, CINI's Cybersecurity National Lab, 2025.
- Baldini, Francis, *AI Regulatory Sandboxes between the AI Act and the GDPR: The role of Data Protection as a Corporate Social Responsibility*, in CEUR Workshop Proceedings, 2024.
- Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in *Rivista italiana di informatica e diritto*, 1, 2025, 258 ss.
- Longo, *Gli spazi di sperimentazione normativa o anche regulatory sandboxes nell'AI Act*, in Calzolaio, Iannuzzi, Longo, Orofino, Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale,* Torino 2025, 111 ss.
- Ranchordas, Vinci, *Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture*, in *Italian Journal of Public Law*, vol. 16, 1, 2024.

VOCI CORRELATE

AI (ARTIFICIAL INTELLIGENCE)
AI ACT (ARTIFICIAL INTELLIGENCE ACT)
CYBER RESILIENCE

REPUTAZIONE

La reputazione è tutelata tra i diritti della personalità ai sensi degli artt. 2 e 3 della Costituzione. Essa viene tradizionalmente intesa come la considerazione sociale di cui gode un soggetto (individuo, persona giuridica o ente collettivo) all'interno della società ed è collegata al concetto di dignità personale. Per tali caratteri, è considerato nullo ogni patto con cui il soggetto rinunzi preventivamente dietro corrispettivo alla tutela della propria reputazione o si obblighi comunque egli stesso a violarla.

Nella società digitalizzata il concetto di reputazione assume un nuovo significato: la reputazione digitale, intesa come proiezione che il soggetto offre di sé attraverso le informazioni condivise online. La reputazione nel mondo fisico e la reputazione digitale però possono non coincidere, perché il soggetto può selezionare e controllare solo parzialmente le informazioni che inserisce direttamente online.

Il diritto soggettivo alla reputazione è tutelato in sede giurisdizionale. In sede civile, la lesione alla sfera reputazionale comporta il diritto al risarcimento del danno (artt. 2043 e 2059 del Codice civile), in particolare nei casi di ingiuria (l'offesa è comunicata alla persona offesa, che può difendersi) o diffamazione (l'offesa è comunicata a terzi, in assenza della persona offesa, che quindi non può difendersi).

In ambito penale, la diffamazione è sanzionata dall'art. 595 del Codice penale, che tutela la reputazione sociale. Inoltre, il Codice penale punisce la diffusione, anche in rete, delle conversazioni carpite con l'inganno e senza il consenso riprese audio o video, registrazioni della persona offesa, allo scopo di arrecare danno alla reputazione altrui (artr. 617-*septies* c.p).
Sono inoltre punite come lesive della reputazione la diffusione di fake news o di immagini *fake*, la divulgazione virale in rete di campagne denigratorie, la divulgazione sui social network e sul web immagini o video privati, a sfondo sessuale, diffusi a scopi vendicativi e lesivi della reputazione della vittima, che integra il reato di *revenge porn* (art. 612-ter c.p.).

APPROFONDIMENTI

- Foglia, *L'identità personale nell'era della comunicazione digitale*, in Bilotta, Raimondi (a cura di), *Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato*, Napoli, 2020, 265 ss.
- Ricci, *Il valore economico della reputazione nel mondo digitale. Prime considerazioni*, in *Contratti e Impresa*, 6, 2010.
- Sorgato, *Revenge Porn. Aspetti giuridici, informatici e psicologici*, Milano, 2020.
- Tampieri, *L'identità personale: un diritto dal volto poliedrico*, in Bilotta, Raimondi (a cura di), *Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato*, Napoli, 2020, 223 ss.

VOCI CORRELATE

r

FAKE NEWS
IDENTITÀ DIGITALE

RETE DI CSIRT

La disciplina NIS (1 e 2) istituisce la Rete di CSIRT quale sistema che ha l'obiettivo di scambiare informazioni di cybersicurezza tra i suoi componenti per garantire un approccio cooperativo e unificato alla sicurezza cibernetica (art. 15, Dir. (UE) 2022/2555; art. 12, Dir. (UE) 2016/1148).

La Rete è composta da rappresentanti dei CSIRT designati o istituiti negli Stati membri (ad es. il CSIRT Italia), dai rappresentanti dei CSIRT degli organi e delle agenzie dell'Unione (riuniti nel cd. CERT-EU). La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'*European Unione Agency for Cybersecurity* (ENISA) ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT.

APPROFONDIMENTI

- Bendiek, *The EU as a force for peace in international cyber diplomacy,* in *Stiftung Wissenschaft und Politik*, 19, 2018.
- Fysarakis, Mavroeidis, Athanatos, Spanoudakis, Ioannidis, *A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness*, in *IEEE International Conference on Big Data (Big Data)*, 2022.
- Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, in *Rivista dell'Associazione Italiana dei Costituzionalisti*, 4, 2022.
- Serini, *Collective cyber situational awareness in EU. A political project of difficult legal realisation?,* in *Computer Law & Security Review*, vol. 55, 2024.

VOCI CORRELATE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)
COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)
EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)
NIS (DIRETTIVE NIS)

RISERVATEZZA

Nel linguaggio comune, il termine riservatezza indica la qualità o la condizione di qualcosa che deve rimanere privato, non accessibile o non condiviso con terze parti. L'uso della nozione di riservatezza può variare a seconda del contesto: nel linguaggio comune, il termine tende ad essere impiegato in modo fungibile rispetto ad altri concetti affini. In particolare, la riservatezza è frequentemente associata a nozioni quali riserbo, segreto, vita privata, intimità, protezione dei dati personali e privacy.
Nell'ambito giuridico si riscontra un'esigenza di maggiore precisione concettuale, che porta a differenziare la riservatezza dagli altri concetti, pur riconoscendone la connessione sostanziale.
È possibile, tuttavia, individuare un nucleo comune a tutte le situazioni che generalmente ricadono sotto l'ombrello della riservatezza. Tale nucleo è identificabile nella centralità della persona, intesa sia nella sua dimensione fisica che nel suo vissuto morale, e nella necessità di tutelare gli interessi socialmente rilevanti ad essa connessi.
Il riconoscimento di tali interessi come meritevoli di protezione giuridica riflette l'evoluzione della riservatezza da mera istanza individuale a principio fondamentale dell'ordinamento. Le implicazioni giuridiche di tale evoluzione si estendono dal diritto alla privacy, inteso come diritto alla protezione della sfera personale, alla protezione dei dati personali, intesa, invece, come la disciplina specifica che regola il trattamento dei dati identificativi e sensibili degli individui.

APPROFONDIMENTI

- Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello,* Napoli, 2018.
- D'Orazio, Finocchiaro, Pollicino, Resta (a cura di), *Codice della privacy e data protection, Milano,* 2021.
- Finocchiaro, *Privacy e protezione dei dati personali,* Bologna, 2012.
- Frosini, *La protezione della riservatezza nella società*

informatica, in Matteucci (a cura di), *Privacy e banche dei dati*, Bologna, 1981, 37 ss.

- Patrono, Privacy e vita privata (dir. pen.), in *Enciclopedia del diritto, Milano,* 1986.
- Rodotà, *Tecnologie e diritti,* Bologna 1995.
- Rodotà, *Intervista su privacy e libertà,* Roma-Bari, 2005.

VOCI CORRELATE

DATI PERSONALI
INTERESSATO (DIRITTI DELL')
PRIVACY

RISK-BASED APPROACH

Il termine *risk-based approach* si riferisce a un approccio che considera il rischio come un fattore determinante nella pianificazione, nella decisione, nella gestione e nell'allocazione delle risorse, trovando applicazione in settori dove è necessario valutare adeguatamente i rischi, quali la finanza, la sicurezza, la salute e il digitale. In particolare, la gestione del rischio, anche sul piano normativo e regolatorio, rappresenta la necessità di fronteggiare l'incertezza anticipando e riducendo i possibili effetti avversi derivanti da esternalità negative.

In questo senso, l'approccio basato sul rischio si basa fondamentalmente sulla creazione di un quadro normativo all'interno del quale responsabilità e obblighi sono gradualmente adeguati al concreto rischio di determinate attività svolte dalle parti. In questo senso il *risk-based approach* prevede che la valutazione del rischio e la successiva individuazione delle relative misure di mitigazione vengano svolte direttamente dai soggetti destinatari della regolazione.

Nel XXI secolo si assiste ad una notevole diffusione del *risk-based approach* nella maggioranza dei sistemi giuridici occidentali.

L'Unione europea ha adottato tale approccio inizialmente con riguardo al diritto ambientale e alla tutela della salute, per poi ampliarne la portata anche alla regolazione delle tecnologie digitali e in particolare, da ultimo, delle applicazioni dell'intelligenza artificiale, per incentivare una maggiore responsabilità da parte degli attori pubblici e privati, specialmente con riferimento ai potenziali effetti connessi all'utilizzo di queste tecnologie e al trattamento dei dati personali. Questo modello regolatorio caratterizza diversi importanti atti normativi dell'Unione europea, tra cui il Regolamento (UE) 2016/679 generale sulla protezione dei dati (*General Data Protection Regulation* - GDPR), il Regolamento (UE) 2022/2065 sui servizi digitali (Digital Services Act - DSA) e il più recente Regolamento (UE) 2024/1689 sull'intelligenza artificiale (*Artificiale Intelligence* Act - AI Act).

APPROFONDIMENTI

- D'Antino, *L'approccio basato sul rischio nell'AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *Federalismi.it*, 18, 2025, 15 ss.
- De Gregorio, Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2, 2022, 473 ss.
- Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020.
- Longo, *La disciplina del "rischio digitale"*, in Calzolaio, Iannuzzi, Longo, Orofino, Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale,* Torino, 2025, 53 ss.
- Mahler, *Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal*, in *Nordic Yearbook of Law and Informatics 2020-2021: Law in the Era of Artificial Intelligence*, 2022, 247 ss.

VOCI CORRELATE

AI (ARTIFICIALE INTELLIGENCE)
AI ACT (ARTIFICIALE INTELLIGENCE ACT)
GENERAL DATA PROTECTION REGULATION (GDPR)

S

SERVICE PROVIDER

Nel diritto dell'informatica e delle tecnologie digitali, il termine *service provider* indica genericamente il fornitore di servizi della società dell'informazione (intermediario, piattaforma, social network, ecc.), identificato anche con la sigla ISP (*internet service provider*) o OSP (*online service provider*).

La Direttiva europea 2000/31 sul commercio elettronico originariamente distingueva, ai fini della definizione del regime di responsabilità, tra provider di servizi di *mere conduit* (trasmissione di informazioni o fornitura di accesso alla rete), *caching* (memorizzazione temporanea) e *hosting* (memorizzazione), escludendo l'esistenza, in capo ai provider, di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, nonché di un obbligo di ricercare attivamente fatti o circostanze indicativi della presenza di attività illecite.
Il Regolamento europeo 2022/2065 sui servizi digitali (*Digital Services Act* - DSA) ha introdotto una nuova disciplina per i fornitori di servizi digitali, alla luce dei nuovi modelli di business e delle nuove funzioni (social network, piattaforme ecc.) che essi attualmente svolgono, nell'economia e nei rapporti sociali.
Accanto ai servizi intermediari di *mere conduit*, *caching*, *hosting*, il DSA si riferisce specificamente alle piattaforme online e ai motori di ricerca. In base al DSA, i *service provider* sono soggetti a un insieme strutturato e corposo di obblighi (di esecuzione dei provvedimenti dell'autorità, di cooperazione, di *due diligence*, di *notice and action*, di valutazione e gestione dei rischi sistemici, ecc.), rispetto a possibili attività o contenuti illeciti, declinati diversamente in dipendenza della tipologia del servizio e delle dimensioni del fornitore.

Le discipline più recenti in materia di prove elettroniche e digitali (*e-evidence*) prevedono il coinvolgimento strutturale dei *service provider* nelle attività di raccolta, conservazione e circolazione della prova. Questo approccio è presente, ad esempio, nel cd. E-Evidence Package adottato dall'Unione europea; nel Secondo Protocollo addizionale alla Convenzione di Budapest; nel Cloud Act in USA.

APPROFONDIMENTI

- Bertolini, Episcopo, Cherciu, *Liability of online platforms*, 2021.
- Church, Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law*, 2023, 53 ss.
- Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford, 2020.
- Tosza, *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in *Computer Law & Security Review*, 2021, 43, 105614.
- Tosza, *Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights*, in *Common Market Law Review*, 2024, 61, 1, 139 ss.
- van Dijck, Poell, de Waal, *The Platform Society*, Oxford, 2018.

VOCI CORRELATE

DIGITAL SERVICES ACT (DSA)
INDIRIZZO IP
INTERNET

SEXTORSION

La parola *sextorsion* deriva dall'unione tra i termini *sex* e *extortion* cioè una estorsione sessuale condotta online a danni di vittime cui vengono estorte immagini erotiche usate poi mezzo di riscatto (per lo più richiesta di denaro).
La vittima è adescata amichevolmente su piattaforme di messaggistica, siti di incontri, social media. Il truffatore instaura un rapporto intimo e di fiducia con la vittima che gli consente di ottenere immagini o video intimi, con o senza il suo consenso (ad es. sfruttando videochiamate o tecniche di *hacking* per registrare materiale audio e video). Segue quindi la minaccia di divulgazione del materiale sensibile e la richiesta di denaro, di norma in criptovalute o mediante trasferimenti non tracciabili. La richiesta di denaro può essere accompagnata da altre minacce e richieste legate alla sfera intima, che avviano un ciclo di abusi psicologici. La *sextorsion* è una condotta criminale potenzialmente lesiva di diversi beni giuridici protetti dall'ordinamento giuridico: estorsione (art. 629 c.p.) diffamazione (art. 595, col. 3, c.p.); interferenze illecite nella vita privata (art. 615 *bis* c.p.); violenza privata (art. 610 c.p.); minacce (art. 612 c.p.).

APROFONDIMENTI

- Ray, Henry, *Sextortion: A Scoping Review,* in *Trauma, Violence & Abuse*, 26, 1, 2025, 138 ss.
- Schiavon, *Cat-Fish, Romance Fraud e Sextortion: le nuove frontiere dell'adescamento nei social media,* in Conti, Pietrangelo, Romano (a cura di), *Social media e diritti. Diritto e social media*, Napoli, 2017, 170 ss.
- Vergara, *L'estorsione online: "sextorsion" e l'estorsione a mezzo "ransomware*" in *Rivista penale,* 9, 2022, 657 ss.

VOCI CORRELATE

CYBERBULLISMO
CYBERCRIME
IDENTITÀ DIGITALE

SICUREZZA NAZIONALE

Il concetto giuridico di sicurezza nazionale esprime l'insieme dei valori supremi su cui si fonda la sopravvivenza dello Stato come comunità di istituzioni e di persone cittadini, ma anche tutti gli strumenti e gli organi preposti al proteggere la Nazione.

Nel 1977 la Corte costituzionale definì la sicurezza dello Stato come «sicurezza esterna ed interna dello Stato, della necessità di protezione da ogni azione violenta o comunque non conforme allo spirito democratico che ispira il nostro assetto costituzionale dei supremi interessi che valgono per qualsiasi collettività organizzata a Stato e che [...] possono coinvolgere la esistenza stessa dello Stato» (sentenza n. 86 del 1977). La sicurezza cioè va oltre la difesa dello Stato democratico e delle sue istituzioni, ma comprende anche aree ulteriori di intervento: l'economia, l'industria, l'energia o lo sviluppo tecnologico.

In questa più ampia accezione, la sicurezza nazionale passa dalla sola dimensione della sicurezza dello Stato-apparato alla sicurezza dello Stato-comunità, che comprende quindi tutte le sue plurime e trasversali declinazioni in campo sociale, economico e scientifico.
Resta in ogni caso una nozione dinamica, aperta alle evoluzioni socio-economiche, prime fra tutte quelle legate alle esigenze di sicurezza e protezione ambientale o digitale, compresa la cybersicurezza.

APPROFONDIMENTI

- Giupponi, *Sicurezza e potere (*voce) in *Encicolpedia del diritto, I tematici, Costituzione e potere*, Milano, 2024, 1149 ss.
- Giupponi, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010.
- Labriola, *Le informazioni per la sicurezza dello Stato*, Milano, 1978.

VOCI CORRELATE

AGENZIA DI CYBERSICUREZZA NAZIONALE (ACN)
ARCHITETTURA NAZIONALE DI SICUREZZA CIBERNETICA
PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA (PSNC)

SISTEMA PUBBLICO DI IDENTITÀ DIGITALE (SPID)

Il Sistema Pubblico di Identità Digitale (SPID) è uno strumento tecnico per l'accesso ai servizi telematici delle amministrazioni pubbliche da parte di cittadini e imprese. Il sistema SPID consente l'identificazione univoca dell'utente del servizio, come previsto in linea generale dalle disposizioni del Codice dell'amministrazione digitale - CAD (d. lgs. 7 marzo 2005 n. 82) e in particolare dall' art. 3-*bis* che impone alle amministrazioni di assicurare a chiunque il diritto di accedere ai loro servizi online.
Secondo la definizione normativa (art. 64 CAD; DPCM 24 ottobre 2014 o "Decreto SPID") lo SPID è il mezzo che «consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati» in modo da permettere «ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano» (art. 2, Decreto SPID). Particolarmente rilevanti le numerose regole tecniche che disciplinano il funzionamento dello SPID, contenute in determinazioni dell'Agenzia per l'Italia Digitale (AGID) aventi ad oggetto: le «regole tecniche» che disciplinano il suo funzionamento; le «modalità attuative per la [sua] realizzazione»; le «modalità di accreditamento dei soggetti SPID»; e, infine, le «procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale».

Negli anni successiva alla pandemia da covid-19, che hanno prodotto una accelerazione nell'uso delle applicazioni digitali anche per l'accesso ai servizi, il quadro normativo si è ulteriormente irrobustito. Col cosiddetto Decreto semplificazioni (d.l. 16 luglio 2020 n. 76), a partire dal 28 febbraio 2021 lo SPID e la Carta d'Identità Elettronica (CIE) sono oggi gli unici strumenti che i soggetti pubblici utilizzano per l'«identificazione dei cittadini che accedono ai propri servizi in rete».
Lo sviluppo dello SPID a livello nazionale è conforme alla strategia eurounionale sulla identità digitale unica europea, prevista Regolamento eIDAS n. 910 del 2014 e dall'adottando Regolamento

eIDAS 2, finalizzato a istituire il cd. Portafoglio Europeo di Identità Digitale (*European Digital Identity Wallet* – EDIW), che dovrebbe consentire ai cittadini dell'Unione di disporre di un'unica identità digitale per accedere a tutti servizi pubblici e privati dell'intera U.E.

A livello nazionale, l'ampia diffusione dello SPID nella popolazione ha indotto il legislatore a consentirne l'uso per la raccolta delle firme necessarie a proporre alcuni referendum abrogativi (in tema di cd. eutanasia legale e di cd. cannabis legale nell'estate del 2021). A questo fine è stato istituito «un apposito fondo [...] destinato alla realizzazione di una piattaforma per la raccolta delle firme degli elettori necessarie per i referendum previsti dagli artt. 75 e 138 Cost. nonché per i progetti di legge *ex* art. 71, co. 2, Cost.» (art. 1, co. 341, legge 30 dicembre 2020 n. 178; e DPCM 9 settembre 2022).

Si tratta di un sistema oramai ampiamente diffuso nella cittadinanza (nel 2024 il numero di identità SPID attive raggiunge i quasi 40 milioni) e con grandi potenzialità per il funzionamento dello Stato costituzionale democratico, purché la cosiddetta *spid-democracy* risulti pienamente rispettosa dei principi fondamentali dell'ordinamento repubblicano.

APPROFONDIMENTI

- Pietrangelo, *Sui "diritti di cittadinanza digitale". Note a margine di un opaco percorso normativo*, in *Federalismi.it*, 2024, 129 ss.
- Pietrangelo, *Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione: luci ed ombre*, in D'Elia, Pietrangelo (a cura di*), Il Codice dell'amministrazione digitale*, Napoli, 2006.
- Resta, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica,* 2007, 511 ss.

VOCI CORRELATE

DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
IDENTITÀ DIGITALE

SPAM

Per spam s'intende un trattamento illecito di dati personali, che si realizza mediante l'invio di comunicazioni promozionali (ad es. pubblicità commerciale) senza preventivo consenso informato. Queste comunicazioni sono risultano così lesive del diritto alla riservatezza e alla protezione dei dati personali.
Le comunicazioni a contenuto promozionale sono trasmesse tramite mail, SMS, app di messaggistica o altri sistemi automatizzati di contatto, anche senza intervento umano.
Il fenomeno è regolato dall'articolo 130 del Codice in materia di protezione dei dati personali (d.lgs. n. 196 del 2003) e dal Regolamento (UE) 2016/679 generale sulla protezione dei dati personali (*General Data Protection Regulation* - GDPR), secondo cui qualsiasi attività di marketing diretto condotta attraverso mezzi elettronici presuppone il consenso informato dell'interessato. Se manca il consenso quindi il trattamento dei dati a fini promozionali è illecito
La normativa prevede un'eccezione a tale regola nel caso del cosiddetto *soft spam* o *soft opt-in*, che consiste nell'invio com mail di comunicazioni promozionali ai propri clienti aventi ad oggetto prodotti o servizi analoghi a quelli già acquistati In questa ipotesi il consenso è presupposto, purché ricorrano alcune specifiche condizioni: l'indirizzo e-mail è stato acquisito nel contesto della vendita di un prodotto o servizio; il cliente non ha espressamente rifiutato la ricezione di messaggi di qeusto tipo (cosiddetto *opt-out*); al cliente è sempre data la possibilità di opporsi agevolmente e gratuitamente in ogni successiva comunicazione. Si tratta di una eccezione che presuppone l'esistenza di una relazione commerciale in cui coesistano più interessi.
La pratica dello spam può essere sanzionata come violazione amministrativa dall'Autorità garante per la protezione dei dati personali (v. per esempio le Linee guida in materia di attività promozionale e contrasto allo spam del 2013) e illecito penale. In questo secondo caso, infatti, la presenza di condotte sistematiche, intrusive o fraudolente, potrebbe configurare reati come il trattamento illecito di dati personali (art. 167, d.lgs. n. 196 del 2003) o, in casi più gravi, molestie o disturbo alle persone (art. 660, c.p.).

APPROFONDIMENTI

- Citarella, *Spamming: interferenze nella sfera privata e violazione del diritto alla privacy,* in *Diritto dell'Internet,* 1, 2007, 27 ss.
- Di Ciommo, *Lo "spamming", dalle reti telematiche alle aule dei tribunali,* in *Il Foro italiano,* 1, 2004, 2908 ss.
- Levi, Zanichelli, *L'utilizzo dell'e-mail a fini pubblicitari: dallo "spamming" al "permission marketing",* in *Rivista di diritto industriale,* 4-5, 2001, 194 ss.
- Vizzoni, *Invii di "e-mail" promozionali ai clienti "non paganti": il "soft spam" al vaglio della Corte di Cassazione,* in *Persona e Mercato,* 3, 2023, 567 ss.

VOCI CORRELATE

DATI PERSONALI
GENERAL DATA PROTECTION REGULATION (GDPR)
INTERESSATO (DIRITTI DELL')

STAZIONI APPALTANTI

Nelle attività di *e-procurement* (digitalizzazione dei procedimenti di acquisto di beni e servizi delle pubbliche amministrazioni) le stazioni appaltanti sono i soggetti che affidano ad un operatore economico un contratto pubblico di appalto o di concessione avente per oggetto l'acquisizione di servizi o forniture oppure l'esecuzione di lavori o opere. Sono quindi stazioni appaltanti le pubbliche amministrazioni aggiudicatrici, gli enti aggiudicatori o in generale soggetti aggiudicatori di gare d'appalto.

Poteri e funzioni delle stazioni appaltanti sono definiti dagli articoli 62 e 63 del nuovo Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36), che sostituiscono la precedente normativa (d.lgs. n. 50 del 2016, artt. 37-39). La normativa del 2023 ha riforma il sistema di gestione degli appalti pubblici introducendo soluzioni per riorganizzare — e ridurre numericamente — le stazioni appaltanti, sia nei settori ordinari sia nei settori speciali. A questo fine, infatti, il nuovo Codice dei contratti pubblici ha previsto incentivi all'utilizzo delle centrali di committenza e delle stazioni appaltanti ausiliarie per l'espletamento delle gare pubbliche; nuove modalità di monitoraggio dell'accorpamento e della riorganizzazione delle stazioni appaltanti; il potenziamento della qualificazione e della specializzazione del personale anche mediante percorsi formativi.

Il nuovo quadro regolatorio distingue tra stazioni appaltanti qualificate e non qualificate. La qualificazione consiste in una valutazione basata su specifici parametri oggettivi previsti dalla normativa.

Le stazioni appaltanti qualificate possono bandire gare ed eseguire contratti in relazione al livello di qualificazione posseduta, oltre che affidarsi alle centrali di committenza. Inoltre, con gli altri enti possono utilizzare la qualificazione ottenuta per avviare un appalto congiunto con le stazioni appaltanti non qualificate o svolgere attività di committenza ausiliaria, offrendo supporto alle attività di committenza.

Le stazioni appaltanti non qualificate non possono procedere autonomamente sul mercato, ma possono ricorrere ad una centrale di committenza qualificata, rivolgersi a centrali di

committenza e stazioni appaltanti qualificate per le attività di committenza ausiliaria o effettuare ordini su strumenti di acquisto messi a disposizione dalle centrali di committenza qualificate e dai soggetti aggregatori. Anche per le stazioni non qualificate però il Codice prevede spazi di autonomia, in relazione all'affidamento e all'esecuzione di contratti per servizi e forniture di importo inferiore alla soglia europea e per lavori di manutenzione ordinaria d'importo inferiore a un milione di euro. In queste procedure le stazioni appaltanti non qualificate possono utilizzare gli strumenti telematici di negoziazione messi a disposizione dalle centrali di committenza qualificate.
Tra i soggetti pubblici con funzioni e poteri in materia di cybersicurezza, l'Agenzia per la cybersicurezza nazionale rientra fra le stazioni appaltanti qualificate; essa può infatti procedere in autonomia all'affidamento e all'esecuzione di appalti sopra la soglia comunitaria.

APPROFONDIMENTI

- Donato, Macchia, *La qualificazione delle stazioni appaltanti. La luce in fondo al tunnel normativo*, in *Astrid*, 14, 2022, 23 ss.
- Macchia, *La qualificazione delle amministrazioni appaltanti,* in *Giornale di diritto amministrativo* 1, 2017, 50 ss.
- Nunziata, *Aggregazione, centralizzazione e qualificazione della committenza*, in Macchia (a cura di) *Costruire e acquistare, Lezioni sul nuovo Codice dei contratti pubblici*, Torino, 2024, 63 ss.

VOCI CORRELATE

CENTRALI DI COMMITTENZA
E-PROCUREMENT

t

TALLIN (MANUALE DI)

Il Manuale di Tallin è un documento redatto in ambito scientifico che affronta il problema dell'applicabilità del diritto internazionale al fenomeno della guerra cibernetica (*cyber war*). Il Manuale nasce guida cioè come codificazione privata, ma esso è riconosciuto come il testo di riferimento in materia, anche per il contesto in cui è stato sviluppato e sistematizzato. Esso supplisce giuridicamente all'assenza di parametri certi, per esempio, per valutare se un cyber attacco può considerarsi un atto di guerra in senso proprio, e quindi, ad esempio, se permette una risposta militare legittima ai sensi del diritto costituzionale e internazionale.

Gli atti di guerra cibernetica vengono infatti realizzati in assenza di un quadro definitorio chiaro. Mancano, ad esempio, le definizioni di responsabilità degli attacchi (o anche solo un criterio che assicuri la riconducibilità degli attacchi agli Stati) e di *contractor* o *cyber-warrior*, ma soprattutto dei parametri universalmente riconosciuti che possano legittimare gli Stati a scendere in guerra dopo un attacco informatico. I conflitti armati dell'era post-bipolare e multipolare contengono numerosi elementi di complessità rispetto a quelli tradizionali: presenza di attori non statuali, impossibilità di definire il campo di battaglia e gli obiettivi precisi, impiego di strumenti non convenzionali da guerra ibrida.

Il Manuale di Tallin nasce dal confronto tra esperti (accademici e militari), occasionato nel 2007 dall'attacco ai danni di infrastrutture governative e d'informazione estoni (la cd. *Web War One*) e dell'incerta applicabilità dell'articolo 5 del Trattato Nato sulla difesa collettiva di uno stato aggredito. Conseguenza di quell'episodio è stata la costituzione del NATO *Cooperative Cyber Defence Centre of Excellence*, che ha sede a Tallin e si occupa di cooperazione tra gli Stati NATO in materia di difesa cibernetica.

Del Manuale esistono due versioni (2013 e 2017), entrambe pubblicate da Cambridge University Press. Nella seconda edizione il focus e il titolo del Manuale cambiano perchè incentrati sul concetto *cyber-operations* (non più di *cyber-warfare*). Le ragioni di tale nuovo orientamento risiedono nella numerosità

di attacchi cibernetici a danno della sicurezza nazionale degli Stati e nell'esigenza di individuare soluzioni diritto internazionale applicabili a operazioni cibernetiche condotte in tempo di pace.
Il *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* del 2017 è diviso in quattro parti (General international law and cyberspace; Specialised regimes of international law and cyberspace; International peace and security and cyber activities; The law of cyber armed conflict) per un totale 154 regole, ciascuna accompagnata da una spiegazione. Si segnalano qui alcune tra le più rilevanti.
La regola n. 68, secondo cui un'operazione cibernetica che costituisce «una minaccia o l'uso della forza contro l'integrità territoriale o l'indipendenza politica di uno Stato o che è in ogni caso in contraddizione con i fini delle Nazioni Unite, è illecita».
La regola n. 69, che definisce l'uso della forza, specificando che una *cyber-operation* è configurabile come tale «quando la sua portata e i suoi effetti (*its scale and effects*) sono comparabili con un'operazione bellica non cibernetica», quindi gli attacchi devono aver provocato danni rilevanti a beni di proprietà o la morte di cittadini. La regola n. 71, in cui sono definiti i presupposti della legittima difesa contro gli attacchi armati, che può essere esercitata dallo Stato vittima di una operazione cibernetica che raggiunga la soglia dell'attacco armato. In questo caso, il Manuale segue la cosiddetta dottrina degli effetti, i quali – in particolare per la loro analogia con i conflitti "analogici" – rilevano come causa di legittimazione per un'eventuale risposta bellica (e non l'atto di forza informatica in sè).

APPROFONDIMENTI

- Bufalini, *Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico*, in Lanciotti, Tanzi (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2012, 405 ss.
- Gatti, Giannelli, *Presupposti per la configurazione e la dichiarazione di guerra cibernetica*, in *DPCE Online*, 1, 2024.
- Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, 2025.

- Schmitt (ed.), *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERDEFENCE
CYBERTERRORISMO

TROJAN

Il *trojan* o captatore informatico è un software che consente di manovrare a distanza una macchina sfruttando un'architettura di rete di tipo *client/server*. Abbattendo la protezione del dispositivo, il captatore penetra nella macchina acquisendo il pieno controllo. Il trojan è quindi un *malware* appartenente alla categoria dei sistemi informatici di controllo da remoto (*Remote Control System*).
Per le sue caratteristiche tecniche, esso può essere impiegato anche come strumento di indagine da parte della polizia, che lo utilizza per infiltrarsi nei dispositivi elettronici (come smartphone o computer) e accedere ai dati in essi presenti. Nella procedura di infiltrazione quindi, semplificando, sono attivi due dispositivi, il target e il controller: il primo esegue le operazioni programmate tramite il secondo mediante la tecnica cosiddetta dell'inoculamento.
Quando il controllo a distanza avvenire a distanza avviene attraverso un *malware,* installato con la collaborazione attiva e inconsapevole della persona che utilizza il dispositivo controllato, le attività di polizia sfruttano tecniche di ingegneria sociale.

APPROFONDIMENTI

- Nocerino, *Il captatore informatico nelle indagini penali interne e transfrontaliere,* Padova, 2021.
- Orlandi, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Rivista italian di diritto processuale penale, 2,* 2018, 538 ss.
- Spangher, *I captatore informatico nella riforma delle intercettazioni*, in *Studium Iuris*, 4, 2021, 469 ss.
- Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017.

VOCI CORRELATE

CYBERCRIME
DIGITAL FORENSIC

INGEGNERIA SOCIALE
INVESTIGAZIONI DIGITALI
MALWARE

t

V

VULNERABILITÀ

Nel linguaggio della cybersicurezza, la vulnerabilità è una debolezza del sistema informatico (di un software o di un hardware) o della rete o persino di una procedura organizzativa.
La vulnerabilità è quindi un profilo, tecnico o umano, che rende un sistema meno sicuro e più esposto ai rischi. Di conseguenza, la vulnerabilità può essere sfruttata da chi ha intenzioni malevole per ottenere un accesso non autorizzato, sottrarre dati, interrompere servizi o causare altri danni.
Se un programma informatico contiene errori di programmazione che non sono stati corretti o il sistema operativo installato su un computer non è aggiornato regolarmente, si creano delle occasioni per coloro che intendono violare la sicurezza del sistema interessato. Inoltre, più la "struttura digitale" è grande e complessa, maggiori sono i rischi legati alla presenza di punti deboli, se ogni componente non viene progettato, configurato o aggiornato correttamente.
Le vulnerabilità possono infatti nascere in molti modi diversi. Spesso derivano da errori di programmazione o di progettazione; o da errate configurazioni (ad es. password o altre credenziali di accesso deboli); ma anche dal mancato aggiornamento di software e dispositivi.
Il fattore umano ha un ruolo decisivo per proteggere dispositivi, sistemi e reti riducendo o eliminando del tutto le vulnerabilità. Distrazioni come il click su un link sospetto o l'uso di una stessa password per più servizi possono determinare incidenti informatici anche di impatto significativo. Gli errori degli utenti, la scarsa attenzione alle regole di sicurezza e la mancanza di formazione sono infatti tra le principali cause di incidenti informatici.

APPROFONDIMENTI

- Camisa, Simoncini, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, 2024.
- Ricotta, *Vulnerability disclosure e penetration testing: questioni da normare,* in Fiorinelli, Giannelli (a cura di), *Il DDL*

Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2 –Instant Book, sezione monografica della *Rivista italiana di informatica e diritto,* 1, 2024, 55 ss.

- Ricotta, *Vulnerability disclosure e penetration testing: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2*, in Pietrangelo (a cura di), *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà*, sezione monografica della *Rivista italiana di informatica e diritto*, 2, 2024, 81 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERRESILIENZA
COMMON VULNERABILITIES AND EXPOSURES (CVE)
FATTORE UMANO

Z

ZERO-DAY

Una *zero-day* o *0-day* è una vulnerabilità della sicurezza informatica di un software, di un'applicazione o di altro sistema operativo non ancora conosciuta dallo sviluppatore o dal produttore. La denominazione deriva dal tempo a disposizione dello sviluppatore per risolvere la vulnerabilità attraverso la costruzione di un'apposita *patch* o aggiornamento specifico.
Con lo stesso termine si indica anche il software che un hacker utilizza per violare la sicurezza informatica del software o del prodotto prima che lo sviluppatore si renda conto della presenza della vulnerabilità. Questo software infatti è denominato *zero-day exploit*.
Gli *zero-day exploit* possono compromettere sistemi e infrastrutture critiche in in ambito civile e militare, tanto da essere annoverati tre le nuove armi cybernetiche. Nel 2010 uno *zero-day exploit* chiamato *stuxnet* è stato utilizzato per un attacco informatico a danno di una centrale nucleare in Iran proveniente da USA e Israele grazie ad alcune vulnerabilità zero-day dei sistemi informatici dell'impianto nucleare.

APPROFONDIMENTI

- Ablon, Bogart, *Zero Days, Thousands of Nights. The life and Times of Zero-Day Vulnerabilities and Their Exploit*, Santa Monica, 2017.
- Contini, *ABC della sicurezza: Zero Day*, in *Teche Economy*, 2015.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
INGEGNERIA SOCIALE
MALWARE
VULNERABILITÀ

ZERO TRUST

Lo *zero trust* è un modello strategico di sicurezza informatica. Esso è stato pensato in particolare per gli enti di grandi dimensioni, pubblici o privati, e presuppone che l'inaffidabilità assoluta dei sistemi informatici. Questo approccio, quindi, implica verifiche preventive interne all'organizzazione.
Non esiste un solo modello *zero trust* valido per tutti i tipi di enti (*one-size-fit-all*), e quindi non esiste una sola tecnica utilizzabile per la sicurezza informatica *zero trust*. Essa può riguardare i sistemi di autenticazione, la gestione delle identità e di eventuali accessi privilegiati o il modello di rete aziendale.
Questo modello per fasi comprende la protezione degli account privilegiati più potenti, il ricorso all'autenticazione multifattoriale per le risorse cosiddette *business-critical*; il rafforzamento della sicurezza sugli *endpoint* ecc.

APPROFONDIMENTI

- Corna, *Modello Zero Trust Security: cos'è, come funziona, perché adottarlo*, in *IT Specialist*, 11 gennaio 2021.
- Garbis, Chapman, *Zero Trust Security: An Enterprise Guide*, New York, 2021.
- Gunuganti, *Zero Trust Network Segmentation*, in *International Journal of Science and Research (IJSR)*, vol. 12, 4, 2023, 1936 ss.

VOCI CORRELATE

CYBERATTACCO (ATTACCO INFORMATICO)
CYBERRESILINZA
VULNERABILITÀ

Finito di stampare in Italia nel mese di settembre 2025

Cosa s’intende esattamente per cybersicurezza e soprattutto “cosa prevede la legge”? Quali sono i soggetti che se ne occupano? Quali sono i comportamenti virtuosi e quali quelli da evitare per essere sicuri online?
Questo volume prova a dare una prima risposta alle domande di chi abita lo spazio digitale, prime "istruzioni per l’uso” per documentarsi e approfondire gli aspetti giuridico-istituzionali della cybersicurezza e per districarsi più agevolmente in un complesso panorama normativo in continua evoluzione.

€ 15,00

9 788880 807124