# LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – LEGGE 28 giugno 2024, n. 90 – Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.


PNRR

*Dossier*

# L'evoluzione del quadro normativo europeo e nazionale in materia di cybersicurezza: la DIRETTIVA NIS2, il d.lgs. 138/2024 e le nuove sfide per la protezione delle infrastrutture digitali

La trasformazione digitale e la crescente interconnessione delle infrastrutture informatiche, rese ancora più pervasive dalla progressiva digitalizzazione delle pubbliche amministrazioni e dei servizi essenziali, hanno determinato un aumento esponenziale delle minacce cibernetiche, rendendo imprescindibile l'elaborazione di un quadro normativo coerente e sistematico per la protezione delle reti, dei dati e delle infrastrutture critiche. La crescente esposizione a cyber minacce sempre più sofisticate, aggravata dall'emergere di attori ostili capaci di sfruttare tecnologie avanzate quali l'intelligenza artificiale generativa, ha indotto il legislatore europeo a rafforzare il precedente impianto normativo in materia di sicurezza informatica, già delineato con la Direttiva NIS del 2016. In tale prospettiva si colloca l'adozione della Direttiva (UE) 2022/2555, nota come Direttiva NIS2, il cui recepimento è avvenuto in Italia attraverso il D.Lgs. 138/2024, che integra e specifica le disposizioni della Legge 90/2024 in materia di cybersicurezza. La Direttiva NIS2 ha introdotto un approccio radicalmente innovativo rispetto al quadro normativo previgente, ampliando il numero di soggetti destinatari degli obblighi di sicurezza e rafforzando il regime sanzionatorio in caso di inadempienza. Il criterio della classificazione tra soggetti essenziali e importanti ha sostituito la distinzione precedente tra operatori di servizi essenziali e fornitori di servizi digitali, con l'intento di rafforzare la capacità di risposta alle minacce cibernetiche anche nei settori ad alta criticità. La disciplina introduce, altresì, una serie di obblighi stringenti per i soggetti rientranti nel perimetro applicativo della norma, prevedendo l'adozione di misure di gestione del rischio, l'implementazione di piani di risposta agli incidenti informatici e la predisposizione di un adeguato livello di resilienza operativa. In questo quadro normativo, il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) diviene sempre più centrale, configurandosi come l'ente preposto alla supervisione della sicurezza cibernetica a livello nazionale, con compiti di indirizzo strategico e di coordinamento delle misure di protezione nei confronti delle minacce informatiche. L'ACN, oltre a promuovere una cultura della

sicurezza informatica attraverso attività di sensibilizzazione e formazione, è chiamata a verificare l'attuazione degli obblighi previsti dalla normativa, esercitando poteri di vigilanza e sanzionatori nei confronti dei soggetti inadempienti. L'impianto normativo delineato dal D.Lgs. 138/2024 prevede inoltre un sistema di notifica obbligatoria degli incidenti informatici, imponendo ai soggetti essenziali e importanti di segnalare alle autorità competenti gli eventi di sicurezza che abbiano un impatto significativo sulla continuità operativa dei servizi erogati. Il regime di notifica prevede tempistiche rigorose, con un primo avviso da inviare entro 24 ore dall'evento e una relazione completa entro 72 ore, allineandosi ai principi già sanciti dal Regolamento Generale sulla Protezione dei Dati (GDPR) in materia di violazioni dei dati personali. La normativa contempla altresì l'obbligo di predisporre piani di continuità operativa e di testare periodicamente l'efficacia delle misure adottate attraverso simulazioni di attacchi informatici e penetration test. Un altro aspetto rilevante della Direttiva NIS2 e della normativa italiana di recepimento è rappresentato dall'attenzione alla sicurezza della catena di approvvigionamento, imponendo alle aziende e alle pubbliche amministrazioni di valutare i rischi derivanti dai fornitori di servizi IT e dalle infrastrutture critiche in outsourcing. In tale ottica, l'adozione di un modello di security by design diventa un principio cardine, richiedendo alle imprese di integrare i requisiti di cybersicurezza fin dalle fasi di sviluppo dei prodotti e dei servizi digitali. L'impatto della Direttiva NIS2 si estende anche alle responsabilità dell'alta direzione, imponendo agli organi direttivi delle aziende soggette alla normativa l'obbligo di supervisionare e approvare le politiche di gestione del rischio informatico, garantendo l'adozione di adeguate misure di prevenzione e protezione. L'inosservanza di tali obblighi comporta sanzioni pecuniarie estremamente severe, con multe che possono raggiungere i 10 milioni di euro o il 2% del fatturato annuo per i soggetti essenziali, e fino a 7 milioni di euro o l'1,4% del fatturato per i soggetti importanti. L'implementazione della normativa, tuttavia, solleva alcune problematiche di carattere interpretativo, specie in relazione all'ambito di applicazione della disciplina nei confronti dei gruppi internazionali e delle aziende multinazionali operanti in Italia. La questione della giurisdizione italiana nei confronti di entità con sede legale all'estero ma con infrastrutture operative in territorio nazionale rappresenta uno degli aspetti più critici dell'applicazione della Direttiva NIS2, richiedendo un coordinamento stretto tra le autorità nazionali ed europee. Un ulteriore elemento di complessità è rappresentato

dal bilanciamento tra spinta alla trasformazione digitale e gestione del rischio, in quanto l'adozione di tecnologie innovative deve necessariamente avvenire nel rispetto dei principi di sicurezza e affidabilità dei sistemi informatici. Un aspetto cruciale nella strategia di cybersecurity delineata dalla normativa è la gestione della vulnerabilità dei fornitori, in quanto il modello di supply chain security impone alle aziende di monitorare i rischi derivanti dalle relazioni con soggetti terzi, riducendo le possibilità di attacchi informatici condotti attraverso compromissioni indirette. La carenza di professionisti qualificati nel settore della cybersicurezza rappresenta, inoltre, una criticità significativa, in quanto la crescente domanda di esperti in cybersecurity e risk management non trova un'adeguata offerta di competenze specializzate nel mercato del lavoro. Il rafforzamento delle misure di sicurezza passa anche attraverso una maggiore cooperazione tra pubblico e privato, con la creazione di partnership strategiche finalizzate allo scambio di informazioni e alla condivisione di best practices. Un modello innovativo di difesa proattiva potrebbe essere rappresentato dall'adozione di un framework collaborativo, in cui le pubbliche amministrazioni e le aziende private cooperano nella gestione delle minacce informatiche attraverso piattaforme di threat intelligence e strumenti avanzati di monitoraggio della sicurezza cibernetica. La Direttiva NIS2, inoltre, sottolinea l'importanza della valutazione dell'autenticità dei dati, introducendo obblighi specifici per garantire l'integrità e la verificabilità delle informazioni digitali. L'adozione di tecnologie di crittografia avanzata e di meccanismi di verifica basati su blockchain potrebbe rappresentare una soluzione efficace per garantire l'affidabilità dei dati e contrastare fenomeni quali la falsificazione delle informazioni e la diffusione di contenuti manipolati. La regolamentazione della cybersicurezza non può prescindere da una armonizzazione con le altre normative europee, in particolare con il Regolamento DORA per la resilienza operativa digitale e con il Cyber Resilience Act, al fine di creare un ecosistema normativo integrato che favorisca la protezione delle infrastrutture critiche senza ostacolare l'innovazione tecnologica. In conclusione, la strategia di cybersicurezza delineata dalla Direttiva NIS2 e dalla normativa nazionale rappresenta un passo fondamentale per la costruzione di un ambiente digitale sicuro e resiliente, richiedendo un impegno congiunto da parte delle istituzioni, delle imprese e della società civile per affrontare le sfide emergenti e garantire un livello di protezione adeguato alle minacce del futuro.

## Analisi della Legge 90/2024 e delle Implicazioni Operative per la Cybersecurity

La sicurezza dei dati rappresenta un pilastro imprescindibile per la tutela dell'integrità delle infrastrutture digitali, sia a livello pubblico che privato. Nell'era della trasformazione digitale, le minacce cibernetiche si sono evolute in modo esponenziale, richiedendo un rafforzamento continuo delle misure di protezione e un adeguamento normativo costante. In tale contesto, la Legge 28 giugno 2024, n. 90, costituisce un punto di svolta nell'ordinamento italiano, introducendo nuove obbligazioni per i soggetti pubblici e privati al fine di incrementare la resilienza del Paese di fronte alle crescenti minacce informatiche. L'obiettivo primario della norma è consolidare l'apparato normativo esistente, armonizzandolo con le direttive europee, in particolare la Direttiva NIS2 (2022/2555/UE), e garantire una protezione adeguata dei dati sensibili, sia nel settore pubblico che in quello privato, con particolare riferimento alle infrastrutture critiche e ai servizi essenziali. La Legge 90/2024 introduce l'obbligo di notifica tempestiva degli incidenti informatici, definendo con precisione le responsabilità dei soggetti coinvolti e stabilendo un quadro sanzionatorio severo per chi ometta o ritardi la comunicazione di eventi che possano compromettere la sicurezza nazionale o la continuità dei servizi essenziali. Tale obbligo si estende non solo agli operatori dei settori critici, ma anche a tutti quei soggetti che trattano dati di rilevanza strategica, come le amministrazioni pubbliche, le aziende fornitrici di servizi digitali e le infrastrutture di telecomunicazione. L'introduzione di criteri stringenti per la governance dei dati impone l'adozione di sistemi di protezione conformi agli standard europei, con particolare attenzione alla gestione del rischio, alla protezione della catena di approvvigionamento e alla sicurezza dei dati personali e sensibili. La Legge 90/2024 prevede inoltre un rafforzamento del ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN), che assume un compito centrale nella supervisione dell'attuazione delle nuove disposizioni normative e nel coordinamento delle attività di prevenzione e risposta agli incidenti informatici. L'ACN si occuperà, tra le altre cose, della valutazione periodica della conformità degli operatori agli obblighi di sicurezza, dell'elaborazione

di linee guida vincolanti per la gestione dei rischi cibernetici e della promozione di iniziative di formazione e sensibilizzazione per incrementare la consapevolezza sui temi della cybersecurity. Un aspetto cruciale della norma è l'integrazione tra cybersicurezza e protezione dei dati personali, in linea con le disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR). In tal senso, la legge stabilisce che i soggetti pubblici e privati devono adottare misure di sicurezza avanzate per garantire l'autenticazione, l'integrità e la riservatezza dei dati trattati, prevedendo specifici obblighi in materia di autenticazione a più fattori, crittografia, monitoraggio degli accessi e tracciamento delle operazioni eseguite sui sistemi informativi. Una delle principali innovazioni apportate dalla Legge 90/2024 riguarda l'adozione di un modello di sicurezza by design e by default, che impone l'integrazione delle misure di sicurezza informatica fin dalla progettazione di qualsiasi infrastruttura digitale o servizio, anziché come elemento accessorio o successivo alla sua implementazione. Questo principio si riflette nell'obbligo di effettuare valutazioni d'impatto sulla sicurezza prima dell'introduzione di nuovi strumenti tecnologici o della modifica di sistemi esistenti. Inoltre, la norma introduce specifiche disposizioni in merito alla protezione dell'autenticità dei dati, ponendo l'accento sulla necessità di sviluppare meccanismi atti a contrastare la manipolazione delle informazioni e la diffusione di contenuti falsificati o alterati. Questo aspetto risulta particolarmente rilevante in considerazione della crescente minaccia rappresentata dai deepfake e dalle tecnologie di intelligenza artificiale generativa, che possono essere sfruttate per scopi malevoli. La normativa prevede altresì misure specifiche per il rafforzamento della sicurezza delle infrastrutture cloud impiegate dalla Pubblica Amministrazione e dai soggetti strategici, introducendo criteri di certificazione obbligatoria per i fornitori di servizi cloud e stabilendo che tali servizi debbano garantire standard elevati di sicurezza, resilienza e continuità operativa. Un ulteriore elemento chiave della Legge 90/2024 è la promozione della cooperazione internazionale in materia di cybersicurezza, favorendo la condivisione di informazioni tra le autorità nazionali ed europee e incentivando l'adozione di protocolli comuni per la gestione degli incidenti e la protezione delle infrastrutture digitali transfrontaliere. A tal fine, la norma prevede la partecipazione attiva dell'Italia ai programmi europei di cybersecurity e il rafforzamento delle relazioni con le organizzazioni internazionali operanti nel settore. La legge stabilisce inoltre un quadro sanzionatorio estremamente severo, con multe che possono

raggiungere dieci milioni di euro o il 2% del fatturato annuo globale per i soggetti essenziali che non rispettino gli obblighi di sicurezza previsti. Oltre alle sanzioni amministrative, sono previste misure interdittive nei confronti delle aziende che, con la loro condotta omissiva o negligente, espongano il Paese a gravi rischi di sicurezza. In tale contesto, un ruolo fondamentale è attribuito agli audit periodici e ai controlli ispettivi condotti dall'ACN e dalle Autorità di settore, i quali avranno il compito di verificare l'effettiva implementazione delle misure di sicurezza prescritte. Le disposizioni della Legge 90/2024 si inseriscono in un panorama giuridico in continua evoluzione, che include anche il Regolamento DORA (Digital Operational Resilience Act), destinato a rafforzare la resilienza operativa nel settore finanziario, il Cyber Resilience Act, volto a garantire la sicurezza dei prodotti digitali connessi, e la Direttiva CER, che introduce misure per il rafforzamento della resilienza delle entità critiche. L'integrazione armoniosa tra questi strumenti normativi rappresenta una sfida cruciale per il futuro della cybersicurezza, richiedendo un approccio coordinato e sinergico tra le istituzioni, le imprese e il settore accademico. In definitiva, la Legge 90/2024 segna un passo decisivo nel rafforzamento della sicurezza dei dati e delle infrastrutture digitali in Italia, ponendo le basi per una gestione più efficace dei rischi cibernetici e per una maggiore resilienza del sistema Paese. La sua attuazione rappresenta una sfida complessa che richiederà un impegno costante da parte di tutti gli attori coinvolti, ma costituisce al contempo un'opportunità unica per consolidare l'Italia come punto di riferimento nel panorama europeo della cybersicurezza.

## Articolo 1 della Legge 28 giugno 2024, n. 90

L'articolo 1 della Legge 28 giugno 2024, n. 90 introduce un quadro normativo stringente in materia di obblighi di segnalazione e notifica degli incidenti informatici, con l'obiettivo di rafforzare la cybersicurezza nazionale mediante l'imposizione di vincoli procedurali e tempistici a carico di soggetti ritenuti strategici per la continuità operativa e la resilienza delle infrastrutture digitali del Paese. In particolare, le disposizioni si applicano a un perimetro di enti pubblici e privati che include le pubbliche amministrazioni centrali individuate dalla Legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e Bolzano, le città metropolitane, i comuni

con popolazione superiore a 100.000 abitanti e, in ogni caso, i capoluoghi di regione, nonché le aziende sanitarie locali, le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e le società di trasporto pubblico extraurbano operanti nelle aree metropolitane. A tali soggetti si aggiungono le società in house che forniscono servizi informatici, i servizi di trasporto pubblico locale e le aziende responsabili della raccolta, smaltimento e trattamento delle acque reflue e dei rifiuti, la cui operatività si interseca con la tutela della sicurezza nazionale cibernetica. La norma stabilisce che tali enti siano obbligati a segnalare tempestivamente ogni incidente informatico rilevante, secondo le tipologie individuate dalla tassonomia definita dall'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, e a notificarlo formalmente all'Agenzia per la Cybersicurezza Nazionale attraverso le modalità stabilite. La prima segnalazione deve avvenire senza indugio e comunque entro ventiquattro ore dalla presa di conoscenza dell'incidente sulla base di evidenze tecniche acquisite, mentre la notifica completa, comprensiva di tutti gli elementi informativi disponibili, deve essere trasmessa entro le settantadue ore successive. Tali tempistiche rigorose rispondono all'esigenza di garantire una reazione tempestiva agli eventi critici, minimizzando l'impatto di eventuali attacchi informatici sulla sicurezza delle reti, dei sistemi informativi e dei servizi digitali essenziali per il funzionamento delle infrastrutture strategiche. L'articolo prevede, inoltre, un regime di applicazione differenziato per alcuni enti, stabilendo un periodo di adeguamento di centottanta giorni per i comuni con oltre 100.000 abitanti, le aziende sanitarie locali e le società di trasporto pubblico urbano ed extraurbano. Parallelamente, la disciplina contempla la possibilità per i soggetti obbligati di effettuare notifiche volontarie relative a incidenti non rientranti nelle categorie previste dalla tassonomia, alle quali si applicano le disposizioni dell'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65. Al fine di garantire il rispetto degli obblighi di notifica, la norma introduce un sistema sanzionatorio progressivo: in caso di mancato adempimento, l'Agenzia per la Cybersicurezza Nazionale emette una comunicazione formale di avviso, segnalando che l'eventuale reiterazione della violazione nell'arco di cinque anni comporterà l'applicazione di una sanzione amministrativa pecuniaria variabile da 25.000 a 125.000 euro. Inoltre, l'inosservanza reiterata può determinare l'attivazione di ispezioni nei dodici mesi successivi alla rilevazione del ritardo o dell'omissione, al fine di verificare l'adozione di misure di rafforzamento della resilienza in conformità alle

linee guida emanate dall'Agenzia. La violazione di tali obblighi può altresì configurare una responsabilità disciplinare e amministrativo-contabile per i funzionari e dirigenti preposti alla sicurezza informatica, con possibili conseguenze sul piano della responsabilità patrimoniale. Tuttavia, le disposizioni dell'articolo 1 non si applicano a determinate categorie di enti, tra cui gli organi dello Stato deputati alla prevenzione, all'accertamento e alla repressione dei reati, le forze di polizia, gli organismi di intelligence e sicurezza, nonché i soggetti già sottoposti a regimi normativi specifici ai sensi del decreto-legge 21 settembre 2019, n. 105 e del decreto legislativo 18 maggio 2018, n. 65. La previsione di tali esclusioni risponde all'esigenza di preservare il carattere riservato e strategico delle attività svolte da tali enti nell'ambito della difesa e della sicurezza nazionale. In ultima analisi, l'articolo 1 della Legge 28 giugno 2024, n. 90 si inserisce in un quadro più ampio di rafforzamento della cybersicurezza nazionale, integrandosi con le misure di resilienza definite nelle linee guida adottate dall'Agenzia per la Cybersicurezza Nazionale, le quali delineano le best practice per l'identificazione e la gestione del rischio informatico, il rafforzamento dei processi di risposta agli incidenti e la promozione di una cultura della sicurezza cibernetica all'interno delle organizzazioni pubbliche e private coinvolte.

## Articolo 2 della Legge 28 giugno 2024, n. 90

L'articolo 2 della Legge 28 giugno 2024, n. 90 stabilisce un preciso obbligo di adeguamento a segnalazioni puntuali dell'Agenzia per la Cybersicurezza Nazionale (ACN) in materia di vulnerabilità informatiche, imponendo tempistiche stringenti per l'attuazione degli interventi correttivi e prevedendo un regime sanzionatorio in caso di mancata o tardiva conformità. L'ambito soggettivo di applicazione della norma si estende ai soggetti già individuati all'articolo 1, comma 1, della presente legge, nonché agli enti di cui all'articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133, e ai soggetti indicati nell'articolo 3, comma 1, lettere g) e i), del decreto legislativo 18 maggio 2018, n. 65, nonché all'articolo 40, comma 3, del Codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259. In virtù di tale previsione normativa, qualora l'ACN rilevi specifiche vulnerabilità cui tali soggetti risultino potenzialmente esposti e comunichi

interventi risolutivi, essi sono tenuti ad adottarli senza indugio e, in ogni caso, entro il termine massimo di quindici giorni dalla ricezione della segnalazione. La ratio della disposizione è quella di garantire una reazione tempestiva alle minacce cibernetiche, prevenendo il rischio che vulnerabilità note e correggibili possano essere sfruttate per condurre attacchi informatici con conseguenze potenzialmente rilevanti per la sicurezza nazionale, la continuità operativa delle infrastrutture strategiche e la protezione dei dati sensibili. In caso di mancato o ritardato adeguamento, si applicano le sanzioni previste dall'articolo 1, comma 6, della medesima legge, le quali comprendono l'irrogazione di sanzioni amministrative pecuniarie comprese tra i 25.000 e i 125.000 euro e possibili responsabilità disciplinari e amministrativo-contabili a carico dei funzionari e dirigenti preposti. Tuttavia, la norma introduce una clausola di salvaguardia per le ipotesi in cui l'adozione degli interventi indicati dall'ACN risulti impraticabile per ragioni di natura tecnico-organizzativa. In tali circostanze, il soggetto destinatario della segnalazione può motivare e comunicare tempestivamente all'ACN l'impossibilità di attuazione nei termini stabiliti o la necessità di un differimento del termine, evitando così l'applicazione delle sanzioni previste. La disposizione si inserisce in un più ampio quadro normativo volto a rafforzare la resilienza cibernetica del Paese, garantendo che i soggetti critici per la sicurezza nazionale operino in un regime di stretta compliance alle direttive dell'ACN, promuovendo al contempo un approccio proattivo nella gestione delle vulnerabilità e nel rafforzamento delle difese informatiche. La previsione dell'obbligo di comunicazione degli impedimenti tecnico-organizzativi risponde altresì all'esigenza di garantire un flusso informativo costante tra i soggetti regolati e l'ACN, permettendo a quest'ultima di monitorare l'effettivo stato di implementazione delle misure di sicurezza e di intervenire con strategie correttive mirate qualora emergano criticità strutturali nell'adeguamento alle segnalazioni.

### Articolo 3 della Legge 28 giugno 2024, n. 90

L'articolo 3 della Legge 28 giugno 2024, n. 90 introduce modifiche sostanziali all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133, al fine di rafforzare il sistema di notificazione degli

incidenti informatici e garantire una maggiore efficienza nel coordinamento delle misure di cybersicurezza a livello nazionale. La norma interviene con due principali modificazioni. In primo luogo, viene ridefinita la tempistica entro cui i soggetti obbligati devono segnalare e notificare gli incidenti informatici, uniformandola ai criteri già stabiliti dall'articolo 1 della Legge n. 90/2024. Nello specifico, il termine per la segnalazione preliminare viene fissato a ventiquattro ore dal momento in cui il soggetto interessato ha acquisito conoscenza dell'incidente, mentre il termine per la notifica completa viene stabilito in settandue ore, a decorrere dal medesimo momento. Questa disposizione mira a garantire una maggiore tempestività nella trasmissione delle informazioni critiche all'Agenzia per la Cybersicurezza Nazionale (ACN), consentendo un monitoraggio più efficace delle minacce e un intervento coordinato per la gestione degli incidenti su scala nazionale. In secondo luogo, l'articolo introduce una sanzione amministrativa pecuniaria per i casi di reiterata inosservanza dell'obbligo di notifica. In presenza di ripetute violazioni degli obblighi previsti dal comma 3-bis del decreto-legge n. 105/2019, i soggetti inadempienti saranno soggetti a una sanzione amministrativa compresa tra 25.000 e 125.000 euro, in linea con il regime sanzionatorio già delineato dall'articolo 1, comma 6, della Legge n. 90/2024. La previsione di una sanzione economica ha lo scopo di rafforzare la compliance alle disposizioni in materia di sicurezza informatica, scoraggiando eventuali condotte omissive o dilatorie e responsabilizzando ulteriormente i soggetti pubblici e privati coinvolti nella gestione di infrastrutture digitali critiche. L'intervento normativo si configura dunque come un adeguamento necessario per garantire una coerenza sistematica tra la disciplina preesistente e le nuove prescrizioni introdotte dalla Legge n. 90/2024, consolidando il quadro regolamentare in materia di gestione degli incidenti informatici e rafforzando l'efficacia del perimetro di sicurezza nazionale cibernetica delineato dal decreto-legge n. 105/2019. La norma, inoltre, si inserisce in un più ampio contesto di potenziamento del ruolo dell'ACN come autorità centrale per la supervisione e il coordinamento della risposta agli incidenti informatici, sottolineando l'importanza della tempestiva comunicazione degli eventi critici come strumento di prevenzione e mitigazione delle minacce cibernetiche.

## Articolo 4 della Legge 28 giugno 2024, n. 90

L'articolo 4 della Legge 28 giugno 2024, n. 90 apporta un'importante modifica al decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, ampliando le funzioni attribuite all'Agenzia per la Cybersicurezza Nazionale (ACN) in materia di raccolta e gestione dei dati relativi agli incidenti informatici. La norma introduce la lettera n-ter) all'articolo 7, comma 1, del citato decreto, assegnando all'Agenzia il compito di raccogliere, elaborare e classificare i dati delle notifiche di incidenti ricevute dai soggetti obbligati ai sensi delle disposizioni vigenti. Tale previsione rafforza il ruolo dell'ACN quale autorità centrale deputata alla gestione delle informazioni strategiche in materia di cybersicurezza, consolidando un approccio basato sulla centralizzazione e sistematizzazione dei dati relativi alle minacce e agli attacchi cibernetici. In particolare, i dati acquisiti nell'ambito di questa attività saranno resi pubblici all'interno della relazione periodica prevista dall'articolo 14, comma 1, del decreto-legge n. 82/2021, diventando dati ufficiali di riferimento sugli attacchi informatici ai soggetti operanti nei settori di rilevanza strategica per la sicurezza nazionale. Questa misura risponde a un'esigenza di trasparenza e accountability, garantendo che le informazioni sugli incidenti informatici siano accessibili in un formato ufficiale e verificabile, contribuendo così alla sensibilizzazione del settore pubblico e privato sulle minacce cyber e alle strategie di mitigazione. Inoltre, l'aggregazione e la pubblicazione dei dati forniranno un quadro statistico e analitico utile per il miglioramento delle politiche nazionali in materia di resilienza cibernetica e gestione del rischio informatico. La disposizione stabilisce, altresì, che gli adempimenti connessi all'attuazione di questa nuova funzione debbano avvenire senza nuovi o maggiori oneri per la finanza pubblica, facendo ricorso esclusivamente alle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Questa scelta normativa mira a garantire un equilibrio tra l'ampliamento delle competenze dell'ACN e la sostenibilità finanziaria, evitando l'introduzione di nuovi costi per il bilancio statale. In definitiva, l'articolo 4 si colloca nel più ampio processo di rafforzamento della cybersicurezza nazionale delineato dalla Legge n. 90/2024, promuovendo un modello di governance basato su raccolta centralizzata dei dati, analisi sistematica delle minacce e diffusione di informazioni qualificate, in linea con

le best practice internazionali in materia di sicurezza cibernetica e gestione delle crisi informatiche.

## Articolo 5 della Legge 28 giugno 2024, n. 90

L'articolo 5 della Legge 28 giugno 2024, n. 90 introduce una modifica all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109, che disciplina la composizione e le funzioni del Nucleo per la Cybersicurezza, organismo istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN) con il compito di supportare il Presidente del Consiglio dei ministri nelle attività di prevenzione, preparazione e gestione di eventuali situazioni di crisi nel settore della cybersicurezza. La modifica consiste nell'introduzione del comma 4.1, il quale amplia la composizione del Nucleo per consentire la partecipazione di ulteriori soggetti in relazione a specifiche questioni di particolare rilevanza, connesse ai compiti di cui all'articolo 9, comma 1, lettera a) del medesimo decreto. In particolare, la norma prevede che il Nucleo possa essere convocato nella sua composizione ristretta, prevista dal comma 4 dell'articolo 8, ma con la possibilità di includere nuovi attori istituzionali e privati, in funzione della tematica trattata. Tra i soggetti espressamente menzionati figurano un rappresentante della Direzione nazionale antimafia e antiterrorismo, un rappresentante della Banca d'Italia e uno o più operatori economici inclusi nel perimetro di sicurezza nazionale cibernetica, individuati ai sensi dell'articolo 1, comma 2-bis, del cosiddetto "decreto-legge perimetro". Inoltre, la disposizione riconosce la possibilità di convocare altri soggetti pubblici o privati ritenuti rilevanti in relazione agli argomenti trattati. La previsione dell'articolo 5 si inquadra in una logica di rafforzamento del coordinamento interistituzionale, garantendo che le decisioni assunte nell'ambito del Nucleo per la Cybersicurezza possano beneficiare del contributo di enti e soggetti direttamente coinvolti nelle dinamiche di sicurezza nazionale cibernetica, con particolare riferimento a settori finanziari e strategici. L'inclusione della Banca d'Italia riflette l'importanza della sicurezza dei sistemi finanziari e bancari, sempre più soggetti a minacce informatiche di alto profilo, mentre il coinvolgimento della Direzione nazionale antimafia e antiterrorismo evidenzia la crescente convergenza tra cybercrime, minacce alla sicurezza nazionale e finanziamento di attività illecite

attraverso strumenti digitali. La norma sancisce inoltre che le amministrazioni e i soggetti convocati partecipino alle riunioni del Nucleo a livello di vertice, garantendo che le decisioni assunte riflettano una strategia unitaria e condivisa ai più alti livelli istituzionali e aziendali. Infine, viene confermato che la partecipazione ai lavori del Nucleo non dà diritto ad alcun compenso, gettone di presenza o rimborso spese, garantendo che l'operatività del Nucleo non comporti nuovi o maggiori oneri per la finanza pubblica. In sintesi, l'articolo 5 si inserisce nel quadro di una strategia di potenziamento della governance della cybersicurezza nazionale, rafforzando la capacità del Nucleo di operare in maniera integrata con attori chiave del sistema economico e della sicurezza nazionale, e consentendo un approccio più dinamico e flessibile nella gestione delle minacce cyber su scala nazionale e internazionale.

## Articolo 6 della Legge 28 giugno 2024, n. 90

L'articolo 6 della Legge 28 giugno 2024, n. 90 disciplina il coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la Cybersicurezza Nazionale (ACN), introducendo un meccanismo che consente, in circostanze eccezionali, il differimento di determinate attività di resilienza cibernetica quando ciò sia ritenuto strettamente necessario per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica. La norma stabilisce che le Agenzie di informazione e sicurezza interna ed esterna (AISI e AISE), di cui agli articoli 6 e 7 della legge 3 agosto 2007, n. 124, qualora vengano a conoscenza di un evento o incidente informatico, possano valutare l'opportunità di differire talune attività di resilienza previste dall'articolo 7, comma 1, lettere n) e n-bis), del decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109. Nel caso in cui tale differimento sia ritenuto necessario, le suddette Agenzie devono informare il Presidente del Consiglio dei ministri o l'Autorità delegata, ove istituita ai sensi dell'articolo 3 della legge n. 124/2007, per il tramite del Dipartimento delle informazioni per la sicurezza (DIS), che funge da organo di raccordo. La decisione finale spetta al Presidente del Consiglio dei ministri, il quale, sentiti il direttore generale del DIS e il direttore generale dell'ACN, può disporre il differimento degli obblighi informativi e delle attività di resilienza normalmente previsti dalla disciplina vigente, ivi compresi gli obblighi

informativi sanciti dall'articolo 17, commi 4 e 4-bis, del decreto-legge n. 82/2021. Questa disposizione risponde all'esigenza di armonizzare le attività dell'ACN con le priorità del Sistema di informazione per la sicurezza della Repubblica, garantendo che la gestione degli incidenti informatici e delle vulnerabilità critiche non interferisca con operazioni di intelligence o attività di sicurezza nazionale in corso. La ratio della norma è dunque quella di preservare il coordinamento strategico tra la risposta alle minacce cibernetiche e le esigenze di riservatezza e tutela degli interessi nazionali, evitando che l'attuazione immediata di misure di resilienza possa compromettere indagini in corso o altre attività sensibili. In tal senso, il ruolo del Presidente del Consiglio emerge come garante del bilanciamento tra la necessità di intervenire tempestivamente sugli incidenti informatici e quella di tutelare gli interessi superiori della sicurezza nazionale. Il meccanismo di attivazione del differimento è concepito in modo tale da garantire la massima selettività e proporzionalità, limitando questa possibilità a casi di assoluta necessità, e prevedendo una consultazione obbligatoria tra i vertici degli organismi coinvolti. Inoltre, la previsione che la comunicazione debba avvenire per il tramite del DIS conferma il ruolo di quest'ultimo come organo centrale di coordinamento della sicurezza nazionale. Nel contesto più ampio delineato dalla Legge n. 90/2024, questa norma si inserisce in un disegno di rafforzamento della cooperazione interistituzionale nella gestione delle minacce cibernetiche, sancendo il principio secondo cui la cybersicurezza non può essere considerata un comparto autonomo, ma deve essere integrata all'interno delle strategie di sicurezza nazionale, in stretta sinergia con i servizi di intelligence e gli organi di governo.

## Articolo 7 della Legge 28 giugno 2024, n. 90

L'articolo 7 della Legge 28 giugno 2024, n. 90 apporta modifiche all'articolo 5, comma 3, della legge 3 agosto 2007, n. 124, ridefinendo la composizione del Comitato interministeriale per la sicurezza della Repubblica (CISR), organo centrale per la definizione degli indirizzi strategici della politica dell'informazione per la sicurezza nazionale. Le modifiche introdotte riguardano l'ampliamento della rappresentanza ministeriale all'interno del Comitato, riflettendo l'evoluzione delle priorità strategiche del Paese in materia di sicurezza e cybersicurezza. In primo luogo, la norma interviene

con un adeguamento terminologico, aggiornando la denominazione del Ministero degli Affari Esteri, che viene ora formalmente indicato come "Ministero degli affari esteri e della cooperazione internazionale", in coerenza con la sua attuale denominazione ufficiale. Questa modifica, sebbene di carattere formale, sottolinea il crescente rilievo della dimensione internazionale della sicurezza nazionale, riconoscendo il ruolo chiave della diplomazia nelle strategie di cybersicurezza e difesa. La seconda e più significativa innovazione consiste nell'ampliamento della composizione del CISR mediante l'inclusione di nuovi dicasteri, in sostituzione delle precedenti competenze attribuite al Ministero dello sviluppo economico e al Ministero della transizione ecologica. La nuova composizione prevede la partecipazione dei seguenti ministri: Ministro delle imprese e del made in Italy, Ministro dell'ambiente e della sicurezza energetica, Ministro dell'agricoltura, della sovranità alimentare e delle foreste, Ministro delle infrastrutture e dei trasporti e Ministro dell'università e della ricerca. Questa estensione riflette un'espansione dell'ambito di competenza del CISR, con l'integrazione di settori strategici la cui rilevanza nella sicurezza nazionale è cresciuta nel contesto delle trasformazioni tecnologiche e geopolitiche. L'inclusione del Ministero delle imprese e del made in Italy evidenzia l'importanza della sicurezza industriale e della protezione delle infrastrutture critiche, in un contesto in cui la digitalizzazione del settore produttivo rende il comparto manifatturiero e tecnologico sempre più esposto a minacce cibernetiche e a tentativi di ingerenza economica da parte di attori statali e non statali. La presenza del Ministero dell'ambiente e della sicurezza energetica risponde all'esigenza di integrare nella strategia di sicurezza nazionale il settore dell'energia e delle risorse ambientali, oggi fortemente esposto a rischi di cyberattacchi, sabotaggi e tensioni geopolitiche legate alla transizione energetica. L'inserimento del Ministero dell'agricoltura, della sovranità alimentare e delle foreste riflette il riconoscimento della sicurezza agroalimentare come ambito strategico, in linea con le più recenti direttive europee sulla protezione delle filiere critiche e sul contrasto alle minacce ibride, comprese quelle cibernetiche. Il Ministero delle infrastrutture e dei trasporti entra a far parte del CISR per garantire un presidio più efficace sulla sicurezza delle reti logistiche e dei trasporti, che rappresentano un target privilegiato di attacchi informatici, mentre la presenza del Ministero dell'università e della ricerca sottolinea il ruolo crescente dell'innovazione e della cooperazione scientifica nella definizione delle strategie nazionali di cybersicurezza.

Queste modifiche rafforzano il carattere interdisciplinare e intersettoriale del CISR, assicurando che le decisioni in materia di sicurezza nazionale siano informate dalle competenze di una platea più ampia di attori istituzionali. La nuova composizione riflette inoltre l'importanza crescente della cybersicurezza e della protezione delle infrastrutture digitali nel quadro delle strategie di difesa nazionale, con una maggiore attenzione alla resilienza economica, energetica e tecnologica del Paese. Nel contesto più ampio della Legge n. 90/2024, questa disposizione si inserisce in un processo di rafforzamento della governance della sicurezza nazionale, garantendo una maggiore capacità di coordinamento tra i diversi ministeri coinvolti nella gestione delle minacce emergenti e delle vulnerabilità sistemiche.

## Articolo 8 della Legge 28 giugno 2024, n. 90

L'articolo 8 della Legge 28 giugno 2024, n. 90 introduce disposizioni mirate al rafforzamento della resilienza delle pubbliche amministrazioni in materia di cybersicurezza, imponendo l'istituzione di strutture dedicate e la nomina di un referente per la cybersicurezza. L'obiettivo è quello di consolidare un sistema di governance della sicurezza informatica, garantendo la pianificazione, l'attuazione e il monitoraggio delle misure di protezione dei sistemi informativi e delle infrastrutture digitali delle amministrazioni pubbliche. La norma stabilisce che i soggetti obbligati ai sensi dell'articolo 1, comma 1, qualora non dispongano già di una struttura specifica, debbano individuare un'unità organizzativa, anche tra quelle già esistenti, che operi nell'ambito delle risorse disponibili a legislazione vigente. Tale struttura assume il compito di sviluppare politiche e procedure di sicurezza delle informazioni, predisporre e aggiornare sistemi di rilevamento preventivo delle minacce informatiche e piani di gestione del rischio, nonché elaborare un documento organizzativo sulla sicurezza delle informazioni e un piano strategico per la protezione di dati, sistemi e infrastrutture. Inoltre, essa è incaricata di implementare interventi di rafforzamento delle capacità di gestione del rischio informatico, assicurando la piena conformità alle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale (ACN) e monitorando in modo continuo le minacce e vulnerabilità. All'interno di tale struttura opera il referente per la cybersicurezza, individuato in base a comprovate

competenze professionali nel settore. Nel caso in cui l'amministrazione non disponga di personale con tali requisiti, è prevista la possibilità di conferire l'incarico a un dipendente di un'altra pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165. Il referente assume il ruolo di punto di contatto unico con l'ACN, assicurando l'integrazione delle disposizioni della presente legge con le normative settoriali in materia di cybersicurezza. A tale fine, il nominativo del referente deve essere formalmente comunicato all'ACN, al fine di garantire un coordinamento strutturato tra l'ente e l'autorità nazionale preposta alla sicurezza cibernetica. La legge consente, inoltre, che la struttura e il referente possano coincidere con l'ufficio e il responsabile per la transizione al digitale, già previsti dall'articolo 17 del Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82). Tale disposizione mira a evitare duplicazioni organizzative, ottimizzando le risorse umane e finanziarie disponibili all'interno delle amministrazioni. Inoltre, le pubbliche amministrazioni possono esercitare le funzioni di cybersicurezza in forma associata, secondo quanto previsto dallo stesso articolo 17, commi 1-sexies e 1-septies, del Codice dell'amministrazione digitale, favorendo la creazione di strutture condivise tra più enti al fine di garantire una gestione più efficiente delle risorse e una maggiore capacità di risposta alle minacce informatiche. L'Agenzia per la Cybersicurezza Nazionale è inoltre autorizzata a definire modalità di coordinamento e collaborazione tra le amministrazioni pubbliche e i referenti per la cybersicurezza, con l'obiettivo di migliorare la resilienza complessiva del settore pubblico. Questo rafforzamento del coordinamento mira a facilitare la condivisione di informazioni sulle minacce, migliorare la gestione degli incidenti e ottimizzare l'adozione delle misure di protezione e prevenzione informatica. Sono tuttavia escluse dall'applicazione di queste disposizioni alcune categorie di soggetti. In particolare, l'articolo 8 esonera: a) Gli enti già soggetti agli obblighi di cybersicurezza previsti dal decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, per i quali continuano a valere le disposizioni di quella disciplina. b) Gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa e alla sicurezza militare dello Stato, nonché gli organismi di intelligence di cui alla legge 3 agosto 2007, n. 124, che già operano sotto regimi di sicurezza informatica differenziati e specifici per la tutela della

sicurezza nazionale. Nel contesto più ampio della Legge n. 90/2024, l'articolo 8 rappresenta un passo significativo verso una maggiore strutturazione della cybersicurezza nel settore pubblico, imponendo a tutte le amministrazioni rilevanti l'adozione di strategie organiche per la protezione delle informazioni e delle infrastrutture digitali. La previsione di una figura di riferimento in ciascun ente, con il compito di garantire il collegamento diretto con l'ACN, risponde all'esigenza di creare un ecosistema di sicurezza integrato, capace di rispondere con maggiore prontezza ed efficacia alle minacce cyber che colpiscono la pubblica amministrazione.

## Articolo 9 della Legge 28 giugno 2024, n. 90

L'articolo 9 della Legge 28 giugno 2024, n. 90 introduce disposizioni volte a rafforzare la sicurezza dei dati attraverso l'uso della crittografia, imponendo specifici obblighi di verifica alle strutture individuate ai sensi dell'articolo 8 della presente legge, nonché a quelle operanti per i soggetti già soggetti agli obblighi previsti dall'articolo 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, e dal decreto legislativo 18 maggio 2018, n. 65 (attuativo della Direttiva NIS in materia di sicurezza delle reti e dei sistemi informativi). La norma stabilisce che le suddette strutture siano tenute a verificare che tutti i programmi, applicazioni informatiche e strumenti di comunicazione elettronica in uso rispettino le linee guida sulla crittografia e sulla conservazione delle password, adottate dall'Agenzia per la Cybersicurezza Nazionale (ACN) e dal Garante per la Protezione dei Dati Personali. L'obiettivo è garantire che le soluzioni crittografiche impiegate siano conformi ai più elevati standard di sicurezza, prevenendo il rischio che vulnerabilità tecniche possano esporre i dati cifrati a intercettazioni o compromissioni da parte di terzi. Un aspetto cruciale della disposizione riguarda l'obbligo di verificare l'assenza di vulnerabilità note nelle implementazioni crittografiche, al fine di evitare configurazioni insicure che potrebbero rendere disponibili e intellegibili i dati cifrati a soggetti non autorizzati. Questo implica che le amministrazioni e gli enti soggetti alla disciplina della legge debbano monitorare costantemente le vulnerabilità di sicurezza note, applicando le necessarie patch e aggiornamenti per eliminare eventuali falle crittografiche. La previsione di un doppio livello di controllo, da parte sia dell'ACN sia

del Garante per la Protezione dei Dati Personali, evidenzia l'intento di coniugare la protezione della cybersicurezza nazionale con la tutela della riservatezza e dell'integrità dei dati personali. Questo è particolarmente rilevante nel contesto della crescente diffusione di minacce avanzate come gli attacchi di tipo quantum computing-resistant, che potrebbero in futuro compromettere la robustezza degli algoritmi crittografici attualmente in uso. Nel quadro più ampio della Legge n. 90/2024, l'articolo 9 rappresenta un passaggio strategico verso un rafforzamento della sicurezza dei dati sensibili e critici, promuovendo l'adozione di tecnologie di cifratura avanzate e la costante verifica della robustezza delle implementazioni crittografiche. Tale disposizione si inserisce in un più ampio approccio di sicurezza proattiva, in linea con gli standard internazionali in materia di cybersicurezza e protezione dei dati.

## Articolo 10 della Legge 28 giugno 2024, n. 90

L'articolo 10 della Legge 28 giugno 2024, n. 90 modifica l'articolo 7, comma 1, lettera m-bis, del decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109, ridefinendo e ampliando il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) in materia di crittografia. L'intervento normativo rafforza la funzione dell'ACN quale autorità di riferimento per lo sviluppo e la promozione di standard crittografici avanzati, con l'obiettivo di garantire un elevato livello di sicurezza nei sistemi informatici e di protezione delle informazioni sensibili e strategiche. La nuova formulazione della lettera m-bis) assegna all'ACN la competenza nella definizione di standard, linee guida e raccomandazioni per la cybersicurezza dei sistemi informatici, con particolare attenzione alla valutazione della sicurezza dei sistemi crittografici e alla divulgazione di pratiche avanzate in materia di cifratura. La norma enfatizza inoltre il ruolo della crittografia come strumento centrale di cybersicurezza, promuovendone l'adozione anche nel contesto delle tecnologie blockchain, la cui diffusione è in costante crescita nel settore finanziario, amministrativo e industriale. Un elemento di particolare rilievo è l'impegno dell'ACN nel rafforzamento dell'autonomia industriale e tecnologica dell'Italia, attraverso la promozione della ricerca e dello sviluppo di algoritmi crittografici proprietari. La norma stabilisce che l'Agenzia favorisca la collaborazione con università, centri di ricerca e partner internazionali per il

potenziamento delle capacità crittografiche nazionali. Questa disposizione risponde alla necessità di ridurre la dipendenza da tecnologie crittografiche sviluppate all'estero, soprattutto in un contesto in cui la cybersicurezza assume una dimensione sempre più strategica nel panorama geopolitico globale. Per dare attuazione a queste nuove funzioni, viene formalmente istituito presso l'ACN il Centro Nazionale di Crittografia, che opererà nell'ambito delle risorse disponibili senza nuovi o maggiori oneri per la finanza pubblica. Tale struttura avrà il compito di fungere da centro di competenza nazionale per tutte le tematiche relative alla crittografia in ambito non classificato, coordinando le attività di ricerca e sviluppo e definendo le strategie per la protezione delle infrastrutture digitali critiche mediante soluzioni di cifratura avanzata. Restano ferme le competenze dell'Ufficio Centrale per la Segretezza (UCSe), di cui all'articolo 9 della legge 3 agosto 2007, n. 124, per quanto concerne la gestione delle informazioni classificate. Allo stesso modo, la norma non interferisce con le prerogative degli organismi di intelligence nazionale di cui agli articoli 4, 6 e 7 della legge n. 124/2007, garantendo una chiara distinzione tra gli ambiti di competenza in materia di sicurezza delle informazioni. L'articolo 10 si inserisce nel quadro di una strategia nazionale volta a rafforzare la resilienza cibernetica del Paese attraverso l'uso di tecnologie crittografiche avanzate e il consolidamento della sovranità tecnologica nel settore della cifratura. In un contesto in cui le minacce informatiche si evolvono rapidamente, e con la prospettiva dell'emergere di computazione quantistica in grado di compromettere gli attuali standard di crittografia, la norma rappresenta un passo fondamentale per garantire l'integrità, la riservatezza e l'inalterabilità delle informazioni strategiche nazionali.

### Articolo 11 della Legge 28 giugno 2024, n. 90

L'articolo 11 della Legge 28 giugno 2024, n. 90 introduce un nuovo comma 4-quater all'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto

2021, n. 109, con l'obiettivo di disciplinare il procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la Cybersicurezza Nazionale (ACN). La norma prevede che la disciplina del procedimento sanzionatorio venga definita attraverso un regolamento, il quale dovrà stabilire termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza, nonché per l'irrogazione delle relative sanzioni. Tale regolamento avrà la funzione di fornire un quadro procedurale chiaro e dettagliato per l'applicazione delle sanzioni amministrative, assicurando trasparenza, uniformità e certezza giuridica nell'azione dell'ACN. Il regolamento dovrà essere adottato entro novanta giorni dalla data di entrata in vigore della presente disposizione, mediante decreto del Presidente del Consiglio dei Ministri (DPCM), anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, che normalmente disciplina l'iter di approvazione dei regolamenti governativi. L'adozione del regolamento dovrà avvenire sentito il Comitato interministeriale per la cybersicurezza e previa acquisizione del parere delle competenti Commissioni parlamentari, garantendo così un controllo istituzionale sul contenuto del provvedimento. Fino alla sua entrata in vigore, i procedimenti sanzionatori seguiranno la disciplina generale contenuta nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689, che regolamenta l'accertamento delle violazioni amministrative, la contestazione degli illeciti e le modalità di applicazione delle sanzioni pecuniarie. Ciò consente di evitare vuoti normativi e garantire la continuità dell'azione amministrativa dell'ACN anche nelle fasi transitorie. La disposizione si inserisce in un quadro normativo più ampio volto a rafforzare i poteri di enforcement dell'ACN, attribuendole strumenti più incisivi per vigilare sulla corretta applicazione delle misure di cybersicurezza, prevenire comportamenti inadempienti da parte dei soggetti obbligati e sanzionare le violazioni in modo efficace e tempestivo. La previsione di un regolamento specifico mira a garantire che l'ACN possa operare con criteri procedurali chiari e coerenti con il principio di legalità, evitando discrezionalità eccessive nell'applicazione delle sanzioni. Nel contesto della Legge n. 90/2024, l'articolo 11 rappresenta un passaggio fondamentale per l'attuazione del nuovo sistema di cybersicurezza nazionale, in quanto assicura la piena operatività del meccanismo sanzionatorio, consolidando il ruolo dell'ACN quale autorità di riferimento per la protezione delle infrastrutture critiche e delle reti strategiche del Paese.

## Articolo 12 della Legge 28 giugno 2024, n. 90

L'articolo 12 della Legge 28 giugno 2024, n. 90 introduce modifiche significative all'articolo 12 del decreto-legge 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109, apportando nuove disposizioni in materia di personale dell'Agenzia per la Cybersicurezza Nazionale (ACN), con particolare attenzione alla gestione delle risorse umane altamente specializzate e alla disciplina delle progressioni di carriera. Una delle principali innovazioni riguarda l'introduzione del nuovo comma 8-ter, il quale stabilisce che i dipendenti appartenenti al ruolo del personale dell'ACN, che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a percorsi formativi di specializzazione, non possano essere assunti né assumere incarichi presso soggetti privati per lo svolgimento di mansioni in materia di cybersicurezza per un periodo di due anni dalla data di completamento dell'ultimo percorso formativo frequentato. La disposizione è volta a prevenire fenomeni di "brain drain" e conflitti di interesse, evitando che le competenze acquisite grazie alla formazione finanziata dall'ACN vengano immediatamente trasferite al settore privato, con possibili ricadute negative sulla sicurezza nazionale e sulla continuità operativa dell'Agenzia. Per garantire l'efficacia di questa limitazione, la norma prevede che i contratti stipulati in violazione di tale divieto siano considerati nulli, impedendo quindi qualsiasi forma di elusione della regola. Tuttavia, la norma introduce alcune eccezioni, escludendo dal divieto il personale che abbia cessato il servizio presso l'ACN per motivi legati a collocamento a riposo d'ufficio, raggiungimento del requisito anagrafico per la pensione di vecchiaia, cessazione a domanda per inabilità o dispensa dal servizio per motivi di salute. Questa previsione risponde all'esigenza di tutelare i diritti dei dipendenti in situazioni di uscita dal servizio per cause non volontarie. Il testo stabilisce inoltre che i percorsi formativi di specializzazione soggetti a questa disciplina debbano essere individuati dal direttore generale dell'ACN, tenendo conto della qualità dell'offerta formativa, dei costi, della durata e del livello di specializzazione conseguito. Ciò garantisce che solo formazioni altamente qualificate e strategiche rientrino nell'ambito di applicazione del divieto, evitando restrizioni eccessive su percorsi di aggiornamento meno rilevanti. Un'ulteriore novità introdotta dalla legge riguarda la progressione di carriera

all'interno dell'ACN. La disposizione stabilisce che, fino al 31 dicembre 2026, il requisito di permanenza minima nell'Area operativa ai fini del passaggio all'Area manageriale e alte professionalità sia ridotto a tre anni. Questa modifica mira a favorire una più rapida crescita professionale del personale, incentivando lo sviluppo di competenze strategiche e accelerando la formazione di una dirigenza specializzata in cybersicurezza. Nel contesto più ampio della Legge n. 90/2024, l'articolo 12 si inserisce in una strategia volta a rafforzare le capacità operative dell'ACN, garantendo una maggiore stabilità del personale altamente qualificato, evitando la dispersione delle competenze acquisite nel settore privato e accelerando la crescita professionale all'interno dell'Agenzia. Queste misure rispondono alla crescente necessità di consolidare un corpo tecnico altamente specializzato in grado di affrontare le sfide della cybersicurezza nazionale, in un contesto caratterizzato da minacce informatiche in continua evoluzione e dalla crescente rilevanza della protezione delle infrastrutture digitali critiche.

### Articolo 13 della Legge 28 giugno 2024, n. 90

L'articolo 13 della Legge 28 giugno 2024, n. 90 introduce disposizioni volte a regolamentare le restrizioni post-incarico per il personale degli organismi di informazione per la sicurezza, al fine di proteggere il patrimonio informativo acquisito durante il servizio e prevenire potenziali conflitti di interesse o compromissioni della sicurezza nazionale. La norma stabilisce che coloro che hanno ricoperto incarichi apicali presso il Dipartimento delle Informazioni per la Sicurezza (DIS), l'Agenzia Informazioni e Sicurezza Esterna (AISE) o l'Agenzia Informazioni e Sicurezza Interna (AISI) – tra cui direttori generali, vice direttori generali e dirigenti di prima fascia con funzioni di preposizione a strutture organizzative di livello generale – non possano svolgere attività lavorative, professionali o di consulenza presso soggetti esteri o soggetti privati italiani che operano in settori strategici, per un periodo di tre anni successivi alla cessazione dall'incarico, salvo specifica autorizzazione del Presidente del Consiglio dei Ministri o dell'Autorità delegata (se istituita). Questa limitazione si applica per prevenire l'utilizzo di informazioni riservate acquisite durante l'incarico in attività che potrebbero compromettere la sicurezza nazionale o generare interferenze

con l'operato dello Stato. L'eventuale autorizzazione è concessa solo dopo una valutazione approfondita delle esigenze di protezione del patrimonio informativo e dell'assenza di pregiudizi per la sicurezza nazionale. Un'ulteriore restrizione riguarda il personale appartenente al ruolo unico del DIS, AISE e AISI, disciplinato dall'articolo 21 della legge 3 agosto 2007, n. 124. Tale personale, nei tre anni successivi alla cessazione dal servizio, non può svolgere attività lavorative, professionali o di consulenza presso enti privati titolari di licenza di investigazione o raccolta informativa, ai sensi dell'articolo 134 del Testo Unico delle Leggi di Pubblica Sicurezza (TULPS, R.D. 18 giugno 1931, n. 773), né presso soggetti che operano in ambiti investigativi o di raccolta dati sensibili. Questa previsione è finalizzata a evitare che competenze acquisite nell'intelligence vengano impiegate in contesti privati con potenziali rischi di abuso o deviazione dall'interesse pubblico. La legge introduce inoltre un divieto specifico per il personale del DIS, AISE e AISI che abbia partecipato, a spese dello Stato, a percorsi formativi di alta specializzazione. In particolare, per tre anni successivi al completamento di tali percorsi, tali soggetti non possono essere assunti né assumere incarichi presso enti privati per svolgere le stesse mansioni per cui hanno ricevuto la formazione, evitando così che le risorse investite dallo Stato in formazione avanzata vengano sfruttate da soggetti privati in contesti potenzialmente contrari all'interesse nazionale. Per garantire il rispetto di queste restrizioni, l'articolo stabilisce che i contratti stipulati in violazione delle disposizioni siano considerati nulli. Questa misura rafforza la capacità dello Stato di prevenire eventuali abusi o elusioni della normativa. La norma prevede inoltre l'adozione di un regolamento attuativo, ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, per disciplinare le procedure di autorizzazione per i casi previsti dal comma 1, gli obblighi di dichiarazione e comunicazione a carico dei dipendenti interessati, le eventuali eccezioni alle limitazioni previste nei commi 2 e 3, nonché le modalità di individuazione dei percorsi formativi che comportano il divieto di cui al comma 3. Nel contesto della Legge n. 90/2024, l'articolo 13 si inserisce in un quadro normativo più ampio volto a rafforzare la protezione delle informazioni strategiche detenute dai servizi di intelligence italiani, evitando rischi di fuga di dati sensibili o compromissioni delle capacità operative dello Stato. La previsione di limiti chiari e vincolanti per il reimpiego del personale di intelligence nel settore privato è una misura in linea con le best practice internazionali, garantendo che le competenze maturate in ambito di sicurezza nazionale non vengano

impiegate in contesti non controllabili o in potenziale conflitto con gli interessi dello Stato.

## Articolo 14 della Legge 28 giugno 2024, n. 90

L'articolo 14 della Legge 28 giugno 2024, n. 90 disciplina i contratti pubblici relativi all'approvvigionamento di beni e servizi informatici destinati a contesti connessi alla tutela degli interessi nazionali strategici, introducendo criteri stringenti di cybersicurezza e raccordandosi con la normativa preesistente, in particolare con il decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133. Al fine di garantire la protezione delle infrastrutture digitali critiche e la sicurezza delle informazioni trattate, il legislatore dispone che, entro centoventi giorni dall'entrata in vigore della presente legge, sia adottato un decreto del Presidente del Consiglio dei Ministri (DPCM) su proposta dell'Agenzia per la Cybersicurezza Nazionale (ACN) e previo parere del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), il quale avrà il compito di individuare, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti pubblici e privati rientranti nel perimetro di applicazione della normativa dovranno obbligatoriamente considerare nei procedimenti di acquisizione, nonché i casi in cui, per la tutela della sicurezza nazionale, dovranno essere previsti criteri di premialità per le offerte che contemplino l'uso di tecnologie sviluppate in Italia, nei Paesi membri dell'Unione Europea (UE), nei Paesi aderenti all'Alleanza Atlantica (NATO) o in Paesi terzi individuati dal medesimo decreto, purché questi ultimi siano parte di accordi di collaborazione con l'UE o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. La norma introduce il concetto di "elementi essenziali di cybersicurezza", definendoli come l'insieme di criteri e regole tecniche la cui conformità garantisce il rispetto dei principi fondamentali di confidenzialità, integrità e disponibilità dei dati trattati, assicurando livelli di protezione adeguati alla rilevanza strategica dei sistemi e delle informazioni coinvolte. Per effetto delle previsioni normative, le stazioni appaltanti, comprese le centrali di committenza, sono obbligate a integrare tali elementi nelle procedure di approvvigionamento, potendo esercitare la facoltà di non aggiudicare un

appalto nel caso in cui un'offerta non soddisfi i requisiti di cybersicurezza stabiliti dal DPCM. In sede di valutazione delle offerte, l'elemento qualitativo legato alla cybersicurezza assume un ruolo centrale, in quanto i requisiti individuati dal decreto dovranno essere tenuti in considerazione per determinare il miglior rapporto qualità/prezzo, mentre nelle procedure basate sul criterio del minor prezzo essi saranno inclusi tra i requisiti minimi obbligatori. Inoltre, quando viene applicato il criterio dell'offerta economicamente più vantaggiosa, viene fissato un limite del 10% per il punteggio economico, al fine di evitare che il fattore economico prevalga a discapito della sicurezza delle soluzioni tecnologiche adottate. La norma stabilisce altresì che, nei casi in cui l'approvvigionamento riguardi beni e servizi informatici destinati a infrastrutture critiche o settori strategici per la sicurezza nazionale, dovranno essere previsti criteri di premialità per le offerte che propongano tecnologie sviluppate in Italia, nell'UE o nei Paesi NATO, incentivando così il rafforzamento dell'autonomia tecnologica nazionale ed europea e la riduzione della dipendenza da fornitori esteri potenzialmente non affidabili. L'applicazione delle disposizioni contenute nel DPCM è estesa anche ai soggetti privati non rientranti nel perimetro delle pubbliche amministrazioni ma che operano in settori strategici per la sicurezza nazionale, come definiti dall'articolo 1, comma 2-bis, del decreto-legge n. 105/2019, garantendo così un'applicazione uniforme dei requisiti di sicurezza informatica su scala nazionale. La norma si coordina con le previsioni già contenute nell'articolo 1 del decreto-legge n. 105/2019, che disciplina l'approvvigionamento di beni, sistemi e servizi di information and communication technology (ICT) destinati all'impiego nelle reti e nei sistemi informativi critici, assicurando la coerenza tra le nuove disposizioni e l'impianto normativo esistente. L'articolo 14 rappresenta un passaggio di fondamentale rilevanza per il rafforzamento della resilienza cibernetica nazionale, in quanto impone che le procedure di approvvigionamento di tecnologie digitali siano allineate ai più elevati standard di sicurezza, riducendo i rischi derivanti dall'impiego di soluzioni informatiche vulnerabili e promuovendo la crescita dell'industria nazionale della cybersicurezza. In un contesto in cui le minacce informatiche si evolvono con crescente rapidità e complessità, la normativa introduce strumenti normativi idonei a garantire la protezione delle infrastrutture strategiche del Paese e a rafforzare il controllo sulle tecnologie impiegate nelle reti pubbliche e private di rilevanza nazionale. L'inserimento di criteri obbligatori di cybersicurezza nelle gare

d'appalto pubbliche e la promozione dell'utilizzo di tecnologie sviluppate da fornitori europei e atlantici costituiscono una misura di autotutela strategica, finalizzata a prevenire il rischio di ingerenze ostili e vulnerabilità sistemiche derivanti dall'uso di prodotti o servizi di provenienza incerta. L'articolo si inserisce pertanto in una visione più ampia di cybersicurezza nazionale, orientata al consolidamento di un sistema di approvvigionamento pubblico altamente sicuro e all'incentivazione dello sviluppo di un ecosistema tecnologico nazionale ed europeo resiliente, in linea con le più avanzate politiche di protezione delle infrastrutture critiche adottate a livello internazionale.

## Articolo 15 della Legge 28 giugno 2024, n.90

L'articolo 15 della Legge 28 giugno 2024, n. 90 introduce una modifica all'articolo 16 della legge 21 febbraio 2024, n. 15, ampliando l'ambito della delega conferita al Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale nel settore finanziario. La modifica interviene con l'inserimento della nuova lettera c-bis), che estende le competenze regolatorie in materia di cybersicurezza e resilienza operativa digitale agli intermediari finanziari iscritti nell'albo di cui all'articolo 106 del Testo Unico Bancario (TUB), nonché alla società Poste Italiane S.p.A. per l'attività del Patrimonio Bancoposta. La finalità di tale intervento normativo è garantire un livello di sicurezza e stabilità del settore finanziario in linea con le prescrizioni europee, assicurando che anche gli operatori non bancari adottino presidi di cybersicurezza equivalenti a quelli previsti per gli altri enti creditizi e finanziari regolamentati dal diritto dell'Unione Europea. Il nuovo impianto normativo richiede che gli intermediari finanziari e il Patrimonio Bancoposta implementino misure di resilienza operativa digitale comparabili a quelle stabilite dal Regolamento (UE) 2022/2554, prevedendo l'obbligo di conformarsi a standard avanzati in materia di sicurezza informatica, protezione dei dati e continuità operativa. L'intervento normativo recepisce il principio di proporzionalità, stabilendo che i requisiti di resilienza operativa debbano essere calibrati in base alla dimensione, alla complessità operativa e alla tipologia di attività svolta dagli intermediari finanziari e dal Patrimonio Bancoposta, evitando così oneri regolamentari eccessivi per gli operatori di minore dimensione, pur garantendo

un'adeguata protezione dei dati e dei servizi finanziari da potenziali minacce cyber. Per assicurare la corretta applicazione della normativa, la disposizione attribuisce alla Banca d'Italia i poteri di vigilanza, di indagine e sanzionatori, allineando la supervisione di questi soggetti a quella esercitata sulle banche e sugli altri istituti finanziari vigilati ai sensi del regolamento europeo. L'attribuzione di tali poteri all'Autorità di vigilanza bancaria nazionale si configura come un elemento essenziale per garantire un'applicazione uniforme delle norme sulla resilienza operativa digitale e per prevenire eventuali vulnerabilità sistemiche nel settore finanziario. La modifica normativa, pur introducendo nuove disposizioni di vigilanza e adeguamento regolamentare, specifica che la sua attuazione non deve comportare nuovi o maggiori oneri a carico della finanza pubblica, stabilendo che le amministrazioni competenti provvedano ai relativi adempimenti con le risorse già disponibili a legislazione vigente. Questa previsione mira a garantire l'efficacia del nuovo quadro normativo senza gravare sul bilancio pubblico, affidando l'implementazione delle nuove misure di sicurezza operativa digitale agli intermediari finanziari e ai soggetti regolati, nel rispetto delle best practices europee e internazionali in materia di cybersicurezza. Nel contesto della Legge n. 90/2024, l'articolo 15 rappresenta un ulteriore passo verso l'armonizzazione del sistema finanziario nazionale con gli standard europei in materia di cybersicurezza e resilienza digitale, ponendo particolare attenzione alla protezione delle infrastrutture critiche finanziarie e alla prevenzione di minacce informatiche che potrebbero compromettere la stabilità dell'intero sistema economico. L'inclusione degli intermediari finanziari non bancari e del Patrimonio Bancoposta nel perimetro della regolamentazione in materia di cybersicurezza rafforza il paradigma di sicurezza nazionale, impedendo che attori strategici del mercato finanziario rimangano esposti a rischi derivanti da attacchi informatici o da falle nei sistemi di sicurezza digitale. L'approccio adottato riflette la crescente consapevolezza dell'importanza della resilienza operativa digitale nel settore finanziario, riconoscendo che la sicurezza informatica non può essere trattata come un elemento accessorio, ma deve essere considerata un pilastro essenziale per la stabilità del sistema economico e per la fiducia degli investitori e degli utenti nei servizi finanziari.

## Articolo 16 della Legge 28 giugno 2024, n. 90

L'articolo 16 della Legge 28 giugno 2024, n. 90 introduce significative modifiche al Codice penale in materia di criminalità informatica, rafforzando il quadro sanzionatorio e ampliando la tutela dei sistemi informatici e telematici di interesse pubblico e privato. L'intervento normativo si inserisce nel più ampio processo di adeguamento dell'ordinamento giuridico alle nuove minacce cibernetiche, ponendo particolare attenzione alla repressione di condotte quali l'accesso abusivo ai sistemi informatici, la diffusione di strumenti atti all'intercettazione o alla compromissione dei dati, la distruzione o l'alterazione di informazioni sensibili e le estorsioni informatiche. La prima modifica riguarda l'articolo 240 del Codice penale, ampliando l'ambito della confisca obbligatoria a beni e strumenti informatici utilizzati per la commissione dei reati di frode informatica, garantendo così la privazione dei mezzi illeciti e il recupero di eventuali profitti derivanti dalle attività criminose. L'articolo 615-ter, relativo all'accesso abusivo a un sistema informatico o telematico, subisce un incremento della pena, che passa da un minimo di due anni a un massimo di dieci anni di reclusione, con un aggravamento per i reati commessi con violenza, minaccia, abuso di qualità professionali o con danni alla funzionalità del sistema o ai dati in esso contenuti. Si introduce inoltre la punibilità per la sottrazione di dati attraverso riproduzione o trasmissione senza autorizzazione del titolare, allineando la norma alle esigenze di protezione delle informazioni digitali. Il terzo comma estende le pene previste per i reati commessi ai danni di sistemi di interesse militare, di pubblica sicurezza, di protezione civile o di sanità pubblica, elevando il massimo edittale a dodici anni di reclusione. L'articolo 615-quater, che disciplina la detenzione, diffusione e installazione abusiva di strumenti informatici idonei all'accesso non autorizzato ai sistemi telematici, introduce il concetto di vantaggio al posto di profitto, ampliando il raggio d'azione della norma, e prevede un aumento di pena per i reati commessi ai danni di sistemi informatici di interesse pubblico. L'articolo 615-quinquies è abrogato, accorpando la sua disciplina alle nuove disposizioni sull'uso illecito di strumenti informatici. Gli articoli 617-bis, 617-quater, 617-quinquies e 617-sexies, che regolano le

intercettazioni illecite, l'impedimento e la falsificazione delle comunicazioni informatiche, vengono riformulati per introdurre aggravanti specifiche nei casi in cui il reato sia commesso da pubblici ufficiali, investigatori privati o operatori del sistema con abuso delle proprie funzioni, con l'obiettivo di reprimere le violazioni più insidiose della privacy digitale. Le pene massime sono elevate fino a dieci anni di reclusione, riconoscendo la gravità delle violazioni ai danni di istituzioni pubbliche o di soggetti vulnerabili. L'intervento normativo estende l'ambito di applicazione dell'articolo 629, includendo tra le condotte estorsive l'uso di minacce legate alla sicurezza informatica, quali il danneggiamento o il blocco di sistemi informatici o la sottrazione di dati sensibili. La pena per questa specifica forma di estorsione informatica varia da un minimo di sei anni fino a un massimo di ventidue anni di reclusione, con aggravanti per i reati commessi contro persone incapaci per età o infermità. Gli articoli 635-bis, 635-ter e 635-quater rafforzano la disciplina del danneggiamento di informazioni, dati e sistemi informatici, con un aggravamento delle pene per i reati che comportano la cancellazione, l'alterazione, la trasmissione o l'inaccessibilità di dati e programmi informatici. Nei casi più gravi, in cui il danneggiamento sia perpetrato da pubblici ufficiali, investigatori privati o attraverso violenza o minaccia, la pena può arrivare fino a dodici anni di reclusione. Viene introdotto il nuovo articolo 635-quater.1, che punisce la detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici finalizzati a danneggiare sistemi informatici o telematici. Questa disposizione mira a colpire la creazione e la distribuzione di malware, ransomware e altri strumenti di attacco cibernetico, prevedendo pene che variano da due a otto anni di reclusione. L'articolo 640 introduce una nuova aggravante per la truffa informatica, punendo con pene da uno a cinque anni di reclusione i reati commessi a distanza attraverso strumenti informatici che ostacolino l'identificazione dell'autore del reato. Tale previsione risponde alla crescente diffusione delle frodi digitali, che sfruttano tecniche di anonimizzazione per eludere le indagini delle autorità. Infine, il nuovo articolo 639-ter introduce circostanze attenuanti per i reati informatici, prevedendo una riduzione di pena nei casi di lieve entità e per i soggetti che collaborino attivamente con le autorità per limitare i danni derivanti dal reato o per recuperare i proventi illeciti. Tale previsione mira a incentivare la cooperazione dei soggetti coinvolti in attività illecite informatiche, con un approccio ispirato alla giustizia riparativa. Queste modifiche al Codice penale delineano un significativo

rafforzamento della normativa penale in materia di cybercrime, rendendo il sistema sanzionatorio più severo e adeguato alle nuove forme di criminalità informatica. L'approccio adottato mira non solo a punire le condotte illecite, ma anche a prevenire e contrastare le minacce informatiche attraverso strumenti giuridici più efficaci, proteggendo la sicurezza nazionale, i dati personali e la stabilità del sistema digitale pubblico e privato.

## Articolo 17 della Legge 28 giugno 2024, n. 90

L'articolo 17 della Legge 28 giugno 2024, n. 90 introduce modifiche di rilevante impatto al Codice di procedura penale, con l'obiettivo di rafforzare la risposta dell'ordinamento agli illeciti di natura informatica e di garantire maggiore efficacia alle indagini preliminari sui reati che coinvolgono sistemi telematici di interesse pubblico o strategico. L'intervento normativo si inserisce in un più ampio quadro di riforma volto a contrastare le minacce cibernetiche e a dotare gli organi inquirenti di strumenti adeguati per perseguire con maggiore incisività i responsabili di attacchi informatici o di altre condotte lesive della sicurezza digitale. Una prima modifica concerne l'articolo 51, comma 3-quinquies, che disciplina la competenza distrettuale per determinate categorie di reati di particolare gravità. Con la novella legislativa, viene eliminato ogni riferimento all'articolo 615-quinquies – abrogato dalla presente legge – e viene contestualmente estesa la competenza distrettuale ai procedimenti relativi ai reati previsti dagli articoli 635-quater.1 e 635-quinquies del Codice penale, i quali puniscono rispettivamente la detenzione e diffusione di strumenti informatici idonei alla compromissione di sistemi informatici e il danneggiamento di sistemi informatici di interesse pubblico. Inoltre, si attribuisce la competenza alle procure distrettuali anche per il reato di inosservanza degli obblighi di notifica di incidenti di sicurezza previsti dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. Quest'ultima previsione mira a garantire un monitoraggio più efficace degli episodi di compromissione della sicurezza informatica, in particolare quelli che coinvolgono soggetti rientranti nel perimetro di sicurezza cibernetica nazionale. Un'ulteriore modifica riguarda l'articolo 406, comma 5-bis, relativo alla proroga dei termini delle indagini preliminari per i reati di maggiore complessità

investigativa. La novella normativa amplia il novero dei delitti per i quali è possibile concedere una proroga senza necessità di notificare la richiesta alle parti, includendo i reati informatici di particolare rilevanza, con specifico riferimento a quelli che colpiscono sistemi critici o di pubblica utilità. L'estensione di questa disciplina ai reati previsti dal nuovo articolo 635-quater.1 del Codice penale conferma l'intento del legislatore di equiparare il contrasto alla criminalità informatica alle misure già previste per i reati di criminalità organizzata o di terrorismo, rafforzando il quadro investigativo. Di particolare rilievo è la modifica dell'articolo 407, comma 2, lettera a), che disciplina i termini di durata massima delle indagini preliminari. Il legislatore introduce il numero 7-ter, il quale prevede un termine massimo di due anni per le indagini relative a specifici reati informatici, quando il fatto è commesso ai danni di sistemi telematici di interesse militare, di ordine pubblico, di sicurezza pubblica, di sanità, di protezione civile o comunque di interesse pubblico. I reati contemplati da questa previsione includono le fattispecie più gravi, quali l'accesso abusivo a sistemi informatici protetti (art. 615-ter), la detenzione e diffusione abusiva di strumenti per l'accesso non autorizzato (art. 615-quater), le intercettazioni illecite di comunicazioni informatiche (art. 617-quater e art. 617-quinquies), la falsificazione delle comunicazioni telematiche (art. 617-sexies), il danneggiamento e l'interruzione di sistemi informatici (artt. 635-bis, 635-ter, 635-quater, 635-quater.1 e 635-quinquies). L'introduzione di un termine massimo di due anni per lo svolgimento delle indagini preliminari su questi reati è motivata dalla necessità di garantire tempestività ed efficacia nelle attività investigative, considerando la rapida evoluzione delle minacce informatiche e la difficoltà di raccolta delle prove digitali, spesso soggette a cancellazione o alterazione. Il termine esteso consente agli inquirenti di sviluppare indagini più approfondite e articolate, riducendo il rischio di prescrizione e assicurando una più efficace repressione dei reati cibernetici. Queste modifiche confermano l'orientamento dell'ordinamento verso un rafforzamento della tutela penale della sicurezza informatica, dotando gli organi investigativi di strumenti più incisivi e prevedendo un regime procedurale specifico per i reati informatici di maggiore gravità. L'adeguamento della normativa processuale penale rappresenta un ulteriore tassello nella costruzione di un sistema di cybersicurezza nazionale solido ed efficace, in grado di fronteggiare con maggiore prontezza le minacce provenienti dal

cyberspazio e di garantire una più elevata protezione delle infrastrutture digitali critiche e dei dati sensibili della collettività.

## Articolo 18 della Legge 28 giugno 2024, n. 90

L'articolo 18 della Legge 28 giugno 2024, n. 90 introduce significative modifiche al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, recante disposizioni in materia di protezione di testimoni di giustizia e collaboratori. L'intervento normativo amplia il campo di applicazione delle speciali misure di protezione e dei benefici penitenziari, estendendone l'operatività anche a determinate figure coinvolte in procedimenti riguardanti reati informatici di particolare gravità e rilevanza strategica per la sicurezza nazionale. In primo luogo, viene modificato l'articolo 9, comma 2, introducendo tra i reati che giustificano l'applicazione delle speciali misure di protezione anche quelli di cui all'articolo 371-bis, comma 4-bis, del codice di procedura penale. Questa disposizione, che disciplina la cooperazione tra le procure e il coordinamento delle indagini su reati informatici gravi, viene ora riconosciuta come rilevante ai fini dell'accesso ai programmi di protezione, equiparando i soggetti che forniscono un contributo investigativo su tali illeciti ai collaboratori di giustizia coinvolti in indagini su criminalità organizzata e terrorismo. Analogamente, l'articolo 11, comma 2, viene integrato con il riferimento all'articolo 371-bis, comma 4-bis, prevedendo che la proposta di ammissione alle speciali misure di protezione possa essere formulata in relazione a procedimenti che vedano coinvolti reati di cybercriminalità connessi alla sicurezza nazionale. In tal modo, si riconosce che la collaborazione nelle indagini relative agli attacchi contro sistemi informatici di interesse strategico può esporre i testimoni e gli informatori a gravi rischi per l'incolumità personale, rendendo necessaria l'adozione di misure di tutela analoghe a quelle previste per i testimoni di giustizia operanti in altri contesti criminali. Un'ulteriore innovazione riguarda l'articolo 16-nonies, che disciplina i benefici penitenziari per i soggetti condannati che abbiano fornito collaborazione con la giustizia. Anche in questo caso, si inserisce tra i reati che possono giustificare la concessione di liberazione condizionale, permessi premio e misure alternative alla detenzione il riferimento all'articolo 371-bis, comma 4-bis, del codice di procedura

penale. Ciò significa che un individuo condannato per reati informatici di alto impatto sulla sicurezza nazionale potrà ottenere benefici carcerari qualora dimostri effettiva e significativa cooperazione con l'autorità giudiziaria, in particolare contribuendo a smascherare organizzazioni criminali attive nel cyberspazio o fornendo elementi utili alla prevenzione di attacchi informatici. Queste modifiche testimoniano un cambiamento di prospettiva del legislatore, che considera ormai le minacce cibernetiche non più come meri reati economici o tecnologici, ma come forme di criminalità organizzata ed eversiva, potenzialmente equiparabili al terrorismo e alla mafia per la loro capacità di compromettere la sicurezza nazionale e l'ordine democratico. Di conseguenza, l'ordinamento si adegua prevedendo forme di protezione e incentivi alla collaborazione analoghe a quelle storicamente riservate ai pentiti di mafia e ai testimoni di giustizia. L'estensione del regime di protezione e dei benefici penitenziari a soggetti coinvolti in reati informatici di particolare gravità rafforza il contrasto alla criminalità digitale e incentiva il dissociarsi dalle organizzazioni dedite ad attività di hacking malevolo, cyber-estorsione e attacchi contro infrastrutture critiche. La riforma, dunque, si inserisce in un più ampio quadro di potenziamento della sicurezza cibernetica nazionale, mirando a facilitare l'emersione di informazioni strategiche e a promuovere una cooperazione più efficace tra il sistema giudiziario e gli esperti del settore digitale, con l'obiettivo di contrastare le minacce più sofisticate che caratterizzano il panorama contemporaneo della sicurezza informatica.

## Articolo 19 della Legge 28 giugno 2024, n. 90

L'articolo 19 della Legge 28 giugno 2024, n. 90 introduce una modifica significativa al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, concernente i provvedimenti urgenti in tema di lotta alla criminalità organizzata. In particolare, l'intervento legislativo estende l'applicabilità delle disposizioni relative alle intercettazioni telefoniche e ambientali ai procedimenti per reati informatici di particolare gravità, quando questi siano riconducibili a minacce alla sicurezza nazionale, all'ordine pubblico e alla protezione delle infrastrutture critiche. L'integrazione avviene con l'introduzione del comma 3-bis all'articolo 13 del decreto-

legge n. 152/1991, il quale stabilisce che le deroghe al regime ordinario delle intercettazioni, già previste per i delitti di criminalità organizzata, si applicano anche ai procedimenti per i reati disciplinati dall'articolo 371-bis, comma 4-bis, del codice di procedura penale. Quest'ultima disposizione si riferisce a reati informatici di particolare rilevanza, come attacchi contro infrastrutture strategiche nazionali, operazioni di cyberwarfare, accesso abusivo a sistemi di sicurezza critica e sabotaggi informatici. L'effetto di questa modifica è duplice. In primo luogo, consente l'autorizzazione all'intercettazione delle comunicazioni, sia telefoniche che ambientali, senza la necessità di soddisfare i requisiti stringenti previsti dall'articolo 267 del codice di procedura penale, qualora il reato rientri nelle fattispecie sopra menzionate. Questo allineamento con le procedure adottate per i reati di stampo mafioso e terroristico rappresenta un chiaro riconoscimento dell'alto livello di pericolosità associato ad alcune tipologie di cybercrimini, ponendoli sullo stesso piano dei reati tradizionalmente considerati più insidiosi per la sicurezza dello Stato. In secondo luogo, la modifica incide sulla durata massima delle intercettazioni, permettendo un primo periodo di quarantacinque giorni e successive proroghe di venti giorni, rispetto ai limiti più rigidi previsti per i reati comuni. Tale disposizione è motivata dalla complessità delle indagini su reati informatici di matrice organizzata, che spesso richiedono lunghi tempi di analisi dei flussi di dati, tracciamento delle comunicazioni criptate e identificazione dei responsabili dietro reti anonime e server offshore. Un ulteriore aspetto rilevante è la possibilità di coordinamento tra il pubblico ministero e le forze di polizia giudiziaria specializzate, in modo analogo a quanto già avviene per le operazioni contro la criminalità organizzata. Questo significa che il Cybercrime Investigation Department e le unità di sicurezza informatica delle forze dell'ordine potranno partecipare attivamente alle attività di intercettazione e analisi dei dati, avvalendosi di strumenti tecnici avanzati per la raccolta di prove digitali. L'inserimento di questa norma nel decreto-legge n. 152/1991, un provvedimento nato per combattere la mafia, dimostra un cambio di paradigma nel contrasto ai crimini informatici: non più considerati reati minori, ma forme di criminalità strutturata e strategica, con impatti che possono compromettere la sicurezza dello Stato, l'integrità del sistema finanziario e la protezione delle infrastrutture critiche. Con questa riforma, l'ordinamento si dota di strumenti più incisivi per contrastare minacce cyber avanzate, come gli attacchi perpetrati da gruppi criminali internazionali o da attori statali ostili,

riconoscendo il ruolo centrale delle intercettazioni nelle indagini su operazioni di cyberterrorismo, cyberestorsione e intrusioni nei sistemi di difesa nazionale. In tal senso, il legislatore rafforza l'integrazione tra intelligence, magistratura e polizia postale, ponendo le basi per un approccio più efficace e coordinato nella lotta alle minacce digitali globali.

## Articolo 20 della Legge 28 giugno 2024, n. 90

L'articolo 20 della Legge 28 giugno 2024, n. 90 introduce rilevanti modifiche al decreto legislativo 8 giugno 2001, n. 231 ampliando e inasprendo il regime di responsabilità amministrativa degli enti per i reati informatici e le condotte estorsive realizzate mediante strumenti digitali con l'obiettivo di rafforzare il sistema sanzionatorio nei confronti delle persone giuridiche e incentivare l'adozione di misure di prevenzione e compliance aziendale in materia di sicurezza informatica e contrasto al cybercrime. L'intervento normativo modifica l'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231 prevedendo un aumento della sanzione pecuniaria applicabile agli enti coinvolti nella commissione dei reati di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale innalzando la relativa forcella sanzionatoria da cento-cinquecento quote a duecento-settecento quote elevando così l'incidenza economica delle misure pecuniarie e accrescendo la deterrenza rispetto a fattispecie criminose quali accesso abusivo a sistemi informatici, intercettazione illecita di comunicazioni, danneggiamento di dati e sistemi e altre condotte lesive dell'integrità e della disponibilità delle infrastrutture digitali. Ulteriore rilevante innovazione è rappresentata dall'introduzione di un nuovo comma 1-bis che estende la responsabilità amministrativa degli enti alla commissione del delitto di estorsione informatica di cui all'articolo 629, terzo comma, del codice penale e stabilisce una sanzione pecuniaria compresa tra trecento e ottocento quote aggravando il trattamento sanzionatorio per condotte quali sequestro di dati informatici, attacchi ransomware e minacce digitali finalizzate all'ottenimento di un indebito profitto attraverso l'inibizione dell'accesso a informazioni sensibili o la minaccia della loro divulgazione con il chiaro intento di contrastare l'allarmante diffusione del fenomeno della cyber-extortion imponendo agli enti l'adozione di idonee misure di mitigazione

del rischio quali incremento della sicurezza dei dati, implementazione di protocolli di monitoraggio delle transazioni finanziarie e sensibilizzazione del personale rispetto alle tecniche di attacco basate su ingegneria sociale. Contestualmente si introduce una revisione del comma 2 dell'articolo 24-bis eliminando il riferimento all'abrogato articolo 615-quinquies del codice penale e sostituendolo con il nuovo articolo 635-quater.1 che disciplina la detenzione, diffusione e installazione abusiva di strumenti informatici idonei a compromettere la sicurezza di sistemi digitali elevando la sanzione pecuniaria massima applicabile agli enti da trecento a quattrocento quote con l'intento di reprimere la produzione e la diffusione illecita di malware, spyware ed exploit che costituiscono strumenti privilegiati per la realizzazione di attacchi informatici su larga scala. Altra significativa innovazione riguarda la modifica del comma 4 dell'articolo 24-bis con l'introduzione di un regime sanzionatorio interdittivo per le persone giuridiche condannate per il delitto di estorsione informatica di cui al comma 1-bis prevedendo l'applicazione delle sanzioni interdittive di cui all'articolo 9, comma 2, del decreto legislativo 231 del 2001 per un periodo minimo di due anni con la possibilità di irrogare misure quali interdizione dall'esercizio dell'attività, sospensione o revoca di autorizzazioni licenze o concessioni funzionali alla commissione del reato, divieto di contrattare con la pubblica amministrazione, esclusione da finanziamenti agevolazioni contributi e sussidi nonché divieto di pubblicizzare beni o servizi determinando un potenziale impatto devastante sulla continuità operativa e la capacità competitiva delle imprese coinvolte che rischiano l'esclusione dal mercato e incentivando le aziende ad adottare rigorosi protocolli di sicurezza e compliance in materia di cybersecurity. L'insieme delle modifiche introdotte evidenzia la volontà del legislatore di equiparare i reati informatici e di cyber-estorsione alle più gravi fattispecie di criminalità economica e organizzata imponendo alle imprese obblighi di prevenzione più incisivi e adeguati alla crescente sofisticazione delle minacce digitali con particolare riferimento alla necessità di implementare sistemi avanzati di difesa dagli attacchi informatici, procedure di monitoraggio e gestione degli accessi ai dati sensibili, politiche di gestione del rischio informatico e resilienza digitale, audit periodici sui sistemi IT, formazione del personale in materia di sicurezza informatica e predisposizione di piani di risposta agli incidenti informatici in modo da conformarsi alle nuove prescrizioni normative ed evitare le pesanti sanzioni pecuniarie e

interdittive che potrebbero compromettere la stabilità operativa e finanziaria delle organizzazioni.

## Articolo 21 della Legge 28 giugno 2024, n. 90

L'Articolo 21 della presente legge introduce una modifica all'articolo 11, comma 2, della legge 11 gennaio 2018, n. 6, che disciplina le disposizioni per la protezione dei testimoni di giustizia, ampliando l'ambito delle ipotesi in cui la Commissione centrale per la definizione delle speciali misure di protezione è tenuta ad acquisire il parere del Procuratore nazionale antimafia e antiterrorismo. L'intervento normativo, in particolare, prevede l'inserimento, tra le fattispecie rilevanti ai fini della richiesta del parere, anche delle ipotesi previste dall'articolo 371-bis, comma 4-bis, del codice di procedura penale, estendendo così la valutazione del Procuratore nazionale anche ai procedimenti relativi a specifici reati di criminalità organizzata, terrorismo e minacce alla sicurezza dello Stato che necessitano di un approccio investigativo integrato e coordinato a livello nazionale. Questa modifica si inserisce in un più ampio quadro di interventi legislativi finalizzati a rafforzare la tutela dei testimoni di giustizia, in considerazione del loro ruolo determinante nell'accertamento di condotte criminose di particolare gravità e nella disarticolazione di organizzazioni criminali dotate di un elevato livello di sofisticazione e pericolosità. L'integrazione normativa risponde all'esigenza di garantire un più alto grado di protezione ai soggetti che, attraverso le proprie dichiarazioni, contribuiscono in modo significativo alle attività investigative e processuali, rendendosi spesso bersaglio di ritorsioni da parte delle organizzazioni criminali colpite dalle loro testimonianze. L'intervento legislativo si fonda sul principio della specializzazione nell'ambito della gestione delle misure di protezione, attribuendo al Procuratore nazionale antimafia e antiterrorismo un ruolo cruciale nella valutazione del rischio e della necessità di attivazione delle tutele previste per i testimoni. La modifica si inserisce inoltre nel contesto di un rafforzamento delle sinergie istituzionali tra l'autorità giudiziaria e gli organi amministrativi deputati alla sicurezza, mirando a garantire una più efficace ed uniforme applicazione delle misure di protezione, riducendo i margini di discrezionalità e assicurando un approccio fondato su criteri oggettivi e su una valutazione tecnico-specialistica delle condizioni

di pericolo. Dal punto di vista sistematico, l'ampliamento delle ipotesi di acquisizione del parere del Procuratore nazionale si colloca nel solco delle riforme volte a migliorare il coordinamento tra le diverse articolazioni dello Stato impegnate nella lotta alla criminalità organizzata e al terrorismo, nonché a incrementare l'efficacia della risposta istituzionale alle minacce provenienti da soggetti o gruppi in grado di esercitare forme di intimidazione o di condizionamento nei confronti dei testimoni. In tale prospettiva, il rafforzamento del ruolo del Procuratore nazionale antimafia e antiterrorismo consente una maggiore omogeneità nella valutazione della rilevanza delle dichiarazioni rese dai testimoni di giustizia, contribuendo a garantire un bilanciamento tra l'interesse pubblico alla repressione dei reati e l'esigenza di assicurare un'adeguata protezione ai collaboratori dell'autorità giudiziaria. Sotto il profilo applicativo, la riforma introduce un vincolo procedurale che impone alla Commissione centrale per la protezione dei testimoni di giustizia di richiedere il parere del Procuratore nazionale non solo per i reati già previsti, ma anche per quelli rientranti nell'articolo 371-bis, comma 4-bis, del codice di procedura penale, garantendo un più elevato livello di approfondimento nella fase di ammissione alle misure di protezione. Tale previsione, oltre a rafforzare la tutela dei testimoni, contribuisce a consolidare l'efficacia della normativa in materia di protezione, assicurando che la valutazione dell'opportunità di concessione delle misure sia affidata a un soggetto istituzionale dotato delle competenze e delle informazioni necessarie per apprezzare il rischio concreto cui il testimone è esposto. L'estensione dell'ambito di applicazione della disciplina trova giustificazione nell'evoluzione delle strategie criminali, che sempre più spesso si avvalgono di strumenti tecnologici avanzati e operano su scala transnazionale, rendendo necessaria una risposta istituzionale flessibile e capace di adattarsi a contesti in rapida trasformazione. In questo scenario, la riforma consente di rafforzare la capacità dello Stato di prevenire e contrastare in modo più incisivo le minacce alla sicurezza pubblica e alla legalità, fornendo ai testimoni di giustizia una protezione più efficace e garantendo al contempo un migliore coordinamento tra gli organi deputati alla sicurezza e alla giustizia.

## Articolo 22 della Legge 28 giugno 2024, n. 90

L'Articolo 22 introduce significative modifiche all'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, rafforzando il ruolo dell'Agenzia per la cybersicurezza nazionale (ACN) e del CSIRT Italia nelle attività di contrasto agli attacchi informatici e nella gestione della sicurezza cibernetica nazionale. La novella normativa conferisce al personale dell'Agenzia addetto al CSIRT Italia la qualifica di pubblico ufficiale, con conseguenti responsabilità e obblighi che ne derivano, tra cui l'immediata trasmissione delle notifiche di incidente informatico all'organo centrale del Ministero dell'interno preposto alla sicurezza e alla regolarità dei servizi di telecomunicazione, in ottemperanza agli obblighi sanciti dall'articolo 331 del codice di procedura penale. Questa disposizione mira a garantire un più efficace coordinamento tra l'ACN e le autorità competenti in materia di sicurezza pubblica, assicurando una risposta tempestiva ed efficace agli attacchi informatici che possano compromettere la sicurezza nazionale o il funzionamento di infrastrutture critiche. Viene inoltre introdotta una disciplina specifica per i casi in cui l'ACN acquisisca notizia di un attacco informatico ai danni di sistemi telematici di particolare rilevanza strategica, come quelli individuati dall'articolo 371-bis, comma 4-bis, del codice di procedura penale. In tali ipotesi, oltre a procedere alle attività di contrasto e mitigazione previste dall'articolo 7, comma 1, lettere n) e n-bis), l'Agenzia ha l'obbligo di informare senza indugio il Procuratore nazionale antimafia e antiterrorismo. Tale previsione si colloca nell'ottica di una gestione centralizzata e coordinata degli attacchi informatici più gravi, con particolare riferimento a quelli riconducibili a fenomeni di cyberterrorismo o ad attività illecite perpetrate da organizzazioni criminali complesse. Contestualmente, il nuovo comma 4-bis.2 stabilisce che, laddove sia il pubblico ministero a venire a conoscenza di reati rientranti nella fattispecie dell'articolo 371-bis, comma 4-bis, del codice di procedura penale, egli ha il dovere di informarne tempestivamente l'ACN, garantendo altresì il raccordo informativo con l'organo del Ministero dell'interno preposto alla sicurezza delle telecomunicazioni. Tale disposizione si inserisce in un quadro di rafforzamento delle sinergie tra autorità giudiziaria e autorità amministrative preposte alla sicurezza cibernetica, assicurando che le attività investigative si svolgano in stretta collaborazione con le istituzioni deputate alla protezione delle infrastrutture digitali

nazionali. Un ulteriore elemento di rilievo è rappresentato dalla previsione, contenuta nel nuovo comma 4-bis.3, che attribuisce al pubblico ministero la facoltà di impartire disposizioni necessarie per garantire il coordinamento tra le attività di resilienza svolte dall'ACN e le esigenze investigative. In particolare, il pubblico ministero può disporre, con provvedimento motivato e adottato senza ritardo, il differimento delle attività di resilienza cibernetica nei casi in cui esse possano arrecare grave pregiudizio al corso delle indagini. Questa norma mira a bilanciare l'esigenza di garantire la sicurezza e l'integrità dei sistemi informatici con quella di preservare l'efficacia dell'azione investigativa, evitando che interventi di mitigazione degli attacchi possano compromettere la raccolta di prove e l'identificazione dei responsabili. Infine, il comma 4-bis.4 introduce un ulteriore strumento di collaborazione tra l'autorità giudiziaria e l'ACN, prevedendo che, in caso di accertamenti tecnici irripetibili relativi ai reati previsti dall'articolo 371-bis, comma 4-bis, del codice di procedura penale, il pubblico ministero debba informare senza ritardo l'Agenzia, la quale può partecipare alle operazioni tramite propri rappresentanti. Questa disposizione si applica anche quando gli accertamenti vengono eseguiti nelle forme dell'incidente probatorio, assicurando così che l'ACN possa fornire il proprio supporto tecnico-specialistico nelle fasi più delicate dell'indagine. Nel complesso, le modifiche introdotte dall'Articolo 22 rispondono all'esigenza di rafforzare il sistema di sicurezza informatica nazionale, garantendo una più stretta collaborazione tra l'ACN, il Ministero dell'interno e l'autorità giudiziaria nella gestione e nel contrasto delle minacce cibernetiche. Esse rappresentano un ulteriore passo verso l'integrazione tra le attività di protezione cibernetica e quelle di contrasto ai reati informatici, assicurando un approccio coordinato e multidisciplinare alla sicurezza delle infrastrutture digitali del Paese.

### Articolo 23 della Legge 28 giugno 2024, n. 90

L'Articolo 23 introduce modifiche significative all'Articolo 7 della legge 12 agosto 1962, n. 1311, concernente l'organizzazione e il funzionamento dell'Ispettorato generale presso il Ministero della Giustizia, con l'obiettivo di rafforzare le misure di sicurezza negli accessi alle banche dati utilizzate dagli uffici giudiziari. Tale intervento normativo risponde alla crescente necessità di tutela della riservatezza e dell'integrità delle

informazioni giudiziarie, che rappresentano un asset strategico nell'ambito della sicurezza e dell'efficienza del sistema giudiziario. La novella normativa stabilisce che, nell'ambito delle ispezioni ordinarie disposte dal Capo dell'Ispettorato generale del Ministero della Giustizia per verificare il corretto funzionamento degli uffici giudiziari e l'osservanza delle disposizioni normative e regolamentari vigenti, venga effettuata anche una verifica specifica sul rispetto delle prescrizioni di sicurezza negli accessi alle banche dati in uso presso tali uffici. Questa integrazione al primo comma dell'Articolo 7 mira a garantire che il trattamento delle informazioni contenute nei sistemi informatici della giustizia avvenga in conformità con i più elevati standard di protezione, riducendo i rischi di accessi non autorizzati e di eventuali violazioni della riservatezza. Parallelamente, la modifica al terzo comma introduce una verifica analoga nell'ambito delle ispezioni straordinarie che il Ministro della Giustizia può disporre in qualsiasi momento per accertare la produttività degli uffici giudiziari, l'entità e la tempestività del lavoro svolto dai magistrati. L'ampliamento dell'oggetto delle ispezioni ministeriali consente di monitorare in modo più puntuale l'efficacia delle misure di cybersecurity adottate negli uffici giudiziari, assicurando che l'accesso alle banche dati sia regolato da protocolli stringenti, atti a prevenire ogni forma di uso improprio o di esposizione a minacce informatiche. L'introduzione di questa duplice verifica ispettiva – sia in ambito ordinario sia in ambito straordinario – risponde all'esigenza di rafforzare la protezione dei dati giudiziari, in un contesto in cui la digitalizzazione dei procedimenti e la crescente interconnessione dei sistemi informatici della pubblica amministrazione impongono un innalzamento dei livelli di sicurezza informatica. Tale intervento normativo si pone dunque in linea con le più avanzate strategie di cybersecurity applicate alle infrastrutture digitali della giustizia, favorendo una maggiore resilienza delle banche dati rispetto a possibili tentativi di accesso non autorizzato, furto di informazioni o alterazione di dati sensibili. L'integrazione normativa si configura come un passo fondamentale verso la creazione di un sistema giudiziario più sicuro ed efficiente, nel quale la tutela delle informazioni e la trasparenza dell'operato degli uffici giudiziari siano garantite attraverso controlli sistematici e approfonditi. Il potenziamento del ruolo ispettivo in materia di sicurezza cibernetica rappresenta inoltre un ulteriore strumento per la prevenzione di fenomeni di cybercrime che potrebbero compromettere il regolare svolgimento delle attività giudiziarie, con possibili ripercussioni sulla fiducia nell'amministrazione della giustizia

e sulla protezione dei diritti dei cittadini. In conclusione, l'articolo 23 si inserisce nel più ampio quadro delle misure di modernizzazione e rafforzamento del sistema di giustizia digitale, introducendo un meccanismo di controllo volto a garantire che le infrastrutture informatiche della magistratura rispondano ai più elevati standard di sicurezza, contribuendo così a preservare l'integrità del sistema giudiziario e a consolidare la protezione delle informazioni sensibili in esso custodite.

## Articolo 24 della Legge 28 giugno 2024, n. 90

L'articolo 24 introduce specifiche disposizioni di carattere finanziario connesse all'attuazione della presente legge, stabilendo un principio fondamentale di invarianza finanziaria per evitare impatti negativi sui conti pubblici. Il primo comma chiarisce che le misure previste dalla normativa devono essere attuate senza determinare nuovi o maggiori oneri a carico della finanza pubblica, imponendo alle amministrazioni competenti di provvedere all'adempimento degli obblighi derivanti dalla legge esclusivamente con le risorse umane, strumentali e finanziarie già disponibili a legislazione vigente. Tale previsione è volta a garantire il rispetto dei vincoli di bilancio e la sostenibilità economica delle misure introdotte, in conformità con i principi di contenimento della spesa pubblica e di razionalizzazione delle risorse amministrative. Il secondo comma disciplina la destinazione delle entrate derivanti dall'irrogazione delle sanzioni previste dall'Articolo 1, comma 6, stabilendo che tali proventi debbano confluire direttamente nel bilancio dell'Agenzia per la cybersicurezza nazionale. In particolare, si fa riferimento all'Articolo 11, comma 2, lettera f), del decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, che disciplina le competenze finanziarie dell'Agenzia, consolidandone il ruolo centrale nella gestione delle risorse destinate al rafforzamento della resilienza informatica del Paese. Questo meccanismo di finanziamento autonomo per l'Agenzia si configura come una misura strategica per garantire un adeguato supporto alle attività di cybersecurity, assicurando un flusso di risorse finanziarie derivanti direttamente dalle sanzioni irrogate per il mancato rispetto delle disposizioni in materia di sicurezza cibernetica.

L'impianto normativo delineato dall'articolo 24 si inserisce, dunque, in una logica di efficienza della spesa pubblica e di autofinanziamento dei settori strategici della sicurezza nazionale, evitando la necessità di ricorrere a nuovi stanziamenti di bilancio e garantendo al contempo un utilizzo mirato e razionale delle entrate derivanti dall'attività sanzionatoria. L'obiettivo principale di questa disposizione è quello di assicurare che le nuove misure di tutela della cybersicurezza e di rafforzamento della protezione delle infrastrutture critiche possano essere implementate senza incidere negativamente sulle disponibilità finanziarie dello Stato, sfruttando le risorse già esistenti e prevedendo una destinazione vincolata dei proventi sanzionatori a favore dell'ente preposto alla sicurezza cibernetica nazionale. In definitiva, l'Articolo 24 rappresenta un elemento cruciale dell'intero impianto legislativo, poiché definisce i principi cardine della sostenibilità economica dell'intervento normativo, garantendo che le nuove disposizioni siano attuate nel rispetto dell'equilibrio di bilancio e senza compromettere la stabilità delle finanze pubbliche. Al contempo, esso assicura che l'Agenzia per la cybersicurezza nazionale possa disporre di risorse finanziarie adeguate per svolgere il proprio ruolo istituzionale, rafforzando la protezione delle reti e dei sistemi informatici strategici per il Paese e promuovendo un'efficace azione di prevenzione e contrasto alle minacce cibernetiche.