Legge italiana sulla Cybersecurity: cosa prevede



La legge italiana sulla cybersecurity 90/2024 segna una svolta decisiva nella protezione digitale del Paese, introducendo per la prima volta un quadro normativo organico e uniforme. Approvata il 28 giugno 2024, questa normativa pionieristica stabilisce nuovi obblighi stringenti per Pubbliche Amministrazioni e aziende private, allineandosi agli standard europei della Direttiva NIS2. L'analisi che segue esamina in dettaglio l'istituzione del Centro Nazionale di Crittografia, il rafforzamento dei poteri dell'Agenzia per la Cybersicurezza Nazionale, il nuovo sistema sanzionatorio con multe fino a 125.000 euro e le modifiche al codice penale che introducono l'estorsione informatica.

Introduzione alla legge italiana sulla cybersecurity 90/2024

Il 28 giugno del 2024 il Parlamento italiano ha approvato la legge n. 90 ("*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"), nota come "Legge sulla Cybersecurity".

La normativa rappresenta il primo tentativo del legislatore nazionale di fornire un'organica disciplina in ambito di sicurezza informatica, allineandosi agli standard internazionali ed europei.

A un anno dalla sua approvazione, analizziamo i principali contenuti della legge per valutarne la rispondenza alle sfide poste dall'attuale quadro tecnologico e normativo.

Obblighi per Pubbliche Amministrazioni e aziende private

La legge 90/2024 prevede nuovi obblighi a carico di aziende e Pubbliche Amministrazioni, con doveri particolarmente stringenti a carico di queste ultime.

Come conferma l'Agenzia per la Cybersicurezza Nazionale (ACN), le P.A. sono infatti tra i primi bersagli del crimine informatico in Italia, soprattutto in settori critici quali la sanità; senza dimenticare le campagne di attacco che prendono di mira – con motivazioni prettamente geopolitiche – Ministeri o altri enti istituzionali.

Ma le nuove norme riguardano anche aziende private, includendo tra i destinatari le società *in house* che forniscono alle Pubbliche Amministrazioni "*servizi informatici, servizi di trasporto […] ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali […] o di gestione dei rifiuti*".

Al fine di prevenire rischi reputazionali o perdite di dati, che sempre più spesso si annidano lungo le catene di fornitura dei servizi, tutti i soggetti così individuati sono tenuti a una serie di adempimenti.

Tra questi:

- l'obbligo di tempestiva segnalazione all'ACN degli attacchi o incidenti informatici rilevanti ai sensi del Perimetro di sicurezza nazionale cibernetica;
- la predisposizione e il costante aggiornamento di "*un piano per la gestione del rischio informatico*", che includa la definizione di ruoli e responsabilità rispetto alla "*sicurezza di dati, sistemi e infrastrutture*";
- l'implementazione di misure per il "*potenziamento delle capacità per la gestione dei rischi informatici*", in

riferimento alla necessità sia di adottare soluzioni tecnologiche adeguate sia di formare tutte le risorse per migliorarne la preparazione cyber.

Ai medesimi obblighi, oltre alle Pubbliche Amministrazioni nazionali, vanno soggette *"le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali"*.

Conformità agli standard dettati dalla Direttiva NIS 2

Recepita in Italia con il decreto legislativo n. 138/2024, la Direttiva UE nota come NIS 2 aveva già introdotto significativi adempimenti in materia di cybersicurezza per imprese e pubbliche amministrazioni europee.

Oltre a imporre l'adozione di un "Modello di Gestione della Cybersecurity" che includa misure di sicurezza proporzionate agli specifici rischi da fronteggiare, la NIS 2 pone particolare accento sulla segnalazione tempestiva degli incidenti. Un'indicazione recepita dalla L. 90/2024, che all'art. 1 chiede ad aziende e P.A. di segnalare *"senza ritardo e comunque entro il termine massimo di ventiquattro ore"* ogni evento che abbia avuto *"impatto su reti, sistemi informativi e servizi informatici"*.

A rispondere alle richieste della Direttiva è anche l'ampliamento delle funzioni dell'ACN. Questa viene infatti investita di un ruolo più attivo nel monitoraggio e nella valutazione delle misure adottate da enti e organizzazioni, da attuare coordinandosi – ove opportuno – con i Servizi di

informazione per la sicurezza nazionale: un approccio che considera il dialogo tra attori istituzionali e l'interscambio di flussi informativi strutturati come strumenti di contrasto alle minacce digitali.

Sempre per garantire rispondenza alla NIS2, tra i destinatari della legge italiana sulla cybersecurity sono stati inclusi anche i fornitori di varie tipologie di servizi, nella consapevolezza dei molteplici rischi sottesi alle articolazioni della *Supply Chain*.

Misure tecniche richieste: crittografia, monitoraggio e gestione dei rischi

La legge 90/2024 ha introdotto anche un nuovo organismo di settore: il Centro Nazionale di Crittografia (CNC), istituito presso l'Agenzia per la Cybersicurezza Nazionale.

Il CNC dovrà favorire *"la diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici […] nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza".*

Al nuovo organo spetterà inoltre il compito di sviluppare, in sinergia con università e centri di ricerca italiani ed esteri, soluzioni crittografiche avanzate per la protezione dei dati *"anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia"*, riducendo la dipendenza da tecnologie straniere nell'ottica di una maggiore sovranità digitale nazionale.

Contratti pubblici e requisiti di cybersecurity: il D.P.C.M. del 30 aprile 2025

La sovranità digitale è, inoltre, alla base della scelta di includere nella nuova legge anche disposizioni relative ai contratti pubblici, stabilendo criteri di premialità per l'adozione di tecnologie EU/NATO ed esigendo la successiva adozione di un decreto attuativo al riguardo.

È stato il D.P.C.M. del 30 aprile 2025 ad adempiere a tale previsione, individuando gli elementi che i destinatari della legge 90 devono considerare al momento di acquistare prodotti o servizi digitali da impiegare in contesti rilevanti per la tutela degli interessi strategici nazionali.

Si tratta in primo luogo di requisiti di cybersecurity, che includono la verifica di aspetti tecnici e capacità di gestione delle vulnerabilità informatiche; ma sono altresì contemplati criteri di opportunità geopolitica, nel preferire partner tecnologici afferenti a Paesi alleati o, comunque, affini all'Italia nella postura di sicurezza e nella protezione delle informazioni classificate.

Sistema sanzionatorio della legge italiana sulla cybersecurity

Organizzazioni ed enti interessati dalle nuove disposizioni, qualora senza giustificato motivo tardino nel notificare un incidente di sicurezza (o nell'adeguarsi alle segnalazioni dell'ACN *"circa specifiche vulnerabilità cui essi risultino potenzialmente esposti"*), vanno soggetti alle misure di cui agli art. 1 e 2 della legge 90/2024.

All'Agenzia spetta pertanto un ruolo preminente anche rispetto all'apparato sanzionatorio previsto: è infatti incaricata non

solo di monitorare gli adempimenti previsti ma di attivare i relativi procedimenti disciplinari, che possono culminare in sanzioni assai severe.

Queste possono includere multe fino a 125.000 € in caso di violazioni reiterate, potendo altresì *"costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili"*; aspetto che solleva numerosi dubbi circa la concreta possibilità di attribuire con esattezza tale responsabilità all'interno di organizzazioni complesse.

L'inasprimento delle pene pecuniarie riguarda anche gli enti, che per di più possono trovarsi a fronteggiare sanzioni interdittive della durata minima di due anni.

Oltre ad ampliare i poteri dell'ACN circa l'erogazione di tali sanzioni, con la l. 90/2024 il legislatore ha scelto di attribuire al personale dell'Agenzia impegnato presso il CSIRT Italia la qualifica di Pubblico Ufficiale nello svolgimento delle proprie funzioni.

Ciò assegna agli operatori dell'Agenzia funzioni di Polizia Giudiziaria quanto alla trasmissione alla magistratura delle notifiche di incidenti informatici, prevedendo al contempo sistemi automatizzati di allerta precoce per il *law enforcement* attraverso il monitoraggio dell'ACN.

Nuovi poteri investigativi: cosa cambia per le agenzie di law enforcement

In caso di attacchi che coinvolgano infrastrutture critiche o sistemi di interesse pubblico, l'ACN è tenuta a segnalarli immediatamente al Procuratore nazionale antimafia e antiterrorismo.

A sua volta, il Pubblico Ministero che abbia notizia di reati informatici rilevanti deve tempestivamente informarne l'Agenzia e coordinarsi con il Ministero dell'Interno, in un meccanismo di cooperazione rafforzata concepito per affrontare eventi cyber di particolare gravità.

La legge 90/2024 ha altresì modificato il quadro esistente in tema di intercettazioni e accertamenti tecnici – prevedendo la partecipazione dell'ACN alle operazioni irripetibili – nonché di protezione dei collaboratori di giustizia, estendendo l'applicabilità delle relative norme ai reati informatici particolarmente gravi.

Per tutti i principali crimini digitali, tenuto conto della complessità investigativa che comportano, la durata massima delle indagini preliminari è stata estesa a 2 anni, con la possibilità di prorogarle ulteriormente anche *inaudita altera parte* (ossia senza necessità di contraddittorio con i soggetti indagati).

Nel corso delle indagini, il PM ha inoltre facoltà di imporre la posticipazione di eventuali attività di resilienza informatica, se ritenga che le stesse possano interferire con lo svolgimento delle attività investigative.

A livello di codice penale la legge ha infine modificato numerose norme (art. 615 *ter* e seguenti) inasprendo le pene previste, che ora arrivano fino a 10 anni nei casi di accesso abusivo aggravato a sistemi informatici; e prevedendo circostanze aggravanti specifiche per gli attacchi rivolti a sistemi o infrastrutture di interesse pubblico, nei quali la condanna può raggiungere i 12 anni di reclusione.

Un'ultima novità della l. 90/2924 riguarda l'introduzione del reato di "estorsione informatica" all'art. 629, co. 3 c.p., mirato con ogni evidenza a contrastare il fenomeno *ransomware*, di gran lunga la più pervasiva e persistente tra le minacce informatiche contemporanee.

Conclusioni

A meno di un anno dalla sua entrata in vigore (avvenuta il 17 luglio 2024) e ad appena 6 mesi dalla scadenza di conformità concessa ad aziende ed enti locali (17 gennaio 2025), la Legge sulla Cybersecurity deve ancora ricevere una piena esecuzione.

Pur con talune criticità, relative anche alle nuove sfide in campo di *Security Testing*, si tratta di un oggettivo avanzamento nella difesa dell'ecosistema cyber italiano.

Inserendosi nella scia della Strategia nazionale di cybersicurezza e definendo un'organica cornice normativa per l'implementazione degli standard internazionali sulla cybersecurity, la l. 90/2024 è infatti la prima normativa italiana a imporre ad aziende e P.A. obblighi uniformi per la protezione dei loro *asset* digitali – primi fra tutti i dati di utenti e cittadini – e la difesa delle infrastrutture critiche nazionali.

La legge ha, inoltre, significativamente ampliato sia gli strumenti d'indagine sia i meccanismi di cooperazione nazionale e internazionale a livello di *law enforcement*, potenziando altresì il ruolo dell'ACN.

Resta da valutare quanto sarà concretamente fatto per favorire l'attuazione delle nuove previsioni e per garantirne l'aggiornamento alla luce di minacce informatiche sempre più pervasive, nonché di un panorama tecnologico in costante evoluzione.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/legge-italiana-sulla-cybersecurity/