di Fabrizio Fratoni

Le disposizioni in materia di rafforzamento della cybersicurezza nazionale e di contrasto alle minacce informatiche introdotte con la legge 28 giugno 2024 n. 90

La legge 28 giugno 2024 n. 90[1] ha introdotto nel nostro ordinamento importanti disposizioni finalizzate ad un necessario rafforzamento della cybersicurezza nazionale delle pubbliche amministrazioni e dei servizi di pubblica necessità, prevedendo al contempo norme per migliorare il funzionamento dell'Agenzia per la cybersicurezza nazionale, e degli organismi di informazione per la sicurezza, anche in relazione alla predisposizione dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici. Le misure introdotte dal provvedimento legislativo mirano a rafforzare la resilienza del nostro paese di fronte alle minacce cibernetiche sempre più sofisticate e frequenti, tanto da costituire un'importante evoluzione nella normativa italiana sulla cybersicurezza, imponendo un quadro di adempimenti, che richiede un'attenta e rapida attuazione da parte di pubbliche amministrazioni e aziende. Per le pubbliche amministrazioni[2], l'implementazione di questi obblighi deve essere interpretata, non solo come efficace e scrupoloso adeguamento ad un dovere legale, ma soprattutto come un necessario atto di responsabilità verso i cittadini e la sicurezza nazionale.

Le pubbliche amministrazioni sono uno dei principali destinatari degli obblighi sanciti dalla nuova normativa, i quali includono l'obbligo di notifica tempestiva degli incidenti informatici che potrebbero compromettere la sicurezza delle informazioni e delle reti. Questo obbligo mira a garantire una rapida risposta e mitigazione degli effetti negativi di eventuali attacchi cibernetici, tanto che la notifica deve includere dettagli sull'incidente, le misure adottate per contenerlo e le azioni intraprese per prevenirne il ripetersi. Inoltre, la normativa impone che nei contratti pubblici sottoscritti dalle pubbliche amministrazioni, vengano inseriti specifici requisiti di sicurezza informatica, per assicurare che i fornitori e i partner commerciali di tali amministrazioni rispettino gli standard di sicurezza richiesti, prevedendo specifiche clausole che obbligano i fornitori a implementare misure di sicurezza adeguate e a notificare, anche loro, eventuali incidenti di sicurezza.

La norma introduce anche delle preclusioni per l'assunzione di alcune tipologie professionisti: che non rispettano determinati requisiti di cybersicurezza, al fine di garantire che solo personale qualificato, in possesso di certificazioni specifiche e competenze aggiornate nel campo della sicurezza informatica e conforme agli standard di sicurezza, possa operare all'interno delle amministrazioni pubbliche. Anche le aziende dovranno interpretare i nuovi adempimenti normativi, non solo come un'ulteriore obbligo normativo ma piuttosto come

un'opportunità per migliorare la propria postura di sicurezza e proteggere le proprie risorse critiche, tanto che in questo ambito, l'accurato adempimento alle procedure di immediata segnalazione realizzerà un adeguata strategia di protezione e prevenzione degli attacchi cyber, in cui si rivelerà indispensabile una sempre più marcata collaborazione tra il settore pubblico e quello privato sarà essenziale per affrontare le sfide poste dalla cybersicurezza in modo efficace e coordinato.

L'obbligo di notificare tempestivamente gli incidenti informatici.

In particolare l'art.1, primo comma del provvedimento, introduce l'obbligo per le pubbliche amministrazioni centrali[3], 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[4] e le aziende sanitarie locali, di segnalare (senza ritardo e comunque entro 24 ore dalla cognizione dell'evento) e notificare[5] (entro 72 ore dall'evento, includendo tutti gli elementi informativi disponibili tramite apposite procedure disponibili sul sito dell'ACN) gli incidenti di sicurezza informatica[6] aventi impatto su reti, sistemi informativi e servizi informatici. Tale disposizione[7] risponde alla necessità di avere una immediata ed adeguata attività di percezione di incidenti o attacchi informatici all'Agenzia nazionale per la cybersicurezza aspetto indispensabile per poter contenerne i danni, atteso l'elevato pericolo di propagazione ad altri sistemi informatici strategici, consentendo il tempestivo intervento del CSIRT[8] e del Nucleo per Cybersicurezza. Tanto che nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, e può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Peraltro nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica, l'Agenzia per la cybersicurezza nazionale[9] applica una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti tenuti alla comunicazione dell'incidente informatico, significando anche la violazione della citata disposizione può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

L'obbligo di adeguarsi alle segnalazioni dell'Agenzia per la cybersicurezza nazionale

Merita particolare attenzione l'analisi dell'art 2 della legge 90/2024, il quale prevede che soggetti che hanno l'obbligo di comunicazione in caso di incidenti informatici e altri soggetti inclusi nel perimetro nazionale di cyber sicurezza nazionale, nonché quei soggetti facenti parte delle categorie "NIS" e "Tel.Co.", in caso di segnalazioni puntuali dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità, cui essi risultino potenzialmente esposti, devono provvedere, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Una norma molto importante essendo finalizzata a prevenire concretamente il rischio di eventuali incidenti informatici ovvero di attacchi hacker, per cui il CSIRT, facente parte della rete dei CSIRT degli stati membri che interloquisce costantemente con l'Agenzia dell'Unione Europea per la cybersicurezza, è in grado di monitorare le maggiori vulnerabilità dei sistemi in base all'analisi delle infrastrutture digitale tanto da evidenziarne tempestivamente le criticità per i sistemi di maggiore rilevanza nazionale, ma soprattutto a contrastare un rischio di propagazione sulle reti interconnesse dei servizi pubblici e di quelli di pubblica necessità. A riguardo la mancata o ritardata adozione degli interventi risolutivi richiesti dalla segnalazione fatta pervenire dall'ACN comporta l'applicazione di una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei manchevoli che sarà comminata dalla stessa Agenzia, salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate a tale ente, ne impediscano l'adozione o ne comportino il differimento oltre il termine di quindici giorni. Tra l'altro ai sensi dell'art 4 del testo l'Agenzia deve provvedere anche alla raccolta, all'elaborazione e alla classificazione dei dati relativi agli incidenti informatici segnalati, tali dati sono resi pubblici nell'ambito della relazione annuale in riferimento agli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza.

Le strutture e i referenti per la gestione della cybersicurezza nell'ambito dei soggetti tenuti alla notifica degli incidenti informatici.

I soggetti che hanno l'obbligo della notifica devono individuare una struttura, anche tra quelle esistenti, che provveda allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni, alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico e alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione. Tale struttura avrà cura di assicurare la produzione e l'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione, alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i citati piani, alla pianificazione e all'attua-

zione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale ed infine al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza. Presso le citate strutture, pertanto, dovrà operare il referente per la cybersicurezza, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Il referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale e va pertanto comunicato alla stessa Agenzia, la quale può individuare anche specifiche modalità e processi di coordinamento e di collaborazione tra le amministrazioni e tra i referenti per la cybersicurezza al fine di facilitare la resilienza delle amministrazioni pubbliche. Le strutture hanno il compito di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia, nonché quelle sulla conservazione delle password adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati. L'Agenzia per la cybersicurezza nazionale, in tale ambito, provvede allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici 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. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia che svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato.

La cybersicurezza pubblica diviene quindi uno degli obiettivi da perseguire in quanto fortemente correlata alla sicurezza nazionale, tanto che la legge estende le disposizioni del Decreto Legislativo 231/2001 ai reati informatici, aumentando le responsabilità degli enti pubblici e delle aziende riguardo alla sicurezza cibernetica, imponendo di fatto anche l'adozione di modelli di organizzazione, gestione e controllo che includano misure specifiche per prevenire e rilevare reati informatici.

Gli adempimenti per le aziende

Anche le aziende private sono soggette a una serie di obblighi previsti dalla nuova normativa, ad iniziare dall'adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio, dall'implementazione di misure di sicurezza, proporzionate alla natura dei dati trattati e alle minacce potenziali alla protezione dei dati personali e delle informazioni aziendali critiche. Altro aspetto rilevante è costituito dal fatto le aziende devono investire nella formazione del proprio personale in materia di sicurezza informatica, anche per sviluppare la consapevolezza dei rischi cibernetici e la capacità di affrontarli sono elementi fondamentali per prevenire incidenti di sicurezza, devono curare i programmi di formazione devono essere periodici e aggiornati in base alle nuove minacce e tecnologie. In tema di valutazione e gestione del rischio, le aziende devono effettuare regolarmente adeguate procedure per identificare e mitigare le vulnerabilità nelle loro infrastrutture IT, un processo che include l'analisi delle minacce, la valutazione delle vulnerabilità e l'implementazione di misure di mitigazione, che devono essere documentate e riesaminate periodicamente. Le aziende, infine, devono garantire la conformità alle normative vigenti, inclusa la nuova legge sulla Cybersicurezza, per evitare sanzioni e responsabilità legali sensi legge 231/2001, implicando l'adozione di politiche e procedure che assicurino il rispetto delle citate disposizioni legislative e dimostrando la conformità in caso di audit o ispezioni.

In conclusione la legge28 giugno 2024, n. 90 rappresenta un'importante evoluzione nella normativa italiana sulla cybersicurezza, imponendo un quadro di adempimenti che richiede un'attenta e rapida attuazione da parte di pubbliche amministrazioni e aziende. Le misure introdotte mirano a rafforzare la resilienza del nostro paese di fronte alle minacce cibernetiche sempre più sofisticate e frequenti, anche se l'adeguamento alla nuova normativa richiederà investimenti in tecnologia, formazione e processi, rappresenta un passo necessario per costruire un ecosistema digitale più sicuro e affidabile. La collaborazione tra il settore pubblico e quello privato sarà essenziale per affrontare le sfide poste dalla cybersicurezza in modo efficace e coordinato, in cui la nuova legge sulla cybersicurezza stabilisce un nuovo standard di protezione che, se adeguatamente implementato, contribuirà a rafforzare la fiducia nelle infrastrutture digitali del nostro paese e a garantire una ben più adeguata difesa contro le future minacce cibernetiche.

***Ufficiale dell'Arma dei Carabinieri**

1 - Entrata in vigore il 17 7 2024.
2- La nuova legge sulla cybersicurezza si caratterizza per un ambito di applicazione molto ampio, riguardando diverse tipologie di soggetti, tra cui: le pubbliche amministrazioni che devono implementare misure di sicurezza cibernetica conformi ai nuovi requisiti, tra questi vi sono anche i soggetti nel perimetro di sicurezza nazionale cibernetica, entità che comunque operano in settori critici per la sicurezza nazionale e che sono pertanto soggette a stringenti obblighi di sicurezza; i soggetti sottoposti alla Direttiva NIS e NIS2: organizzazioni che devono conformarsi agli standard europei di sicurezza delle reti e dei sistemi informativi di rilevante interesse pubblico e di pubblica necessità e gli organi dello Stato essenziali per la cybersicurezza: tra cui il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), gli Organismi di informazione per la Sicurezza e l'Agenzia per la Cybersicurezza Nazionale (ACN) con il suo Nucleo per la Cybersicurezza.
3 - Individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano.
4 - Mentre per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società in house che forniscono servizi informatici, i servizi di trasporto ovvero quelli di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali (ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991) o di gestione dei rifiuti (ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008), gli obblighi previsti dalla norma si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della legge allo scopo di dare un periodo di adeguamento alle nuove prescrizioni considerata la loro ridotta struttura organizzativa.
5 - Con le modalità e nei termini previsti dettagliatamente dal comma 2 dell'articolo della stessa legge. Mentre i soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati, al CSIRT Italia anche se le notifiche obbligatorie sono trattate prioritariamente rispetto alle notifiche volontarie e sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.
6 - Specificamente indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge.
7 -Che non si applica ai soggetti rientranti nel perimetro della cybersicurezza nazionale e agli organi dello Stato preposti alla prevenzione, accertamento e repressione dei reati, alla tutela dell'ordine e della sicurezza e della sicurezza e sicurezza militare, e agli organismi di informazione per la sicurezza, oltre che ai soggetti NIS (operatori dei servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali)
8 - Computer security incidente response team, un organo tecnico operativo di esperti deputato a compiere il monitoraggio degli incidenti a livello nazionale, l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti, e soprattutto interviene in caso di incidenti curandone l'analisi dinamica dei correlati rischi (interloquendo con l'Agenzia dell'Unione Europea per la cybersicurezza, facente parte della rete dei CSIRT degli stati membri).
9 - La stessa deve provvedere alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza, come prevede l'art 4 della legge 90/2024.
10 - La disciplina del procedimento sanzionatorio amministrativo dell'Agenzia è definita con regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi delle disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. Il regolamento è adottato, entro novanta giorni dalla data di entrata in vigore della legge, con decreto del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Fino alla data di entrata in vigore del regolamento di cui al presente comma, ai procedimenti sanzionatori si applicano, per ciascuna fase procedimentale di cui al primo periodo, le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 68
11 - Nel rispetto delle disposizioni dell'articolo 17, comma 4-quater, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, introdotto dall'articolo 11 della presente legge.
12 - Come prevede l'art. 3 della stessa legge dato che all'articolo 1 comma 3 bis dalla legge 18 novembre 2019, n. 133, il secondo periodo è sostituito dal seguente: «I medesimi soggetti provvedono a effettuare la segnalazione degli incidenti di cui al presente comma senza ritardo, comunque entro il termine massimo di ventiquattro ore, e ad effettuare la relativa notifica entro settantadue ore».
13 - Quegli operatori dei servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali meglio individuati dal decreto legislativo 18 maggio 2018, n. 65, e quelle imprese del settore delle telecomunicazioni che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico identificati dal decreto legislativo 1° agosto 2003, n. 259.
14 - I compiti pertinenti alla struttura ed al referente i compiti di cui ai commi 1 e 2 possono essere esercitati in forma associata secondo quanto previsto dall'articolo 17, commi 1-sexies e 1-septies, del codice di cui al decreto legislativo 7 marzo 2005, n. 82.
15 - Qualora i soggetti di cui all'articolo 1, comma 1, non dispongano di personale dipendente fornito di tali requisiti, possono conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, nell'ambito delle risorse disponibili a legislazione vigente. Peraltro la struttura e il referente possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.
16 - L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni.
17 - Ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge».