MISSIONE 1 – IL PIANO NAZIONALE RIPRESA E RESILIENZA (PNRR) E LA CYBERSICUREZZA

PNRR

Dossier

Sommario

Capitolo I

Il Piano nazionale ripresa e resilienza (PNRR) e la Cybersicurezza

1.1 Sicurezza e la Missione 1 del PNRR

La sicurezza delle reti e dei sistemi informatici costituisce uno dei 7 investimenti previsti dal *Piano nazionale di ripresa e resilienza* (PNRR) nell'ambito delle azioni di *Digitalizzazione della pubblica amministrazione*.

La componente 1 della prima Missione 1 del PNRR (*Digitalizzazione, Innovazione e Sicurezza nella PA*)[1] si propone di sviluppare un'offerta integrata e armonizzata di servizi digitali all'avanguardia orientati a cittadini, residenti e imprese. Il raggiungimento di un tale risultato permetterebbe all'Italia di raggiungere gli ambiziosi traguardi fissati in sede europea dal *Digital Compass 2030*, il quale prevede che entro il 2030 tutti i servizi pubblici chiave siano disponibili *online*[2].

Nella prospettiva italiana del PNRR, per il comparto della pubblica amministrazione, lo snodo decisivo è rappresentato dal passaggio al digitale, con particolare riferimento allo sviluppo di servizi *on-line*[3]. In tale sguardo è possibile individuare le infrastrutture realizzate su cui poggia l'intervento programmato nella componente in analisi:

a) l'identità digitale[4];

b) i pagamenti digitali tra cittadini e Pubblica amministrazione[5];

[1] Alla quale sono destinati circa 9,72 miliardi di euro a cui si somma 1,40 miliardi del *Fondo complementare* di cui al D.L. 6 maggio 2021, n. 59, convertito con modificazioni dalla L. 1° luglio 2021, n. 101.

[2] La *missione 1, componente 1, del PNRR,* si pone in linea di coerenza con il contesto europeo, in cui i diritti e i principi digitali andranno ad integrare i diritti esistenti (come ad es. quelli sanciti dalla *Carta dei diritti fondamentali dell'UE* e dalla legislazione in materia di protezione dei dati e di *privacy*). In tale ambito si completeranno sia il quadro di riferimento per i cittadini sui loro diritti digitali, sia gli orientamenti per gli Stati membri dell'UE e per le imprese che si occupano di nuove tecnologie. Le persone e i loro diritti saranno al centro della trasformazione digitale, grazie ad un processo che:

- sostiene la solidarietà e l'inclusione;
- garantisce la libertà di scelta *online*;
- promuove la partecipazione allo spazio pubblico digitale;
- incrementa la sicurezza, la protezione e la responsabilizzazione delle persone;
- promuove, altresì, la sostenibilità del futuro digitale.

[3] Come quelli appena avviati dall'anagrafe nazionale della popolazione residente e nella migrazione su *cloud pubblico* che rappresenta uno degli investimenti più importanti nell'agenda del sistema paese

[4] Gli obiettivi fissati sono il superamento della soglia di 40 milioni di utilizzatori delle piattaforme esistenti per l'identificazione informatica (CIE e SPID) e la presenza di tutti i comuni nell'*Anagrafe della Popolazione residente* ANPR.

[5] Promuovendo l'adozione di PagoPA in oltre 14.000 amministrazioni locali.

c) le notifiche digitali[6].

Nel dettaglio, il rafforzamento dei servizi pubblici digitali si radica su una serie di interventi *abilitanti*, tra cui la migrazione al *cloud* delle pubbliche amministrazioni, la diffusione della *App "IO"* come punto di accesso preferenziale per il cittadino e il *rafforzamento della cybersecurity nazionale*.

Proprio per ovviare alla necessità di un rafforzamento del generale grado di sicurezza informatica a livello nazionale l'Investimento 1.5 della Missione 1, Componente 1.1, del PNRR (denominato *cybersecurity*) promuove l'implementazione e il potenziamento dei sistemi nazionali di *Cybersecurity*. Specificamente, il *Piano* segnala una serie di criticità che necessitano di un'attenta valutazione del rischio presente e futuro e, quindi, di una risposta adeguata da parte del Paese:

- la sempre maggiore diffusione della digitalizzazione in ogni campo del vivere civile incrementa, su tutti i fronti, il grado complessivo di vulnerabilità della società nei confronti di minacce di tipo cyber (ad es. frodi, ricatti informatici, attacchi terroristici, ecc.)[7].
- la crescente dipendenza da servizi *software* di terze parti comporta una sempre maggiore esposizione dei sistemi delle amministrazioni pubbliche alle *intenzioni* dei fornitori/sviluppatori/proprietari dei servizi stessi;
- l'aumento di interdipendenza tra le diverse PA, aziende controllate dallo Stato, privati)[8].

Il Piano, al fine di favorire una transizione digitale nazionale resiliente, prevede investimenti incentrati sulla capacità di *monitoraggio*, *prevenzione* e *risposta* più efficaci contro le minacce cyber[9] e sulla certificazione delle tecnologie *cyber*.

Gli investimenti sono organizzati su quattro aree di intervento principali:

[6] Tramite la creazione della nuova *Piattaforma unica di notifiche digitali* per comunicare efficacemente con cittadini e imprese, garantendo la validità legale degli atti.
[7] A tal proposito si evidenzia che la minaccia cibernetica cresce continuamente sia in quantità che in qualità. Tale tendenza è determinata anche dall'evoluzione delle tecniche di ingegneria sociale volte a ingannare gli utenti finali dei servizi digitali.
[8] Sotto tale profilo mette conto segnale come, nel corso del tempo si sia assistito ad un incremento notevole degli attacchi rivolti alle *supply chain*, ovvero alle catene dei fornitori di beni e servizi nell'indotto della PA.
9 Per identificare tempestivamente gli eventi informatici malevoli e mitigarne gli effetti dannosi, così da garantire la conservazione e la gestione, in tutta sicurezza, di dati e servizi della Pubblica Amministrazione.

- sono rafforzati i presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale;
- sono costruite o rese più solide le capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale;
- si investe nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche;
- sono irrobustiti gli *asset* e le *unità cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.

La realizzazione di tutto ciò si svolge in pieno raccordo con le iniziative Europee finalizzate ad assicurare la protezione degli interessi comuni dei cittadini e delle imprese.[10] Nell'orizzonte del 2024 tali interventi porteranno al dispiego integrale dei *Servizi nazionali di cybersecurity* nonché al completamento della rete dei laboratori a supporto del conseguimento dell'autonomia strategica nazionale nel settore e alla realizzazione di un piano operativo delle attività di monitoraggio tecnico-organizzativo[11].

Il *Piano Nazionale di Ripresa e Resilienza*, l'istituzione della nuova *Agenzia per la Cybersicurezza nazionale* e il decreto attuativo del *Perimetro di sicurezza nazionale cibernetica* pongono la cybersecurity a fondamento della digitalizzazione della Pubblica Amministrazione e del Sistema Italia. In tale contesto sono necessarie infrastrutture tecnologiche e piattaforme in grado di offrire a cittadini e imprese servizi digitali efficaci, sicuri e resilienti.

È necessario, quindi, per tutte le PA un cambio di approccio in cui la *cybersecurity* non può più essere vista come un costo o un mero adempimento normativo, bensì come un'opportunità per la crescita e la trasformazione digitale sia della Pubblica Amministrazione che dell'intero Paese. È questa la chiave di riflessione del PNRR legata alla cybersecurity. Punti focali di questa valutazione sono le tematiche relative al *Cyber Security Awareness*, in quanto da tale

[10] https://www.governo.it/sites/governo.it/files/PNRR.pdf
[11] Con almeno 50 interventi di potenziamento delle capacità cyber della PA a protezione dei dati e dei servizi dei cittadini.

consapevolezza possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche e alle evoluzioni degli attacchi informatici[12].

La sicurezza delle reti e dei sistemi informatici deve considerare anche lo sviluppo delle infrastrutture digitali – parte integrante della strategia di modernizzazione del settore pubblico – poiché queste sostengono l'erogazione sia di servizi pubblici a cittadini e imprese sia di servizi essenziali per il Paese. Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere, infatti, disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica amministrazione.

Conseguentemente nella M1C1 si pone l'esigenza di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi erogati dalle amministrazioni mediante la migrazione diretta a data center più sicuri e verso infrastrutture e servizi cloud qualificati, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità13.

Il quadro normativo vigente in merito alla *Strategia nazionale di Cybersicurezza* (in particolare all'art. 6 del D.lgs. 18 maggio 2018, n. 65[14]) affida al Presidente del Consiglio dei ministri adotta, sentito il *Comitato interministeriale per la cyber sicurezza*[15], la definizione della *Strategia nazionale per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale*. La trasformazione digitale della PA necessita, infatti, di importanti misure di rafforzamento delle difese cyber, a partire dalla piena attuazione della disciplina in materia di "*Perimetro di Sicurezza Nazionale Cibernetica*[16]".

Detto provvedimento in questione individua, nell'ambito della strategia nazionale di cybersicurezza, obiettivi e priorità in materia di sicurezza delle reti e dei sistemi informativi. In

[12] Nei tempi più recenti le minacce cibernetiche hanno conosciuto uno sviluppo esponenziale sia in quantità che qualità. Il contrasto delle minacce è diventata, quindi, un'esigenza fondamentale della PA, in quanto la protezione dei dati rappresenta il presupposto necessario per far crescere, sempre più, la fiducia di cittadini e imprese nei servizi digitali erogati dalla PA.
13 Le amministrazioni che devono attuare il processo di migrazione potranno avvalersi dei finanziamenti previsti dalla componente richiamata per un ammontare complessivo di 1,9 miliardi di euro, nello specifico con i due investimenti che mirano all'adozione dell'approccio Cloud first da parte della PA, ovvero "Investimento 1.1: Infrastrutture digitali" e "Investimento 1.2: Abilitazione e facilitazione migrazione al cloud"
[14] Come novellato dall'art. 15, comma 1 lett. f) del D.L. 14 giugno 2021, n. 82.
[15] Istituito dall'art. 4, D.L. n. 82/2021 presso la Presidenza del Consiglio dei ministri, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.
[16] Istituito dall'art. 1 del D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (cfr. *infra*).

tale sede sono, altresì, indicati il quadro di governance17 per il conseguimento degli obiettivi e delle priorità sulle quali impattano le misure del PNRR.

Vengono, inoltre, contemplati i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi, i piani di ricerca e sviluppo e un piano di valutazione dei rischi con l'elenco dei vari attori coinvolti nell'attuazione.

Nella prospettiva d'attuazione, **l'Agenzia per la Cybersicurezza Nazionale** (ACN), in stretto contatto con l'Amministrazione titolare, il Dipartimento per la Trasformazione Digitale (DTD), curerà l'attuazione dell'investimento connettendo il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. La trasformazione digitale della PA contiene anche importanti misure di rafforzamento delle difese cyber, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica".

In tale ambito è compito dell'Agenzia per la Cybersicurezza Nazionale curare l'evoluzione dell'infrastruttura e dei servizi per l'attuazione della strategia cyber nazionale che si articola su tre pilastri:

a) sviluppare le capacità di *cyber resilience* in modo diffuso nel Paese;

b) rafforzare le capacità nazionali di scrutinio e certificazione tecnologica;

c) potenziare le capacità cyber della Pubblica Amministrazione.

[17] Inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti e le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato.

Capitolo II

La Cybersicurezza nella normativa italiana: il DECRETO-LEGGE 14 giugno 2021, n. 82

2.1 L'architettura istituzionale

Con il D.L. 14 giugno 2021, n. 82, *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale* – convertito con modificazioni dalla L. 4 agosto 2021, n. 109 – il legislatore è intervenuto con un primo, significativo provvedimento di attuazione dei principi espressi dal PNRR in tema di *cybersicurezza*.

Tale normativa ha rimodellato l'architettura istituzionale di cybersicurezza, riorganizzando quadro normativo di riferimento, ruoli e responsabilità specifiche delineando, così, una nuova cornice di *governance* istituzionale, incardinata su di una nuova agenzia pubblica specializzata – denominata *Agenzia per la cybersicurezza nazionale* – vocata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica. Tale normativa ha rimodellato l'architettura istituzionale di cybersicurezza, riorganizzando quadro normativo di riferimento, ruoli e responsabilità specifiche delineando, così, una nuova cornice di governance istituzionale, incardinata su di una nuova agenzia pubblica specializzata – denominata Agenzia per la cybersicurezza nazionale – vocata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica.

La cruciale tematica della gestione della sicurezza cibernetica sul piano sistemico costituisce uno snodo fondamentale per gli interventi del *Piano Nazionale di Ripresa e Resilienza* (c.d. "PNRR"), trasmesso dal Governo alla Commissione europea il 30 aprile 2021, all'interno del primo intervento della missione 1 relativa alla *Digitalizzazione, innovazione, competitività, cultura e turismo*. Nel merito, le linee strategiche del Piano desiderano sostenere la transizione digitale del Paese per offrire a cittadini e imprese servizi efficaci, in sicurezza e pienamente accessibili. In particolare, relativamente agli aspetti di *cybersercurity* il PNRR si prende cura del rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale. Inoltre, il Piano pone lo sguardo sulla costruzione e il consolidamento delle capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi

critici da parte di soggetti che esercitano una funzione essenziale e sull'irrobustimento degli asset e delle unità cyber incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber. A tale intervento sono destinati investimenti per circa 620 milioni di euro, distribuiti nel quadriennio 2021-2024, con un impulso determinante nell'attuazione effettiva della nuova *governance* istituzionale e alle funzioni della Agenzia per la cybersicurezza nazionale. Alla luce di tale cornice introduttiva, i temi trattati nei paragrafi successivi analizzano le principali linee, tra loro interconnesse, sottese all'introduzione del D.L. 82/2021 in considerazione della necessità di ridefinire la *governance* istituzionale di cybersicurezza e la connessa necessità di riorganizzare il quadro normativo nazionale applicabile.

La ridefinizione dell'architettura istituzionale di cybersicurezza contenuta nelle norme si sostanzia in una serie di interventi finalizzati a riordinare i diversi ambiti di operatività della cybersicurezza nazionale (ambiti correlati, ma comunque distinti) e propedeutici, da un lato, **allo sviluppo di capacità di resilienza cibernetica nazionale** e, dall'altro lato, **allo svolgimento di attività di "*cyber-intelligence*"** (di competenza degli organismi di informazione per la sicurezza), di ***cyber-defense*** (intesa come difesa e sicurezza militare dello Stato, di competenza del Ministero della difesa) e alla ***prevenzione e repressione dei reati*** (di competenza delle Forze di polizia)[18]. Nel merito, il D.L. n. 82/2021 pone al centro delle politiche di implementazione e sviluppo dei sistemi di sicurezza informatica la Presidenza del Consigli dei Ministri e il ***Comitato interministeriale per la cybersicurezza***.

In particolare, l'art. 2 del D.L. n. 82/2021, attribuisce in via esclusiva alla competenza del Presidente del Consiglio dei ministri le seguenti funzioni in materia di *cybersicurezza*:

a) l'alta direzione e la responsabilità generale delle politiche di *cybersicurezza*;

b) l'adozione della strategia nazionale di *cybersicurezza*, sentito il *Comitato interministeriale per la cybersicurezza*;

c) la nomina e la revoca del direttore generale e del vicedirettore generale dell'*Agenzia per la cybersicurezza nazionale*, previa deliberazione del Consiglio dei ministri.

Ai fini dell'esercizio delle competenze relative all'alta direzione delle politiche di *cybersicurezza*, il Presidente del Consiglio dei ministri, sentito il Comitato, impartisce le

[18] Rivista Privacy& n. 3 ottobre 2021

relative direttive ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'*Agenzia per la cybersicurezza nazionale*.

Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può demandare le funzioni che lo stesso D.L. 82/2021 gli attribuisce in via non esclusiva all'*Autorità delegata* di cui all'art. 3, della L. 3 agosto 2007, n. 124[19]. In tal caso il Presidente del Consiglio dei ministri resta costantemente informato dall'*Autorità delegata* circa le modalità di esercizio delle funzioni delegate e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

L'Autorità delegata, in relazione alle funzioni delegate in materia di *cybersicurezza*, partecipa alle riunioni del *Comitato interministeriale per la transizione digitale*.

– Il Comitato interministeriale per la cybersicurezza

Presso la Presidenza del Consiglio dei ministri è istituito, ai sensi dell'art. 4 del D.L. n. 82/2021, il *Comitato interministeriale per la cybersicurezza* (CIC), con funzioni di *consulenza*, *proposta* e *vigilanza* in materia di politiche di *cybersicurezza*. Il CIC è presieduto dal *Presidente del Consiglio dei ministri* ed è composto dall'*Autorità delegata per la sicurezza della Repubblica*, dal *Ministro degli affari esteri e della cooperazione internazionale*, dal *Ministro dell'interno*, dal *Ministro della giustizia*, dal *Ministro della difesa*, dal *Ministro dell'economia e delle finanze*, dal *Ministro delle imprese e del made in Italy*, dal *Ministro dell'ambiente e della sicurezza energetica*, dal *Ministro dell'università e della ricerca* e dal *Ministro delle infrastrutture e dei trasporti*. Le funzioni di segretario del CIC sono svolte dal Direttore Generale dell'Agenzia.

Il Presidente del Consiglio dei ministri, inoltre, può invitare alle sedute del Comitato, anche a seguito di loro richiesta e senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

[19] Il primo comma del citato art. 3 della L. n. 124/2007, prevede che il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva soltanto ad un *Ministro senza portafoglio* o ad un *Sottosegretario di Stato*, denominati "*Autorità delegata*". L'*Autorità delegata* non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate, ad eccezione delle funzioni attribuite al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, con funzioni di Segretario del Consiglio medesimo.

In particolare, il Comitato:

a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di *cybersicurezza* nazionale;

b) esercita l'*alta sorveglianza* sull'attuazione della strategia nazionale di *cybersicurezza*;

c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla *cybersicurezza*, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della *cybersicurezza* e allo sviluppo industriale, tecnologico e scientifico in materia di *cybersicurezza*;

d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la *cybersicurezza* nazionale.

Il sesto comma dell'art. 4 chiarisce che il Comitato svolge altresì le funzioni già attribuite al *Comitato interministeriale per la sicurezza della Repubblica* (CISR), dal c.d. *decreto-legge perimetro*[20] e dai relativi provvedimenti attuativi (fatta eccezione per le determinazioni del Presidente del Consiglio dei ministri previste dall'art. 5 dello stesso decreto-legge perimetro in caso di crisi di natura cibernetica).

– L'Agenzia per la cybersicurezza nazionale

L'art. 5 del D.L. n. 82/2021 istituisce, a tutela degli interessi nazionali nel campo della *cybersicurezza*, l'*Agenzia per la cybersicurezza nazionale*, con sede in Roma.

L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti previsti dalla legge. Il Presidente del Consiglio dei ministri e l'Autorità delegata (ove istituita) si avvalgono dell'Agenzia per l'esercizio delle competenze indicate dal D.L. n. 82/2021.

Il direttore generale ha la rappresentanza legale dell'Agenzia. Egli è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata (ove istituita), ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia.

[20] L'art. 1, comma 1, lett. c) del D.L n. 82/2021 con la locuzione *decreto perimetro* indica il D.L. 21 settembre 2019, n. 105 (convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*), recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*.

Il direttore generale dell'Agenzia è scelto tra magistrati delle giurisdizioni superiori ordinaria ed amministrativa, avvocati dello Stato, dirigenti generali dello Stato ed equiparati, professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione.

Gli incarichi del direttore generale e del vicedirettore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni[21].

L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze armate, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali[22].

2.2 L'Organizzazione dell'Agenzia per la cybersicurezza nazionale

L'organizzazione, l'articolazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento adottato con decreto del Presidente del Consiglio dei ministri[23], entro centoventi giorni dalla data di entrata in vigore della legge di conversione del D.L. 82/2021[24].

Sono organi dell'Agenzia:

- il Direttore Generale;
- il Collegio dei revisori dei conti.

Con il regolamento sull'organizzazione e il funzionamento dell'agenzia sono disciplinati altresì:

a) le funzioni del Direttore generale e del Vice direttore generale dell'Agenzia;

b) la composizione e il funzionamento del Collegio dei revisori dei conti;

c) l'istituzione di eventuali sedi secondarie.

[21] Il direttore generale ed il vicedirettore generale, ove provenienti da pubbliche amministrazioni sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza.
[22] Inoltre, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124, il COPASIR, può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.
[23] Di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, del COPASIR, sentito il *Comitato interministeriale per la cybersicurezza* CIC.
[24] In particolare, l'Agenzia può essere articolata fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse finanziarie destinate all'Agenzia.

2.3 Le Funzioni dell'Agenzia per la cybersicurezza nazionale

L'Agenzia, ai sensi dell'art. 7del D.L. n. 82/2021:

a) è *Autorità nazionale per la cybersicurezza* e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni[25], il coordinamento tra i soggetti pubblici coinvolti in materia di *cybersicurezza* a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore;

b) predispone la strategia nazionale di *cybersicurezza*;

c) svolge ogni necessaria attività di supporto al funzionamento del *Nucleo per la cybersicurezza*;

d) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS[26], a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

e) è Autorità nazionale di certificazione della cybersicurezza e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al *Ministero dello sviluppo economico* dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni;

f) assume tutte le funzioni in materia di *cybersicurezza* già attribuite dalle disposizioni vigenti al *Ministero dello sviluppo economico*, ivi comprese quelle relative al perimetro di sicurezza nazionale cibernetica, alla sicurezza e all'integrità delle comunicazioni elettroniche e alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

[25] In particolare, restano ferme le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121 *Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*.
[26] L'art. 1, comma 1, lett. d) del D.L. n. 82/2021 per *decreto legislativo NIS* intende il D.Lgs. 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento (istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56);

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi;

i) assume tutte le funzioni già attribuite al *Dipartimento delle informazioni per la sicurezza* (DIS)

l) provvede, sulla base delle attività di competenza del *Nucleo per la cybersicurezza* alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro per le ipotesi di crisi di natura cibernetica;

m) assume tutte le funzioni in materia di *cybersicurezza* già attribuite all'*Agenzia per l'Italia digitale* dagli artt. 51 e 71[27] del CAD. L'Agenzia assume, altresì, i compiti di determinare, con proprio regolamento i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione e di definizione delle caratteristiche di qualità, sicurezza, *performance* e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione (di cui all'art. 33-*septies*, comma 4, del D.L. 18 ottobre 2012, n. 179, già attribuiti all'Agenzia per l'Italia digitale);

m-*bis*) assume le iniziative idonee a valorizzare la crittografia come strumento di *cybersicurezza*, anche attraverso un'apposita sezione dedicata nell'ambito della strategia nazionale di *cybersicurezza*. In particolare, l'Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali;

m-*ter*) provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi

[27] Con particolare riferimento al potere di adottare linee guida contenenti regole tecniche di *cybersicurezza* ai sensi dell'articolo 71 del CAD.

informatici. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della *cybersicurezza*, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la *cybersicurezza*;

q) coordina, in raccordo con il *Ministero degli affari esteri e della cooperazione internazionale*, la cooperazione internazionale nella materia della *cybersicurezza*[28];

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di *cybersicurezza* e, in particolare, con il *Ministero della difesa* per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della *cybersicurezza*, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di *cybersicurezza*, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di *cybersicurezza*, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della *cybersicurezza* e dei correlati servizi

[28] Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di *cybersicurezza*, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di *cybersicurezza* definite dal Presidente del Consiglio dei ministri;

applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di *cybersicurezza*, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della *cybersicurezza*, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni[29];

z) per il perseguimento delle proprie finalità istituzionali, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

aa) è designata quale *Centro nazionale di coordinamento* ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la *cybersicurezza* nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Presso l'Agenzia, anche ai fini dell'esercizio delle funzioni sub r), s), t), u), v), z) e aa), è istituito, con funzioni di consulenza e di proposta, un *Comitato tecnico-scientifico*, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri[30]. La composizione e l'organizzazione del Comitato

[29] In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile.
[30] Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento che disciplina l'organizzazione, l'articolazione e il funzionamento dell'Agenzia.

Il CSIRT (*Computer Security Incident Response Team*) italiano, che svolge i compiti e le funzioni del *Computer Emergency Response Team* (CERT) nazionale è trasferito presso l'Agenzia e assume la denominazione di: «*CSIRT Italia*».

È trasferito, altresì presso l'Agenzia anche il Centro di valutazione e certificazione nazionale.

Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia consulta detto Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

– Il Nucleo per la cybersicurezza

L'art. 8 del D.L. n. 82/2021 costituisce in via permanente, presso l'Agenzia, il *Nucleo per la cybersicurezza*, a supporto del Presidente del Consiglio dei ministri nella materia della *cybersicurezza*, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il Nucleo per la cybersicurezza è presieduto dal *Direttore Generale dell'Agenzia* o, per sua delega, dal *Vice Direttore Generale*, ed è composto *dal Consigliere militare del Presidente del Consiglio dei ministri*, da un rappresentante, rispettivamente, del *Dipartimento delle informazioni per la sicurezza* (DIS), dell'*Agenzia informazioni e sicurezza esterna* (AISE), dell'*Agenzia informazioni e sicurezza interna* (AISI), del *Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri* (PCM), del *Ministero degli esteri e della cooperazione internazionale* (MAECI), del *Ministero dell'interno*, del *Ministero della giustizia*, del *Ministero della difesa*, del *Ministero dell'economia e delle finanze* (MEF), del *Ministero delle imprese e del made in Italy* (MIMIT), del *Ministero dell'ambiente e della sicurezza energetica* (MASE), del *Ministero dell'università e della ricerca* (MUR), del *Ministero delle infrastrutture e dei trasporti* (MIT) e del *Dipartimento della protezione civile* della PCM. Per gli aspetti relativi alla trattazione di informazioni classificate[31] il Nucleo è integrato da un rappresentante dell'*Ufficio centrale per*

[31] Si tratta delle informazioni inserite nelle classifiche di segretezza di cui all'art. 42, della L. 3 agosto 2007, n. 124. In particolare, le classifiche di segretezza sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali. La classifica di segretezza è apposta, e può essere elevata, dall'autorità che forma il documento, l'atto o acquisisce per prima la notizia, ovvero è responsabile della cosa, o acquisisce dall'estero documenti, atti, notizie o cose. Le classifiche attribuibili sono: *segretissimo*, *segreto*, *riservatissimo*, *riservato*. Le classifiche sono attribuite sulla base dei criteri ordinariamente seguiti nelle relazioni internazionali.

la segretezza. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del *Ministero della salute* e del *Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile*.

2.3.1 Tavolo interministeriale Perimetro di Sicurezza Nazionale Cibernetica

Ai sensi dell'art. 10 del D.L. 82/2021, qualora nella gestione di situazioni di crisi che coinvolgono aspetti di *cybersicurezza*, il Presidente del Consiglio dei ministri convochi il CISR alle sedute di quest'ultimo sono chiamati a partecipare il (ministro) *delegato per l'innovazione tecnologica e la transizione digitale* e il *Direttore generale dell'Agenzia*. Il *Perimetro di Sicurezza Nazionale Cibernetica* è stato istituito dal D.L. n. 105 del 2019 al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Per assicurare il raccordo tra le amministrazioni impegnate, a vario titolo, nell'attuazione del *Perimetro di Sicurezza Nazionale Cibernetica* è istituito, presso l'Agenzia per la cybersicurezza nazionale e presieduto dal proprio Direttore Generale, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica* (articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131), cosiddetto Tavolo Perimetro, a supporto del CIC, specie in relazione all'individuazione delle funzioni e dei servizi essenziali dello Stato, nonché dei soggetti che li erogano da includere nel Perimetro.

2.4 Il Trattamento dei dati personali

L'art. 13 del D.L. n. 82/2021 precisa che il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione dello stesso D.L. n. 82/2021 è effettuato ai sensi dell'art. 58, commi 2 e 3, del D.Lgs. 30 giugno 2003, n. 196[32] *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.*

2.5 Le relazioni annuali

Entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri trasmette al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di *cybersicurezza* nazionale.

Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato.

2.6 L'applicazione del D.L. n. 82/2021

Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, l'Agenzia ***può provvedere***, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (di cui all'art. 7-*bis* del D.L. 27 luglio 2005, n. 144).

---

[32] Nello specifico le norme citate prevedono che:
[...]
2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base a disposizioni di legge o di regolamento o previste da atti amministrativi generali, che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonché quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.
3. Con uno o più regolamenti sono individuate le modalità di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.
[...]

Per lo svolgimento delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del c.d. *decreto-legge perimetro*, l'Agenzia ***provvede*** con l'ausilio dell'*Organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione* (di cui al citato art.7-bis del D.L. n. 144/2005). Il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del c.d. *decreto-legge perimetro*, riveste la qualifica di pubblico ufficiale.

Riveste, altresì la qualifica di pubblico ufficiale il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni. La trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale[33].

Con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, da adottare entro centottanta giorni dalla data di entrata in vigore della legge di conversione del D.L. 82/2021, sono definiti i termini e le modalità:

a) per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni del presente decreto;

b) mediante opportune intese con le amministrazioni interessate, nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento, per il trasferimento delle funzioni, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata, per l'attuazione delle disposizioni del presente decreto e la corrispondente riduzione di risorse finanziarie ed umane da parte delle amministrazioni cedenti.

[33] L'art. 331 c.p.c. disciplina la *Denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio*:
1. Salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito.
2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria.
3. Quando più persone sono obbligate alla denuncia per il medesimo fatto, esse possono anche redigere e sottoscrivere un unico atto.
4. Se, nel corso di un procedimento civile o amministrativo, emerge un fatto nel quale si può configurare un reato perseguibile di ufficio, l'autorità che procede redige e trasmette senza ritardo la denuncia al pubblico ministero.

In relazione al trasferimento delle funzioni precedentemente di pertinenza dell'AgID detti decreti definiscono, altresì, i raccordi tra le due amministrazioni, per le funzioni che restano di competenza dell'AgID.

L'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del Testo Unico approvato con R.D. 30 ottobre 1933, n. 1611.

Capitolo III

La Cybersicurezza e le minacce informatiche

3.1 La Cybersicurezza

La *cybersicurezza* può essere definita come *l'insieme di mezzi, tecnologie, attività e procedure teso a garantire la sicurezza informatica dei computer, server, dispositivi mobili, sistemi elettronici, reti informatiche (con particolare attenzione alla rete internet) in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici*. Essa, quindi, è riferita all'insieme di tecnologie, processi e procedure finalizzate alla protezione di reti, dispositivi, programmi e dati da attacchi, danni o accessi non autorizzati.

La necessità di garantire la sicurezza di reti e sistemi informatici emerge in tutta la sua urgenza ove si tenga conto del fatto che la pubblica amministrazione e le organizzazioni private raccolgono, elaborano e archiviano sui propri dispositivi una quantità sempre maggiore di dati, con precisione sempre più capillare e, a tal fine, utilizzano reti e altre infrastrutture (es. la *Piattaforma Digitale Nazionale Dati*) che permettono la trasmissione e la condivisione dei dati in proprio possesso con altri soggetti istituzionali (come nel caso della c.d. *cooperazione applicativa*).

Più in generale, a fronte della crescita esponenziale dell'importanza della rete in molteplici attività umane[34] corrisponde un analogo incremento della quantità e della qualità dei dati *on-line* molti dei quali sensibili o strettamente riservati (es. informazioni sanitarie o personali, dati genetici, dati biometrici, dati finanziari, ecc.).

L'accesso non autorizzato a tali dati, la loro esposizione senza il previo consenso, la loro alterazione o distruzione sono tutti eventi in grado di dare vita a conseguenze negative per il titolare dei dati stessi.

Purtroppo, l'esperienza comune ci insegna che la "crescita" della rete è stata accompagnata da un analogo incremento ed una continua evoluzione delle minacce in essa presenti[35]. È divenuta, dunque, sempre più impellente **la necessità di una tutela efficace contro le**

[34] La tendenza verso una sempre maggiore importanza della rete nella società odierna appare sostenuta da due impulsi fondamentali. Da un lato la crescita costante del numero di utenti e, dall'altro, l'incremento del numero dei dispositivi connessi (PC, *tablet*, *smartphone*, *smart* TV, ecc.). Quest'ultimo aspetto sembra destinato ad una crescita sempre maggiore grazie alle nuove frontiere della *domotica* e del c.d. *internet delle cose*.

[35] Le tecniche utilizzate per portare a segno attacchi *cyber* sono divenute, infatti, sempre più raffinate ed all'avanguardia, al punto da essere in grado, in molti casi, di superare o aggirare i sistemi e le procedure di sicurezza implementate proprio per contrastarle.

minacce e gli attacchi di *hacker* e malintenzionati in genere e, quindi, di un rafforzamento dei sistemi di sicurezza che coinvolga strumenti, procedure e professionalità adeguate.

I settori maggiormente colpiti dagli attacchi criminali sono: i servizi bancari, i servizi medici, i rivenditori e gli enti pubblici. Qualunque dispositivo proiettato sulla rete è, però, potenzialmente esposto a rischio di attacchi *cyber*.

3.2. Le diverse tipologie di attacchi informatici

Schematicamente possiamo indicare tre diversi tipi di comportamenti illegali:

1. **Cybercrimine**: attività sanzionate dall'ordinamento penale, poste in essere per mezzo (e spesso con l'abuso) delle tecnologie dell'informazione e della comunicazione[36] (sia *hardware* che software) orientate contro i beni informatici[37].
2. **Cyberattacchi**: azioni, manovre o tentativi posti in essere da individui singoli o organizzazioni verso sistemi informatici, infrastrutture, reti di calcolatori e/o dispositivi elettronici con la finalità di raccogliere, alterare o distruggere dati e informazioni[38];
3. **Cyberterrorismo**: attacchi illegali e minacce rivolti contro sistemi informativi di organizzazioni nazionali messi in atto per intimidire o costringere un governo o il suo popolo ad un dato comportamento o per ingenerare paura e disorientamento nella società e perseguire, così, obiettivi politici e/o sociali[39].

[36] Il *cybercrimine* è materia disciplinata dal diritto penale che nel corso del tempo ne ha delineato lo scenario – anche in funzione dell'evoluzione tecnologica e del consolidamento di tecniche criminali sempre più raffinate – sia individuando nuove figure criminose sia riconducendo i comportamenti in rete a figure criminose già esistenti (ad es. l'accesso abusivo ad un sistema informatico che è stato assimilato al reato di violazione di domicilio di cui all'art. 614 del Codice penale). Nello scenario attuale i crimini informatici più diffusi consistono in aggressioni mirate a sistemi aziendali o istituzionali, finalizzati al conseguimento di un vantaggio economico o a provocare l'interruzione di un dato servizio o un'attività aziendale.
[37] Pertanto, sono considerati reati informatici sia la frode o il furto di informazioni riservate realizzate grazie all'utilizzo di dispositivi digitali, sia il danneggiamento di sistemi informatici.
[38] Le motivazioni alla base degli attacchi informatici possono essere ricondotte essenzialmente a tre categorie principali: *politica*, *criminale* e *personale*. Gli attacchi a sfondo politico sono perpetrati da organizzazioni che intendono sfruttare l'evento per attirare l'attenzione sulle cause portate avanti e quindi, essenzialmente, per avere visibilità. Le aggressioni di tipo criminale sono, invece, finalizzate al conseguimento di facili guadagni finanziari grazie al furto di denaro, al furto di dati (incluso lo spionaggio industriale) o al danneggiamento o all'interruzione dell'attività di concorrenti commerciali. Le aggressioni animate da motivazioni personali sono riferibili a soggetti che hanno particolari legami con l'organizzazione colpita (es. dipendenti, ex dipendenti, utenti, ecc.) e possono avere motivazioni piuttosto varie che vanno dalla ricerca di profitti illeciti (furto di dati o di denaro), al mero risentimento (come nel caso di danneggiamenti fini a sé stessi).
[39] Gli atti di *cyberterrorismo* si caratterizzano per la loro attitudine a provocare violenza o a mettere in pericolo persone o beni, provocando danni sufficienti ad ingenerare sentimenti di paura (es. attacchi che determinano esplosioni, incidenti aerei, contaminazione delle condotte idriche acqua, gravi perdite economiche, ecc.).

3.2.1 I Malware

La minaccia informatica più comune e più diffusa in campo informatico è rappresentata dai *malware*[40]. Con tale termine si intende, genericamente, un programma o un codice dannoso che mette a rischio un sistema informatico danneggiandolo o provocandone il malfunzionamento, che si diffonde, normalmente attraverso la diffusione di allegati e-mail non richiesti o *download* in apparenza legittimi[41].

I *malware* non sono in grado arrecare danni fisici alle componenti *hardware* dei dispositivi ma, intervenendo sulla componente *software*, possono compromettere le funzioni fondamentali di un terminale (computer, tablet, *smartphone*, ecc.) o spiare le attività degli utenti o, infine, rubare, criptare o eliminare dati.

L'utilizzo dei *malware* è, quindi, finalizzato ad invadere, danneggiare o disattivare reti, sistemi, e terminali, assumendone parzialmente il controllo. Per questa via i criminali informatici mirano ad ottenere vantaggi (economici o di altro tipo) a danno degli utenti.

Le tipologie di *malware* più comuni sono:

- **Virus:** *software malevolo* in grado di replicarsi autonomamente e non rilevabile dall'utente, che infetta uno o più *file* residenti sul sistema attaccato, integrandosi nei codici eseguibili e/o nel sistema operativo del sistema informatico aggredito[42];
- **Worm**: *malware* simile ad un virus ma che non necessita di legarsi ad altri programmi eseguibili per diffondersi, in quanto utilizza le e-mail o le reti di computer. Solitamente i *worm* danneggiano o distruggono i file dei dispositivi aggrediti;
- **Trojan (**o cavallo di Troia**)** [43]**:** *malware* che assume l'apparenza di *software* legittimo, ma che consente accessi non autorizzati al computer della vittima. I *trojan* vengono utilizzati per rubare dati finanziari o per installare altre minacce e, più in generale per assumere il controllo remoto del terminale all'insaputa del legittimo proprietario[44];

[40] Il termine *malware* nasce dalla contrazione di "*malicious software*" (*software* malevolo).
[41] In particolare, i *malware* si attivano nel momento in cui l'utente apre un collegamento o un allegato apparentemente innocuo che, però, installa sul dispositivo uno o più *software* pericolosi.
[42] Si tratta di file di tipo eseguibile es. *.exe, *.bat in grado di integrarsi nei codici eseguibili (incluso il sistema operativo) del sistema informatico vittima, senza essere rilevati dall'utente. Un virus informatico è capace di replicarsi autonomamente, quando vengono eseguiti i programmi infettati e, così, diffondersi nell'intero sistema informatico.
[43] Il nome è ispirato all'Iliade e alla vicenda della guerra di Troia, in quanto il *trojan* si nasconde all'interno di un altro programma apparentemente utile e innocuo. Un *trojan* può contenere qualsiasi tipo di istruzione malevola. Spesso i *trojan* sono usati come veicolo alternativo ai *worm* e ai virus per installare delle *backdoor* o dei *keylogger* sui sistemi bersaglio.
[44] Un particolare tipo di utilizzo dei *trojan*, sempre più diffuso, è rappresentato dal c.d. *cryptomining dannoso* (o *drive-by mining* o *cryptojacking*). Attraverso l'installazione di un *trojan* i criminali informatici sono in grado di utilizzare le risorse del computer infettato per "*estrarre*" criptovalute (*mining*) ed inviare, poi, la valuta raccolta ai propri account.

- **Rootkit**: *malware* che fornisce agli *hacker* l'acceso a dispositivo bersaglio con i privilegi da amministratore. I *rootkit* operano in maniera da rimanere invisibili agli utenti, altri *software* e al sistema operativo stesso[45];
- **Spyware:** *software malevolo* che spia segretamente le attività e i comportamenti dell'utente, al fine di far acquisire ai criminali informatici informazioni utili da sfruttare a proprio vantaggio (es. dati delle carte di credito);
- **Keylogger:** *malware* o dispositivi *hardware* in grado interporsi tra la tastiera e il sistema operativo di computer o altri dispositivi (eventualmente come processo di *background*), in grado di registrare qualsiasi *input* proveniente dalla tastiera, memorizzare le informazioni raccolte e inviarle ai criminali informatici[46]. Di norma i *keylogger* di tipo *software* infettano i PC attraverso un *malware* più grandi, di cui fanno parte;
- **Ransomware:** *malware* che impedisce all'utente l'accesso al proprio dispositivo o ai dati criptando i file. Solitamente il *ransomware* è associato ad una richiesta di un riscatto per poter sbloccare i file criptati;
- **Adware:** *software* indesiderati utilizzati per presentare materiale pubblicitario (spesso all'interno del *browser*) che presentandosi come una componente legittima possono essere utilizzati per diffondere *malware;*
- **Botnet**: rete di dispositivi infettati da *malware* (detti *bot* o *zombie*) che i criminali informatici riescono a controllare tramite un unico dispositivo (detto *botmaster*). Il Botnet permette l'esecuzione di *task online* senza l'autorizzazione dell'utente ed aumenta esponenzialmente le capacità offensive di chi ha sferrato l'attacco. Attraverso i dispositivi infettati è possibile lanciare attacchi definiti *Distributed Denial of Service* (attacco DDoS)[47] contro altri sistemi.

3.2.2 Le altre minacce informatiche

Nel corso del tempo a fianco ai *malware* il crimine informatico ha elaborato anche modalità differenti per utilizzare illegalmente e a proprio vantaggio dati, informazioni e sistemi

[45] In alcuni casi i *rootkit* possono arrivare ad infettare anche il *firmware* dei dispositivi infettati.
[46] In tal modo i cybercriminali riescono ad ottenere informazioni sensibili come nomi utente, password, PIN delle carte di credito, ecc.
[47] Gli attacchi di tipo *Distributed Denial of Service* (*attacco distribuito di negazione del servizio*) determinano l'esaurimento delle risorse di un sistema informatico che fornisce un servizio *on line* attraverso una crescita esponenziale delle richieste (e, più in generale, del traffico dei dati in entrata) rivolte al sistema bersaglio da molte fonti diverse.

informatici o per interferire con servizi in rete o attività aziendali. Si tratta di condotte criminali abbastanza sofisticate che interferiscono con le modalità di funzionamento dei sistemi di elaborazione o di comunicazione, insinuandosi nei punti di eventuali debolezza dei sistemi stessi. Tra questi i più diffusi sono:

- **Immissione di codice SQL**: attacco informatico finalizzato al furto dei dati contenuti in un'applicazione *web* interfacciata con un *database* (tipico esempio sono le pagine *web* degli erogatori di servizi *on line* che richiedono un nome utente e una *password*), attraverso l'inserimento nel *database* stesso di un'istruzione SQL dannosa, che permette l'accesso alle informazioni sensibili contenute nel *database*;
- **Attacco *Man-in-the-Middle***: minaccia informatica in cui il criminale informatico, allo scopo di sottrarre dati. intercetta, ritrasmette o altera segretamente le comunicazioni fra due parti che credono di comunicare direttamente tra di loro;
- **Attacco *Denial of Service***: attacchi informatici che mirano ad impedire agli utenti l'accesso alla rete, ad un server *web*, FTP o di posta elettronica attraverso l'invio di molti pacchetti di richieste con la finalità di saturare le risorse e di un dato sistema[48];
- **Attacco MITM**: attacco in cui il criminale informatico si inserisce nel flusso di informazioni che si instaura tra un utente e una rete Wi-Fi pubblica non protetta. Di norma ciò avviene attraverso un *malware* che consente l'acquisizione fraudolenta di informazioni riservate.

3.3 I contenuti della *Cybersecurity*

Le *policy* di sicurezza informatica sono rivolte verso tutti i potenziali rischi provenienti da soggetti sia interni che esterni all'organizzazione ed operativamente agisce su due livelli principali:

- il livello di *sicurezza fisica ed ambientale* che attiene alle componenti *hardware* ed alle condizioni in cui dette componenti operano (ad es. la limitazione dell'accesso fisico nei locali in cui sono custoditi *server* ed altre componenti critiche);

[48] L'elevato numero di richieste rende il sistema *instabile* e non disponibile agli altri utenti. Il sovraccarico di reti e *server* impedisce, infatti, al servizio di soddisfare le richieste legittime;

- livello di *sicurezza logica* che attiene, invece, agli strumenti di tipo *software*.

In ragione dello specifico oggetto di protezione le attività di *cybersecurity* possono essere classificate in diverse categorie:

- **Sicurezza di rete**: insieme di strategie, procedure e tecnologie finalizzate a proteggere le reti informatiche dalle azioni dei criminali informatici (come attacchi mirati o *malware* opportunistici) finalizzate ad accedere a una rete, a modificarla o a violarla[49]. Estremamente importante, in quest'ambito, è la capacità di prevenire ed individuare eventuali intrusioni fornendo risposte adeguate;
- **Sicurezza delle applicazioni**: insieme di strategie, procedure e tecnologie per la protezione dei *software* e dei dispositivi da possibili minacce che potrebbero consentire a soggetti non autorizzati l'accesso i dati e informazioni meritevoli di protezione o permettere di apportare modifiche al codice dall'applicazione[50]. Per garantire la sicurezza delle applicazioni si utilizzano *hardware*, *software* e procedure specifici che mirano ad identificare e minimizzare i fattori di vulnerabilità
- **Sicurezza delle informazioni**: insieme di strategie, procedure e tecnologie per la protezione del patrimonio informativo di una organizzazione (tra cui rientrano anche i dati detenuti a titolo temporaneo) da accessi, divulgazioni, utilizzi, alterazioni, interruzioni o distruzioni non autorizzate, al fine di garantire integrità[51], riservatezza[52] e disponibilità[53]. La sicurezza delle informazioni copre un campo più ampio della cybersicurezza e si concentra principalmente sulla prevenzione di fughe, distorsioni e distruzione di informazioni;
- **Sicurezza operativa**: gestione e protezione degli asset di dati attraverso attente *policy* in tema di autorizzazioni utilizzate dagli utenti per accedere ad una rete e di procedure standardizzate per la memorizzazione o la condivisione dei dati;

[49] La sicurezza di rete si raggiunge integrando più linee di difesa in corrispondenza delle possibili criticità. In primo luogo è necessaria un'adeguata *policy* di controllo degli accessi alla rete che riguardi sia gli utenti autorizzati, sia i dispositivi collegati e i dati immessi. Un'altra linea di difesa di particolare importanza è rappresentata dalla capacità di filtrare, grazie ad appositi dispositivi *hardware* o *software*, denominati *firewall*, il traffico in entrata e in uscire dalla rete.
[50] Per poter massimizzare l'efficacia delle strategie di sicurezza delle applicazioni è necessario che la sua implementazione venga programmata già nella fase di progettazione dell'applicazione stessa.
[51] Dati ed informazioni devono essere protetti rispetto ad interventi ed alterazioni illeciti che ne compromettono validità, accuratezza o completezza.
[52] L'accesso alle informazioni deve essere consentito solo agli utenti autorizzati. A tal fine è necessario proteggerle da accessi non autorizzati da parte di soggetti interni ed esterni all'organizzazione.
[53] I soggetti autorizzati devono poter disporre dei dati nel momento stesso in cui ne hanno bisogno, secondo i requisiti di servizio stabiliti. Occorre, quindi, che le informazioni siano protette da eventi che possano comprometterne la disponibilità (guasti, interruzioni delle connessioni di rete, ecc.).

- ***Disaster recovery* e continuità operativa**: strategie che permettono di rispondere efficacemente a qualsiasi evento che determina una perdita in termini di operazioni o dati (inclusi gli incidenti di *cybersecurity*)[54];
- **Formazione degli utenti finali**: adeguamento della capacità e della propensione degli utenti al rispetto delle procedure di sicurezza per minimizzare il rischio di introdurre accidentalmente un *malware* o altre minacce in un sistema altrimenti sicuro (es. eliminare e-mail sospette, non inserire unità USB di cui non se ne conosce il grado di sicurezza, ecc.).

3.4. La *Cybersecurity* e le attività dinamiche connesse

Considerando in chiave approfondita il macro-tema della Cybersecurity appare necessaria una valutazione di carattere interdisciplinare. In prima istanza appare opportuno considerare **l'analisi euristica**. Nel merito si tratta di un metodo di rilevazione dei virus basato sull'esame del codice informatico per la ricerca di proprietà sospette, segmenti infetti o dubbi, anomalie e comandi pericolosi[55].

Tale modalità di analisi consente anche di intercettare facilmente le anomalie e permette di prevenire la comparsa di virus, ostacolando la proliferazione di nuove minacce in una novazione costante e progressiva[56]. Dal punto di vista pratico l'analisi euristica consente di poter aumentare il livello di sicurezza informatica raffinando gli strumenti di difesa contro ogni tipo di *cyber attacco*. Proprio per tali ragioni l'analisi euristica rappresenta una delle tecniche di base per lo sviluppo dei *software* antivirus[57] Queste caratteristiche sono interconnesse con l'economicità e il costante aggiornamento operato dagli sviluppatori, dai programmatori e dai produttori di antivirus.

Ulteriore elemento dinamico che afferisce al macro-ambito Cybersecurity è il *pattern recognition* che declina specialisticamente l'area dell'apprendimento automatico.

[54] La *disaster recovery* individua le procedure utili per ripristinare le operazioni e le informazioni di un'organizzazione e, conseguentemente, la capacità operativa disponibile prima dell'evento. La *continuità operativa* sta ad indicare la capacità di un'organizzazione di mantenere determinati standard nell'erogazione di prodotti e servizi successivamente al verificarsi di un incidente.
[55] I metodi tradizionali di rilevamento dei virus sono, per lo più, basati sul confronto del codice di un programma con quello di virus già noti e registrati in un *database* (il c.d. *rilevamento delle firme*). Tale metodologia, però, nel tempo si è rivelata, almeno in parte, non adeguata di fronte allo sviluppo delle nuove minacce. L'approccio euristico permette, invece, di superare i limiti in questione in quanto è in grado di offrire una difesa più efficace.
[56] L'analisi euristica, infatti, permette di combattere anche i virus c.d. *polimorfici*, ossia quelli il cui codice dannoso è in grado di cambiare e adattarsi costantemente.
[57] Diventa, quindi strategica la capacità di fornire una rapidissima identificazione di virus e programmi indesiderati e la connessa dinamicità di esecuzione. In tale ultima prospettiva, cruciale per la sicurezza informatica, tale forma di analisi assume centralità costruendo nel tempo una memoria strutturata inerente il comportamento dei *malware*. In questo modo si dà vita a numerosi database in cui sono presenti tutte le informazioni relative a intere famiglie di *malware*.

Specificamente, la *pattern recognition* è una tecnologia che consente alle macchine di rilevare disposizioni di caratteristiche o dati che forniscono alcune informazioni importanti su un dato sistema[58]. Si tratta, quindi, di una *dinamica di sicurezza informatica attiva* che si radica nel processo di osservazione ed elaborazione i dati, volto all'identificazione di eventuali regolarità all'interno dei dati stessi. I *pattern* da classificare sono tipicamente gruppi di misure che definiscono punti in uno spazio multidimensionale (al contrario del *pattern matching*, in cui il pattern è specificato in modo rigido). Da molti anni i motori di analisi euristica e di riconoscimento dei *pattern* d'azione dei sistemi operano con tali tecnologie per aumentare la protezione e fornire una difesa innovativa in grado di adattarsi alle tante minacce che animano il mondo del web e quello informatico in generaleIn una visione interdisciplinare la cybersicurezza si connette con l'**intelligenza artificiale** cioè con l'insieme di tecnologie che combinano dati, algoritmi e potenze di calcolo.

L'impatto dei sistemi di intelligenza artificiale può essere considerato non solo da una prospettiva individuale del cittadino, ma anche dal punto di vista della società nel suo complesso in relazione al suo impatto su pubbliche amministrazioni e imprese

3.5 La moderna gestione delle minacce

Come si è già avuto modo di sottolineare, i sistemi informativi delle moderne organizzazioni (pubbliche amministrazioni, aziende, ecc.) si caratterizzano per un elevato grado di complessità che se da un lato permette il trattamento di una ingente mole di dati e l'erogazione di servizi capillari ed articolati, dall'altro espone tali sistemi informativi a rischi specifici quali *malware* mutevoli[59], APT (*Advanced Persistent Threats* - Minacce avanzate persistenti[60]),

[58] Per comprendere tale concetto è necessario riflettere sull'analisi computazionale delle immagini e dei modelli più astratti. Nel dettaglio, la tecnologia di *computer vision* comporta l'acquisizione di immagini digitali utilizzando sensori di immagine, l'elaborazione e l'analisi delle foto per acquisire una certa comprensione dell'*input* visivo. La *visione artificiale* è un sottoinsieme dell'*intelligenza artificiale* ed è utilizzata per estrarre informazioni significative dalle immagini. La *computer vision* è un campo dell'apprendimento automatico e dell'intelligenza artificiale che si occupa di come i *computer* possono essere addestrati a ricavare informazioni significative da immagini o video digitali. Viene utilizzata in un'ampia gamma di aree applicative, come il riconoscimento facciale, il rilevamento dei difetti, la verifica dell'assemblaggio, il rilevamento degli intrusi e sicurezza dei *server*. Per l'interpretazione delle minacce potenziali e attuali ai sistemi informatici, la *computer vision* è strettamente correlata alla *pattern recognition*. Il riconoscimento dei modelli o riconoscimento degli schemi è un metodo di analisi dei dati che riconosce modelli e regolarità dei flussi informatici utilizzando algoritmi di apprendimento automatico. È uno studio su come le macchine possono classificare gli oggetti in una serie di categorie e classi similmente a come il cervello umano valuta il gli accadimenti esterni.

[60] La locuzione anglosassone *Advanced Persistent Threat* (in italiano *minaccia avanzata e persistente*) individua una minaccia informatica posta in essere da criminali informatici dotati di elevate competenze tecniche e grandi risorse umane e finanziarie e, quindi, in grado di realizzare attacchi su larga scala, non visibili, protratti per lunghi periodi di tempo. Le APT sono finalizzate ad ottenere informazioni riservate o a rendere inutilizzabili alcuni servizi dell'organizzazione attaccata per motivazioni generalmente politiche o economiche. Gli attacchi APT sono molto utilizzati anche per il cyberspionaggio.

minacce interne[61]. Ulteriori momenti di vulnerabilità possono essere legati all'utilizzo di soluzioni *cloud* per il trattamento dei dati e l'erogazione dei servizi e per l'impiego della forza lavoro (tutto o in parte) *remota*[62].

I più comuni sistemi di gestione delle minacce seguono un'architettura logica di supporto riferita a standard internazionali comuni[63] che individuano cinque funzioni fondamentali:

- ***Identificazione***: individuazione dettagliata degli asset e delle risorse più importanti dell'organizzazione quali la gestione delle risorse, la *mission* istituzionale, la *governance*, la valutazione dei rischi, la strategia di gestione dei rischi;
- ***Protezione***: messa in atto delle verifiche e dei controlli di sicurezza tecnica e fisica finalizzati allo sviluppo e all'implementazione di livelli di sicurezza efficace e alla protezione di infrastrutture critiche[64].;
- ***Rilevamento***: perfezionamento di misure in grado di segnalare all'organizzazione i possibili attacchi informatici. L'attività di rilevamento comprende: la segnalazione delle anomalie e degli eventi critici, il monitoraggio continuo della sicurezza e l'implementazione dei processi di rilevamento precoce;
- ***Risposta***: reazione appropriata agli attacchi informatici e ad altri eventi di sicurezza informatica. Questa fase comporta la pianificazione della risposta, la comunicazione, l'analisi, la mitigazione del danno e i miglioramenti del sistema di gestione delle minacce;
- ***Ripristino***: Implementazione dei piani per la resilienza informatica al fine di garantire la continuità operativa in caso di attacco informatico, violazione della sicurezza o altri eventi di sicurezza informatica.

[61] Le minacce interne sono rappresentate da un uso improprio dei dati di un'organizzazione (pubbliche amministrazioni, aziende, ecc.) per cause accidentali o dolose. Le minacce interne sono particolarmente pericolose per la sicurezza informatica di PA e imprese e possono rivelarsi più costose delle minacce esterne.
[62] Di norma i dispositivi utilizzati dai *lavoratori remoti* sono meno protetti rispetto alle reti interne di PA e imprese, e rappresentano, quindi, uno degli anelli deboli della catena di protezione dalle aggressioni esterne. Occorre, infatti, tener presente che rispetto a tali aggressioni la protezione offerta dai normali *software* antivirus risulta, per lo più, insufficiente.
[63] Nello specifico il riferimento è al *framework* di sicurezza informatica istituito dal *National Institute of Standards and Technology* (NIST) definito nella guida denominata *NIST Cybersecurity Framework* (NIST CF) ove, anche con il ricorso a standard e *best practice*, il NIST fornisce una guida completa per migliorare la sicurezza delle informazioni e la gestione dei rischi relativi alla sicurezza informatica per le organizzazioni del settore privato.
[64] Rientrano in quest'ambito la gestione delle identità, il controllo degli accessi, la formazione, la sicurezza dei dati, i processi e le procedure di sicurezza delle informazioni, la manutenzione e la tecnologia di protezione.

Capitolo IV

4.1 I reati informatici

La locuzione *reati informatici* indica in via generale tutti i crimini commessi grazie all'utilizzo di tecnologie e supporti informatici o telematici (sia *hardware* che *software*) o, più precisamente, gli atti criminosi in cui un sistema informatico è coinvolto come strumento di offesa (per sottrarre, compromettere o distruggere beni e/o informazioni riservate) o quale obiettivo ultimo dell'azione illegale[65]. Tale definizione discende direttamente dal primo comma dell'art. 640-*ter* del Codice Penale (di cui al Regio Decreto 19 ottobre 1930, n. 1398) che punisce *chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno [...].*

Sul punto la dottrina più accorta non ha mancato di sottolineare la necessità, ai fini di una migliore tassonomia, della distinzione tra *reati telematici veri e propri* ed i crimini cosiddetti tradizionali o convenzionali, in cui l'uso delle tecnologie dell'informazione e della comunicazione costituisce solamente uno strumento che supporta o agevola il raggiungimento dello scopo criminoso.

Dal punto di vista dei soggetti e del bene giuridico colpiti i cybercrimini possono essere suddivisi in tre diverse tipologie:

- *Cybercrimini contro la Proprietà* in cui un criminale si impossessa illegalmente dei dati bancari o della carta di credito di una persona (si tratta, quindi, di crimini analoghi a quelli che è possibile commettere nel mondo reale: truffe, *phishing*, ecc.);
- *Cybercrimini contro beni individuali della personalità* consistenti nella distribuzione *on line* di informazioni ingannevoli o illegali (es. *stalking* informatico, *revenge porn*, ecc.);

[65] I criminali informatici utilizzano i dispositivi informatici:
- per accedere ai dati riservati degli utenti dei servizi pubblici *on line* e della rete in generale;
- pe accedere alle informazioni di pubblica amministrazione e aziendali private;
- per bloccare un altro dispositivo.

Rientrano nel novero dei cybercrimini anche la vendita e l'acquisizione online di informazioni vietate.

– *Cybercrimini contro lo Stato o cyberterrorismo* che comporta l'accesso illegale a siti web della pubblica amministrazione o delle forze armate.

L'esigenza di una tutela giuridica, anche di tipo penalistico, in ambito alle tecnologie della comunicazione e dell'informazione (ICT) è emersa alla fine degli anni Ottanta del secolo scorso, quando è iniziata la migrazione sulle reti telematiche di molte attività di tipo economico, lavorativo, ricreativo, ecc. Nell'ordinamento italiano la disciplina di tali figure criminose ha trovato la sua prima definizione grazie alla L. 23 dicembre 1993, n. 547 recante *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*[66] grazie alla modifica e all'integrazione delle norme del codice penale e del codice di procedura penale. Successivamente, la L. 18 marzo 2008, n. 48 di *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* ha integrato e ulteriormente definito gli strumenti codicistici di lotta al cybercrimine.

4.2. I reati informatici nel codice penale e nell'elaborazione dottrinaria

Le fattispecie criminose riconducibili all'ambito telematico all'interno del *Codice penale* attengono, per lo più, a reati contro la persona, con particolare riferimento all'inviolabilità del domicilio e dei segreti, e a reati contro il patrimonio commessi mediante mezzi informatici. Non esiste, però, nel nostro codice penale una sezione specifica dedicata ai reati informatici. All'interno del codice i reati informatici sono, infatti, incardinati, per lo più, nel Titolo XII del Libro secondo, dedicato ai *delitti contro la persona*. Si tratta quindi, di un'ampia serie di fattispecie criminose. Nella tabella che segue sono riportate, senza pretesa di esaustività, le principali fattispecie di reati informatici (o, comunque, che è possibile compiere con l'ausilio di strumentazioni di tipo telematico) individuati dal codice penale.

[66] In questo caso, quindi, il legislatore è intervenuto con un certo grado di tempestività, rispetto all'emergere delle nuove esigenze in ambito telematico. Lo scarto di alcuni anni tra l'emergere di tali esigenze (fina anni '80) e l'emanazione della normativa (fine 1993) appare, infatti, riconducibile a problematiche di carattere tecnico-giuridico legate alla migliore conoscenza del nuovo fenomeno (che spesso assume i caratteri dell'interdisciplinarietà) e alla sua riconduzione all'interno di fattispecie giuridicamente definite. Il tempismo del legislatore testimonia, seppur indirettamente, l'importanza attribuita (sia dall'ordinamento italiano sia da quello eurounitario) al consolidamento in rete di un *clima di fiducia*, anche in vista del consolidamento di un *mercato elettronico comune*.

I principali reati informatici individuati dal codice penale

Art. 491 *bis*	Falsità nei documenti informatici
Art. 600 *ter*	Pornografia minorile
Art. 609 *undecies*	Adescamento di minorenni
Art. 612 *ter*	Diffusione illecita di immagini o video sessualmente espliciti (*revenge porn*)
Art. 615 *bis*	Interferenze illecite nella vita privata
Art. 615 *ter*	Accesso abusivo ad un sistema informatico o telematico
Art. 615 *quater*	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
Art. 615 *quinquies*	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
Art. 616	Violazione, sottrazione e soppressione di corrispondenza
Art. 617	Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche
Art. 617 *bis*	Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche
Art. 617 *ter*	Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche

Art. 617 *quater*	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
Art. 617 *quinquies*	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
Art. 617 *sexies*	Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
Art. 618	Rivelazione del contenuto di corrispondenza
Art. 619	Violazione, sottrazione e soppressione di corrispondenza commesse da persona addetta al servizio delle poste, dei telegrafi o dei telefoni
Art. 620	Rivelazione del contenuto di corrispondenza, commessa da persona addetta al servizio delle poste, dei telegrafi o dei telefoni
Art. 623 *bis*	Altre comunicazioni e conversazioni
Art. 635 *bis*	Danneggiamento di informazioni, dati e programmi informatici
Art. 635 *ter*	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
Art. 635 *quater*	Danneggiamento di sistemi informatici o telematici
Art. 635 *quinquies*	Danneggiamento di sistemi informatici o telematici di pubblica utilità
Art. 640 *ter*	Frode informatica
Art. 640 *quinquies*	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Tradizionalmente la dottrina giuridica, dal canto suo, è solita classificare i reati informatici disciplinati dal nostro ordinamento in quattro macrocategorie:

- *frodi informatiche* in cui i cybercriminali alterano un sistema informatico al fine di procurare a se stessi o ad altri un ingiusto profitto;
- *accesso abusivo ad un sistema informatico o telematico*;
- *detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici*;
- *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*.

In ogni caso quella contenuta nel codice penale è una serie piuttosto ampia e non particolarmente omogenea al suo interno in cui figurano reati contro la persona o contro la *privacy* a fianco di fattispecie criminose in grado di ledere l'integrità dello Stato. Nel prosieguo di questa breve trattazione, per evidenti ragioni di economia espositiva, verranno prese in considerazione solo le figure di reato direttamente o indirettamente in grado di ledere l'interesse all'integrità dei sistemi nazionali di erogazione dei servizi pubblici e, più in generale, di gestione della cosa pubblica.

4.3. Le singole fattispecie di reato

– L'accesso abusivo ad un sistema informatico o telematico

Ai sensi del primo comma dell'art. 615-*ter* del Codice Penale[67] *chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La norma, così formulata, sanziona l'accesso di tipo logico-informatico ad un sistema informatico o telematico[68], senza necessità di aggressione fisica al sistema cui si accede.

[67] Introdotto dall'art. 4, comma 1, della L. 23 dicembre 1993, n. 547.
[68] Per *sistema informatico o telematico* il legislatore intende un insieme di dispositivi *hardware* e *software* che consentono all'utilizzatore la fruizione di funzioni in grado di apportare un certo grado di utilità.

Pertanto, il bene giuridico oggetto di tutela è rappresentato dalla *riservatezza informatica*[69], mentre la condotta penalmente rilevante va individuata *nell'accesso informatico a distanza, attraverso reti telematiche*.

Altro elemento determinante al fine della concretizzazione del comportamento rilevante è rappresentato dal fatto che *l'accesso debba avere per oggetto un sistema informatico o telematico protetto da misure di sicurezza*. La presenza di detti sistemi di protezione testimonia, infatti della volontà contraria del soggetto di far accedere altri al proprio sistema.

Ai fini della configurabilità del reato previsto dall'art. 615-ter c.p. (accesso abusivo ad un sistema informatico o telematico), la protezione del sistema può essere adottata anche con misure di carattere organizzativo, che disciplinino le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo (Cassazione penale, Sez. V, sentenza 1 ottobre 2008, n. 37322)[70].

Al contrario, nel caso in cui l'agente si introduca in un sistema informatico o telematico non protetto, la condotta assume rilevanza penale *solo nel caso in cui la permanenza in detti sistemi (e, quindi, in una fase necessariamente successiva al mero accesso) si protragga contro la volontà espressa o tacita del titolare*[71]. In ogni caso l'accesso abusivo ad un sistema informatico o telematico è un reato di mera condotta e, quindi, si consuma con la semplice violazione del sistema informatico, a prescindere da una effettiva acquisizione dei dati.

Nell'ipotesi testé descritta il delitto è punibile a querela della persona offesa, mentre in quelle che seguono si procede d'ufficio.

A tal proposito la Sesta Sezione penale della Suprema Corte di Cassazione, con la Sentenza 14 dicembre 1999, n. 3067 ha precisato che *deve ritenersi «sistema informatico», secondo la ricorrente espressione utilizzata nella legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti computer's crimes, un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di «codificazione» e «decodificazione» - dalla «registrazione» o «memorizzazione», per mezzo di impulsi elettronici, su supporti adeguati, di «dati», cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente*.

[69] Ciò rimanda ad una nozione più ampia di *dimora* (intesa sia come spazio ideale sia quale spazio fisico in cui sono custoditi i dati informatici) che travalica i meri elementi materiali e si pone quale proiezione spaziale della persona. In un tale visione la libertà individuale non può che ricomprendere anche l'interesse alla tranquillità e sicurezza dei propri sistemi informatici.

[70] Ai fini della configurabilità del reato di *accesso abusivo ad un sistema informatico o telematico* non è, quindi necessario, che le *misure di sicurezza* siano costituite da *chiavi di accesso* o altre analoghe protezioni interne. Assume rilevanza, infatti, qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso (inclusi strumenti esterni al sistema e meramente organizzativi) in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi. (cfr. in tal senso Cassazione penale, Sez. V, Sentenza 6 dicembre 2000 n. 12732).

[71] Rientra in tale fattispecie anche l'ipotesi in cui colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema.

La particolare configurazione di tale delitto ha fatto sorgere la questione circa il luogo di consumazione del delitto stesso. Intervenuta sul punto la Cassazione penale, a Sezioni Unite, con la Sentenza 24 aprile 2015 n. 17325, ha chiarito che il luogo di consumazione del delitto di cui all'art. 615-ter cod. pen. coincide con quello in cui si trova l'utente che, tramite elaboratore elettronico o altro dispositivo per il trattamento automatico dei dati, digitando la "*parola chiave*" o altrimenti eseguendo la procedura di autenticazione, supera le misure di sicurezza apposte dal titolare per selezionare gli accessi e per tutelare la banca-dati memorizzata all'interno del sistema centrale ovvero vi si mantiene eccedendo i limiti dell'autorizzazione ricevuta.

I commi 2 e 3 individuano specifiche circostanze aggravanti, a cui sono (ovviamente) ricondotte maggiorazioni di pena. In particolare, il secondo comma dell'art. 615-*ter* prevede una pena maggiore, uno a cinque anni:

1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*

2) *se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;*

3) *se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.*

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico[72], la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni (comma 3).

[72] Sul punto la Quinta sezione penale della Corte di Cassazione, con la Sentenza 16 marzo 2021 n. 24576 ha precisato che ai fini della configurabilità dell'aggravante di cui all'art. 615-*ter*, comma terzo, cod. pen., sono "*di interesse pubblico*" solo i sistemi informatici o telematici di pubblica utilità, ossia destinati al servizio di una collettività indifferenziata e indeterminata di soggetti, e non anche quelli a vario titolo riconducibili all'esercizio di diritti, pur di rilevanza collettiva, costituzionalmente tutelati. (Nella specie la Suprema Corte ha escluso la sussistenza dell'aggravante nel caso di accesso abusivo al sito del fondatore di un movimento politico di livello nazionale utilizzato per la divulgazione delle idee del movimento stesso).

– Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

L'art. 615-*quater* del Codice Penale[73] prevede che *Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.*

Oggetti di sanzione da parte della norma è la detenzione o la messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela di sistemi informatici o telematici[74], ossia una *condotta prodromica alla commissione del delitto di accesso abusivo ad un sistema informatico o telematico* (di cui al precedente art. 615-*ter*)[75].

Per l'integrazione degli estremi del delitto di *detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici* è richiesto il *dolo specifico*[76] consistente nella finalità di un profitto ingiusto o, in alternativa, del danneggiamento (incluso il comportamento di chi rende possibile il danneggiamento da parte di altri) o comunque il non funzionamento (anche temporaneo) di un sistema informatico.

Ai sensi del secondo comma la pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se la detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici è compiuta:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.

[73] Introdotto dall'art. 4, comma 1, della L. 23 dicembre 1993, n. 547 e, successivamente, novellato dall'art. 19, comma 1, lett. a), b) e c) della L. 23 dicembre 2021, n. 238.
[74] La dottrina prevalente riconduce tra le condotte che integrano il delitto di cui all'art. 615-*quater* anche quella l'attivazione di un telefono cellulare clonato su un numero intesto ad altro soggetto o la clonazione dei decoder necessari per la ricezione via satellite o via cavo di programmi televisivi.
[75] Sul punto la giurisprudenza (Cassazione penale, Sez. II, Sentenza 20 maggio 2019, n. 21987) ha chiarito che il delitto di cui all'art. 615-*quater* cod. pen. non può concorrere con quello, più grave, di cui all'art. 615-*ter* cod. pen., del quale costituisce naturalisticamente un antecedente necessario, sempre che quest'ultimo, oltre ad essere procedibile, risulti integrato nel medesimo contesto spazio-temporale in cui sia stato perpetrato l'antefatto ed in danno della medesima persona offesa.
[76] Il dolo viene definito *specifico*, quando un fatto diventa punibile solo quando viene compiuto per un determinato fine o uno scopo specifico (il c.d. *movente*).

– Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329 (art. 615-*quinquies* del Codice Penale[77]).

Questa norma tutela la riservatezza informatica e la fruizione indisturbata del sistema informatico da parte del titolare. Anche in questo caso, come avviene per l'art. 615-*quater*, la norma sanziona una condotta prodromica alla commissione del delitto di *accesso abusivo ad un sistema informatico o telematico* consistente nella detenzione o nella messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela della *dimora* intesa nell'ampia accezione che ricomprende ogni proiezione spaziale della persona.

L'art. 615-*quinquies* c.p. ha introdotto nell'ordinamento una fattispecie di *reato di pericolo*. Affinché siano integrati gli estremi di reato non è, quindi, necessario che si verifichi concretamente l'evento lesivo (il danneggiamento o l'interruzione), ma è essendo sufficiente la mera elaborazione, detenzione, diffusione e installazione abusiva di apparecchiature o programmi astrattamente idonei ad esporre i sistemi al rischio di danneggiamento.

Anche in questo caso viene richiesto il dolo specifico costituito dallo scopo di danneggiare (o di permettere il danneggiamento) o impedire il funzionamento (anche temporaneo) di un sistema informatico.

[77] L'art. 615-*quinquies* c.p. è stato introdotto dall'art. 4, comma 1, della L. 23 dicembre 1993, n. 547 e, successivamente, modificato dall'art. 4, comma 1, della L. 18 marzo 2008, n. 48 e dall'art. 19, comma 2, lettera a), della L. 23 dicembre 2021, n. 238.

– Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Ai sensi dell'art. 617-*quater*, comma 1, del Codice Penale[78] *chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.*

Tale disposizione tutela l'inviolabilità delle comunicazioni a distanza tra due o più soggetti. Oggetto della condotta è l'apprensione, l'interruzione o l'impedimento fraudolento di comunicazioni relative ad un sistema informatico o tra sistemi telematici.

Salvo che il fatto costituisca più grave reato, il secondo comma dell'art. 617-*quater* prevede l'applicazione della stessa pena nei confronti di chi riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni carpite fraudolentemente[79].

Rispetto ai presupposti del reato di cui all'art. 617-*quater*, comma secondo, c.p. la Suprema Corte di Cassazione ha chiarito detta norma – nel sanzionare la condotta di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte il contenuto delle comunicazioni di cui al primo comma – non richiede quale presupposto del reato l'intercettazione fraudolenta delle comunicazioni (sanzionata dall'art. 617-quater, comma primo), in quanto la ratio della tutela penale è quella di evitare che siano divulgate con qualsiasi mezzo di informazione al pubblico comunicazioni cosiddette «chiuse» destinate a rimanere segrete, delle quali l'agente sia comunque venuto a conoscenza (Cassazione penale, Sez. V, sentenza 1 febbraio 2006, n. 4011).

I delitti di intercettazione, impedimento, interruzione e diffusione illecita di comunicazioni informatiche o telematiche sono punibili a querela della persona offesa (comma 3). Tuttavia, il quarto comma, prevede che si proceda d'ufficio se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

[78] Introdotto dall'art. 6, comma 1, della L. 23 dicembre 1993, n. 547 e modificato dall'art. 19, comma 5, lett. a) e b), della L. 23 dicembre 2021, n. 238.
[79] La dottrina prevalente individua nel secondo comma dell'art. 617-*quater* c.p. un'autonoma fattispecie di reato.

3) da chi esercita anche abusivamente la professione di investigatore privato.

Inoltre, in tali casi la pena è della reclusione da tre a otto anni.

– Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

L'art. 617-*quinquies* Codice Penale[80]punisce con la reclusione da uno a quattro anni *chiunque, fuori dei casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi.*

La norma si pone a presidio della libertà e della segretezza delle comunicazioni telematiche e, quindi, dell'inviolabilità delle comunicazioni a distanza tra due o più soggetti e, a tal fine, sanziona fatti prodromici alla commissione del delitto di *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (di cui all'art. 617-*quater* c.p.).

La condotta penalmente rilevante è rappresentata dalla detenzione, produzione, installazione, diffusione e consegna di apparecchiature idonee ad intercettare o impedire comunicazioni relative ad un sistema informatico o tra sistemi telematici. Ai fini della sussistenza del delitto è richiesto, inoltre, il dolo specifico consistente nella finalità di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle.

Il secondo comma prevede circostanze aggravanti specifiche elevando a cinque anni il massimo della pena qualora il fatto sia commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

[80] Introdotto dall' art. 6, comma 1 della L. 23 dicembre 1993, n. 547 e novellato dall'art. 19, comma 6, lett. a) e b) della L. 23 dicembre 2021, n. 238.

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

– Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

L'art. 617-*sexies* del Codice Penale[81] dispone che *chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.* Tale delitto è punibile a querela della persona offesa.

La norma tutela la veridicità e l'inviolabilità delle comunicazioni a distanza tra due o più soggetti. Infatti, la condotta penalmente rilevante è rappresentata dalla falsificazione del contenuto delle comunicazioni relative ad un sistema informatico o tra sistemi telematici, al fine di procurare un vantaggio o di arrecare ad altri un danno (dolo specifico).

L'art. 617-*sexies*, comma 1, c.p. istituisce un *reato proprio* che, in quanto tale, può essere commesso solamente da chi sia obbligato a formare o trasmettere ad altri il contenuto di comunicazioni altrui, avendo, per ragioni del suo ufficio o della sua professione, l'autorizzazione a captare tale forma di comunicazione.

Il secondo comma, il quale prevede una circostanza aggravante specifica, commina la pena è della reclusione da uno a cinque anni quando il fatto sia stato commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

[81] Introdotto dall'art. 6, comma 1, L. 23 dicembre 1993, n. 547 e modificato dall'art. 4, comma 1, del D.Lgs. 10 aprile 2018, n. 36.

3) da chi esercita anche abusivamente la professione di investigatore privato.

– Danneggiamento di informazioni, dati e programmi informatici

L'art. 635-*bis* del codice penale[82] dispone che, *salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*

La norma introduce una fattispecie di reato finalizzata a tutelare l'inviolabilità dei beni informatici altrui (dati e programmi informatici) e, quindi, in ultima analisi, il patrimonio del titolare di tali dati e/o programmi[83].

Dal punto di vista civilistico la condotta incriminata può essere ricondotta nell'ambito della responsabilità extracontrattuale ex art. art. 2043 c.c. (il c.d. *illecito aquiliano*). Gli elementi ulteriori, rispetto a questo schema (che ne delimitano l'ambito senza alterare i profili giuscivilistici), sono rappresentati dalla tipizzazione dell'oggetto del danno (un programma informatico e relativi dati) e l'elemento soggettivo, che richiede il dolo ma resta esclusa la colpa.

Il secondo comma prevede una pena maggiore della reclusione da uno a quattro anni se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore informatico.

[82] Introdotto dall'art. 9, comma 1, della L. 23 dicembre 1993, n. 547, modificato dall'art. 5, comma 1 della L. 18 marzo 2008, n. 48 e, successivamente, dall'art. 2, comma 1, lettera m), del D.Lgs. 15 gennaio 2016, n. 7.

[83] L'art. 635-*bis* estende esplicitamente a dati e programmi di natura informatica quanto previsto in linea generale dall'art. 635 il quale punisce con la reclusione da sei mesi a tre anni *chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui con violenza alla persona o con minaccia ovvero in occasione del delitto previsto dall'articolo 331, è punito con la reclusione da sei mesi a tre anni.* Il rapporto tra queste due norme è stato anche oggetto di indagine da parte della Giurisprudenza di legittimità. In particolare, la Cassazione penale, Sez. Unite, con la Sentenza 13 febbraio 1997, n. 1282 ha precisato che *Antecedentemente all'entrata in vigore della L. 23 dicembre 1993, n. 547 (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi dell'art. 635 c.p. in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore*. Inoltre, la S.C. ha ravvisato, tra le due norme, un rapporto di successione di leggi nel tempo, riferibile, quindi all'art. 2 c.p. che disciplina la successione nel tempo delle leggi penali.

– Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Ai sensi dell'art. 635-*ter* del codice penale[84], *salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

La norma tutela il patrimonio pubblico, in relazione ai dati e ai programmi informatici statali punendo anche condotte prodromiche all'evento lesivo (danneggiamento di dati o programmi informatici utilizzati da organi dello steso).

La dottrina prevalente individua nell'art. 635-*ter* c.p. un'autonoma ipotesi di reato, destituendo, quindi, di fondamento ricostruzioni che intravedono in tale norma un'ipotesi aggravata del delitto di danneggiamento di informazioni, dati e programmi informatici (di cui al precedente art. 635-*bis* c.p.). Quest'ultimo, infatti, costituisce una tipica figura di *delitto di attentato*, rispetto ai quali la condotta oltre ad essere diretta a cagionare l'evento lesivo, deve essere altresì idonea al raggiungimento dello scopo prefissato (anche sulla base della considerazione di condizioni storiche e sociali presenti al momento del fatto). La possibilità di sanzionare anche condotte prodromiche colloca, però l'art. 635-*bis* al di fuori di tale ricostruzione concettuale.

I commi 2 e 3 individuano, poi, le fattispecie aggravanti e segnatamente:

- *se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.*
- *se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.*

[84] Introdotto dall'art. 5, comma 2 della L. 18 marzo 2008, n. 48 in attuazione degli impegni assunti dallo Stato Italiano con la *Convenzione di Budapest del 2001* (nel senso di una rimodulazione della normativa interna in funzione di una lotta efficace alle nuove forme di manifestazione della criminalità informatica). La norma è stata, poi oggetto di una successiva modifica ad opera dell'art. 2, comma 1, lettera n), del D.Lgs. 15 gennaio 2016, n. 7.

– Danneggiamento di sistemi informatici o telematici

L'art. 635-*quater* del codice penale[85] punisce con la reclusione da uno a cinque anni, salvo che il fatto costituisca più grave reato, *chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni*[86].

La norma è posta a tutela del patrimonio, in relazione ai sistemi informatici altrui da condotte lesive di sistemi informatici o telematici altrui tramite la distruzione, la cancellazione, il deterioramento o alterazione di dati o programmi informatici, o mediante l'introduzione abusiva nel sistema informatico.

In particolare, le condotte sanzionate sono le stesse sanzionate dall'art. 635-*bis*[87] che vengono, però, punite più duramente quando da esse derivi la compromissione *irreversibile di un sistema informatico*, e non già di semplici dati o informazioni.

Anche in questo caso, come già sottolineato rispetto all'art. 635-*bis* la condotta incriminata descrive un fatto illecito da cui deriva, sul piano civilistico, una responsabilità di tipo extracontrattuale. Nel caso di specie, però, viene delimitato l'oggetto del contegno lesivo (un programma informatico e relativi dati) mentre rispetto all'elemento soggettivo viene dato rilievo solamente al dolo (e non anche alla colpa).

Il secondo comma prevede un incremento di pena per le ipotesi in cui il fatto sia commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore informatico, la pena è aumentata.

[85] Introdotto dall'art. 5, comma 2, della L. 18 marzo 2008, n. 48 e novellato dall'art. 2, comma 1, lettera o), del D.Lgs. 15 gennaio 2016, n. 7.
[86] Anche tale norma è stata introdotta in attuazione degli impegni assunti dallo Stato Italiano con la *Convenzione di Budapest* del 2001 per adeguare la normativa interna alle nuove forme di manifestazione della criminalità informatica.
[87] È, quindi, punito colui che *forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi*.

– Danneggiamento di sistemi informatici o telematici di pubblica utilità

Ai sensi dell'art. 635-*quinquies* del codice penale[88], se le azioni di danneggiamento di sistemi informatici o telematici (di cui al precedente art. 635-*quater*) sono dirette *a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.*

L'elemento di differenziazione di questa fattispecie rispetto a quella di cui all'art. 635-*quater* è rappresentato dalla funzione a cui sono destinati i sistemi informatici o telematici oggetto dell'azione criminosa, i quali devono essere strumentale allo svolgimento di funzioni di *pubblica utilità*. È, infatti, la pubblica utilità che fa acquisire ai beni informatici e telematici oggetto di aggressione una più spiccata sensibilità, in quanto destinati all'utilizzo o godimento collettivo. Inoltre, un'altra differenza significativa rispetto alla fattispecie descritta nell'articolo precedente è rappresentata dal fatto che l'art. 635-*quinquies* punisce anche condotte prodromiche al danneggiamento di un sistema informatico di pubblica utilità.

L'art. 635-*quinquies* individua un delitto di attentato, in cui la condotta oltre ad essere diretta a cagionare l'evento lesivo, deve essere altresì idonea al raggiungimento dello scopo prefissato (anche sulla base della considerazione di condizioni storiche e sociali presenti al momento del fatto).

Fattispecie aggravanti sono individuate dai commi 2 e 3, alla luce dei quali, rispettivamente:

- *se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.*
- *se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.*

[88] Introdotto dall'art. 5, comma 2, della L. 18 marzo 2008, n. 48 e modificato dall'art. 2, comma 1, lettera p), del D.Lgs. 15 gennaio 2016, n. 7. Anche l'art. 365-*quinquies* è stato introdotto in attuazione degli impegni assunti dallo Stato Italiano con la *Convenzione di Budapest* del 2001 per adeguare la normativa interna alle nuove forme di manifestazione della criminalità informatica.

– Frode informatica

L'art. 640-*ter* del codice penale[89] punisce con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032 *chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*.

L'art. 640-*ter* c.p. si pone a tutela del patrimonio individuale attraverso il regolare funzionamento dei sistemi informatici e la riservatezza dei dati in essi contenuti. La norma evidenzia la medesima struttura e quindi i medesimi elementi costitutivi del reato di truffa (di cui all'art. 640 c.p.) dal quale, però, si differenzia per due aspetti fondamentali:

- nel reato di truffa la condotta è orientata ad indurre in errore della vittima mentre nella frode informatica l'attività fraudolenta investe un sistema informatico;
- nella truffa la condotta penalmente rilevante consiste nel porre in essere artifizi o raggiri (con cui la vittima viene indotta in errore) nella frode informatica, invece, essa si consiste nella manipolazione o alterazione, comunque realizzata, di un sistema informatico o telematico, senza averne diritto.

Identico, invece, è il momento della consumazione del delitto che coincide con quello in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui.

Tali differenze pongono il delitto di frode informatica in rapporto di specialità con quello di truffa. Viene, quindi, esclusa la possibilità di concorso tra di esse. Nel caso in cui, la condotta si tale da realizzare contestualmente l'alterazione del sistema informatico e l'induzione in errore della persona, prevarrà il reato base di truffa[90].

Ai sensi del secondo comma la pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se il fatto è commesso:

- a danno dello Stato o di un altro ente pubblico o dell'Unione europea;
- col pretesto di far esonerare taluno dal servizio militare;

[89] Introdotto dall'art. 10, comma 1, della L. 23 dicembre 1993, n. 547 e modificato, a più riprese, dall'art. 9, comma 1, lett. a) e b) del D.L. 14 agosto 2013, n. 93 (convertito con modificazioni dalla L. 15 ottobre 2013, n. 119), dall'art. 9, comma 1 del D.Lgs. 10 aprile 2018, n. 36, dall'art. 2, comma 1, lettera c), del D.Lgs. 8 novembre 2021, n. 184 e dall'art. 2, comma 1, lettera p) del D.Lgs. 10 ottobre 2022, n. 150.

[90] Al contrario, secondo la giurisprudenza di merito (Cassazione penale, Sez. V, sentenza 27 gennaio 2004, n. 2672) *il delitto di accesso abusivo a un sistema informatico previsto dall'art. 615 ter c.p. può concorrere con quello di frode informatica di cui all'art. 640 ter c.p., in quanto si tratta di reati diversi: la frode informatica postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica.*

– con abuso della qualità di operatore del sistema.

La medesima pena, inoltre, trova applicazione se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale. A tal proposito, si segnala che l'art. 640-*quater* del codice penale, prevede l'applicazione, per quanto compatibili, delle disposizioni in tema di confisca di cui all'art. 322-*ter*[91], tra gli altri, alle ipotesi di cui all'art. 640-*ter*, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema.

Il successivo terzo comma dell'art. 640-*ter* c.p. prevede la reclusione da due a sei anni e della multa da euro 600 a euro 3.000 quando il fatto sia stato commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto di frode informatica è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o ricorre la circostanza aggravante dell'aver approfittato di circostanze di persona, anche in riferimento all'età (art. 640-*ter*, comma 4).

– Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Ai sensi dell'art. 640-*quinquies* del codice penale[92] *il soggetto che presta servizi di certificazione di firma elettronica (2), il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.*

---

[91] Art. 322-*ter* c.p. *Confisca*:
Nel caso di condanna, o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale, per uno dei delitti previsti dagli articoli da 314 a 320, anche se commessi dai soggetti indicati nell'articolo 322 bis, primo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto o il prezzo, salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto.
Nel caso di condanna, o di applicazione della pena a norma dell'articolo 444 del codice di procedura penale, per il delitto previsto dall'articolo 321, anche se commesso ai sensi dell'articolo 322 bis, secondo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a quello di detto profitto e, comunque, non inferiore a quello del denaro o delle altre utilità date o promesse al pubblico ufficiale o all'incaricato di pubblico servizio o agli altri soggetti indicati nell'articolo 322 bis, secondo comma.
Nei casi di cui ai commi primo e secondo, il giudice, con la sentenza di condanna, determina le somme di denaro o individua i beni assoggettati a confisca in quanto costituenti il profitto o il prezzo del reato ovvero in quanto di valore corrispondente al profitto o al prezzo del reato.
[92] Introdotto dall'art. 5, comma 3 della L. 18 marzo 2008, n. 48 di ratifica della *Convenzione di Budapest* sulla criminalità informatica.

La norma introduce una figura autonoma di truffa consistente nella violazione gli obblighi certificativi da parte del soggetto preposto al servizio di certificazione telematica che, al fine di procurare a sé o ad altri un ingiusto profitto con altrui danno.

La condotta sanzionata esprime il disvalore consistente nella violazione dolosa degli obblighi di certificazione da parte di un soggetto a cui la legge, per l'importanza della funzione, conferisce una particolare forma di fiducia. In altri termini, la fattispecie indicata dall'art. 640-*quinquies* c.p. individua un'ipotesi specifica di frode informatica che assume i caratteri tipici del *reato proprio* in quanto può essere posta in essere solamente dai certificatori di firma elettronica.