Nota di lettura

Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" pubblicata nella Gazzetta Ufficiale SG n. 153 del 2 luglio 2024

Considerazioni generali

La sicurezza informatica è ormai un tema ineludibile per tutte le Pubbliche Amministrazioni, di qualunque dimensione e livello amministrativo: il progressivo intensificarsi di attacchi di diversa natura, che siano finalizzati alla messa fuori uso dei sistemi informativi o all'estrazione fraudolenta di dati, rende ineludibile un rafforzamento delle difese cibernetiche, da attuarsi a livello regolamentare e, conseguentemente, operativo a livello di singolo ente.

Il tema, di conseguenza, assume centralità anche per i Comuni, le loro forme associate e le Città metropolitane che, pur gestendo dati i quali, secondo la classificazione della Strategia Nazionale di Cybersicurezza 2022-2026, vengono identificati "ordinari" e non "critici" o "strategici", sempre più spesso sono oggetto di attacchi ai propri sistemi informativi che causano grandi problemi alla gestione dell'attività amministrativa e all'erogazione dei servizi, fino a causarne il blocco per periodi prolungati.

In questo scenario, si inserisce il Decreto in esame, che vuole indirizzare e sensibilizzare anche i Comuni di grandi dimensioni, o comunque capoluogo di Regione, e loro in-house dedicate alla gestione di servizi e sistemi informatici, ovvero a servizi attinenti agli ambiti considerati all'interno del perimetro di sicurezza nazionale, verso l'individuazione di strutture dedicate alla resilienza cibernetica dell'ente.

Allo stato attuale, infatti, pur in presenza di casi virtuosi di singole amministrazioni comunali capaci di difendersi e rispondere agli attacchi in maniera efficace, per gli enti locali permane una generalizzata difficoltà ad attrezzarsi adeguatamente. I motivi principali che ostacolano l'adozione di adeguate misure di sicurezza, riassunti di seguito, non trovano, tuttavia, riscontro positivo nel testo in esame, rimanendo irrisolti, a meno dell'adozione di misure di supporto successive o in fase di decretazione attuativa:

- la carenza di risorse umane dipendenti con competenze tecniche adeguate, unita alla difficoltà a reperirne sul mercato di così specialistiche, anche a causa della bassa appetibilità, in termini retributivi, delle posizioni di lavoro all'interno dei Comuni;

- la ristrettezza di risorse di bilancio da dedicare a interventi organizzativi e sui sistemi informativi;
- l'impossibilità, quindi, di rispettare i dettami normativi e attuare le disposizioni previste ad invarianza finanziaria e di risorse umane, sia per le figure professionali richieste, sia per gli inevitabili adeguamenti informatici o rinnovi di licenze a nuove condizioni, necessari a rafforzare la resilienza cibernetica.

Ciò premesso, di seguito si procede con una sintetica nota di lettura dell'articolato di diretto impatto sui Comuni.

- **Art. 1 (obblighi di notifica di incidenti)**

Comma 1

L'ambito di applicazione del DDL in esame ricomprende, tra gli altri: i Comuni con popolazione superiore a 100.000 abitanti e comunque i Comuni capoluogo di Regione, le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nelle città metropolitane e le aziende sanitarie locali. Sono, inoltre, soggetti interessati dall'applicazione della norma anche le rispettive società in-house che forniscono servizi informatici, i servizi di trasporto pubblico su specificato, i servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali e i servizi di gestione dei rifiuti.

Per i soggetti su menzionati **vige l'obbligo di segnalazione e notifica all'Agenzia per la Cybersicurezza Nazionale degli incidenti,** come classificati nella tassonomia definita con determinazione tecnica del direttore generale dell'Agenzia, ai sensi dell'art. 1 comma 3-bis del DL 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133, che abbiano impatto su reti, sistemi informativi e servizi informatici.

Al momento la determinazione tecnica di definizione della tassonomia non risulta emanata.

Comma 2

I termini per la comunicazione all'Agenzia per la Cybersicurezza Nazionale per il tramite delle procedure disponibili sul sito istituzionale della stessa **sono, rispettivamente, di massimo 24 ore** dal momento in cui se ne è venuti a conoscenza **per la segnalazione e di massimo 72 ore per la notifica completa** di tutti gli elementi informativi disponibili.

Comma 3

Ai Comuni con popolazione superiore a 100.000 abitanti e comunque i Comuni capoluogo di Regione, alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, alle società di trasporto pubblico extraurbano operanti nelle città metropolitane, alle aziende sanitarie locali, nonché alle rispettive società in-house che forniscono servizi informatici, i

servizi di trasporto pubblico di cui al comma 1, i servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali e i servizi di gestione dei rifiuti, **gli obblighi previsti dai commi 1 e 2 si applicano a decorrere dal 180mo giorno successivo all'entrata in vigore della legge**.

Comma 4

Alle notifiche volontarie di incidenti da parte dei soggetti interessati dall'applicazione della norma, **al di fuori dei casi indicati nella tassonomia di cui al comma 1**, **si applicano le disposizioni** dell'art. 18, commi 3,4 e 5, del Dlgs 18 maggio 2018, n. 65 in attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (meglio nota come **Direttiva NIS**).

Commi 5 e 6

La reiterazione dell'inosservanza degli obblighi di segnalazione e notifica nell'arco di cinque anni comporterà l'applicazione da parte di una sanzione amministrativa pecuniaria da 25.000 a 125.000 euro a carico dei soggetti di cui al comma 1 **e la violazione degli obblighi di comunicazione può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.**

L'Agenzia per la Cybersicurezza Nazionale, nell'arco di dodici mesi successivi all'accertamento del ritardo o dell'inosservanza, può disporre l'invio di ispezioni, anche al fine di verificare l'attuazione di interventi di rafforzamento della resilienza cibernetica indicati direttamente dalla stessa o contenuti in Linee Guida da questa emanate. Le modalità di ispezione saranno disciplinate con determinazione del Direttore Generale dell'Agenzia, pubblicate sulla Gazzetta Ufficiale.

Si nota la mancanza di un coordinamento con l'articolo 18bis del Dlgs 82/2005 - Codice dell'Amministrazione Digitale – che attribuisce all'AgID poteri di vigilanza, verifica, controllo e monitoraggio sul rispetto delle disposizioni in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione, in parte trattate nel provvedimento in esame, inclusa l'irrogazione di sanzioni amministrativo-pecuniarie da 10.000 a 100.00 euro in caso di inadempienza da parte delle PPAA.

- **Art. 2 (Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la Cybersicurezza Nazionale)**

Commi 1 e 2

Tutti i soggetti di cui all'articolo 1, in caso di segnalazioni puntuali dell'Agenzia circa specifiche vulnerabilità a cui risultano potenzialmente esposti, **devono provvedere entro 15 giorni dalla segnalazione a dare seguito agli interventi risolutivi dalla stessa indicati. La mancata o ritardata adozione degli interventi risolutivi comporterà l'applicazione delle sanzioni previste dall'art. 1**

comma 6, a meno di motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'Agenzia, che ne impediscano l'adozione o ne comportino il differimento oltre il termine previsto.

Art. 8 (Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la Cybersicurezza)

Commi 1-2-3-4-5

I soggetti di cui all'art 1 comma 1 individuano, ove non già presente, una struttura, anche tra quelle esistenti, che provvede:

1. Allo sviluppo delle politiche e delle procedure di sicurezza.

2. Alla produzione e aggiornamento:

- di sistemi di analisi preventiva e di un piano per la gestione del rischio informatico;
- di un documento che definisca ruoli e organizzazione del sistema per la sicurezza informatica;
- di un piano programmatico per la sicurezza dei dati, sistemi e infrastrutture dell'amministrazione.

3. Alla pianificazione e attuazione:
- di interventi di potenziamento della capacità di gestione dei rischi informatici;
- dell'adozione delle misure di sicurezza previste nelle Linee Guida emanate dall'Agenzia per la cybersicurezza.

4. Al monitoraggio continuo delle minacce alla sicurezza e delle vulnerabilità dei sistemi.

All'interno di tale struttura opererà il referente per la cybersicurezza, dotato di comprovate competenze e professionalità in tema di cybersicurezza, che assumerà il ruolo di punto unico di contatto con l'Agenzia per la Cybersicurezza nazionale alla quale andrà comunicato il nominativo.

Qualora i soggetti di cui all'articolo 1 comma 1 non dispongano di tali figure professionali dipendenti **potranno conferire l'incarico di referente per la cybersicurezza ad un dipendente di altra Pubblica Amministrazione**, previa autorizzazione di quest'ultima ai sensi dell'art. 53 del d.lgs. 165/2001.

La struttura e il referente preposti alla cybersicurezza possono coincidere con quelli del Responsabile per la Transizione Digitale previsti dall'art. 17 del d.lgs. 82/2005, ai sensi del quale è possibile che i compiti assegnati possano essere svolti in forma associata.

L'Agenzia può individuare modalità e processi di collaborazione e coordinamento tra i soggetti di cui all'articolo 1 comma 1 e i referenti per la cybersicurezza al fine di facilitare la resilienza delle Pubbliche Amministrazioni.

- **Art. 9 (Rafforzamento delle misure di sicurezza dei dati attraverso la crittografia)**

Le strutture preposte alle funzioni in tema di cybersicurezza devono 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, al fine di evitare che i dati cifrati siano intellegibili e disponibili a terzi.

Rimane aperto il tema di come si debba procedere una volta che certi asset (sistemi, programmi, applicativi, servizi, ecc.) **non superino la verifica** specialmente per ambienti preesistenti e già in esercizio.

- **Art. 11 (Procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale)**

Con Decreto del Presidente della Repubblica, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari, **da emanarsi entro 90 giorni dall'entrata in vigore del presente decreto legge**, **viene adottato un regolamento che individua i termini, le modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza nonché l'irrogazione delle relative sanzioni di competenza dell'Agenzia**, disciplinando di conseguenza il procedimento sanzionatorio amministrativo dell'Agenzia. **Fino all'entrata in vigore del suddetto regolamento**, **si applica** quanto previsto dalle Sezioni I, II, III del Capo I della Legge 24 novembre 1981, **n. 689 recante "Modifiche al sistema penale".**

- **Art. 14 (Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e misure di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)**

Comma 1

Entro 120 giorni dall'entrata in vigore del provvedimento in esame **è prevista l'emanazione di un decreto del Presidente del Consiglio dei Ministri su proposta dell'Agenzia per la Cybersicurezza nazionale, previo parere del Comitato interministeriale per la Sicurezza della Repubblica**, **che disciplini**, per specifiche categorie tecnologiche di beni e servizi informatici, **gli elementi essenziali di cybersicurezza che le PPAA, i gestori di servizi pubblici e le società a controllo pubblico** (come indicati all'art. 2 comma 2 del Dlgs 82/2005 recante il Codice dell'Amministrazione Digitale) **dovranno tenere in considerazione nell'approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e nei casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane, EU, NATO o Paesi Terzi tra quelli rientranti in Accordi di collaborazione con Paesi EU o NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, individuati dal decreto su menzionato.**

Comma 2

Nei casi individuati dal comma 1, le stazioni appaltanti, incluse le centrali di committenza:

- possono esercitare la facoltà di non aggiudicare l'appalto all'offerente che ha presentato l'offerta economicamente più vantaggiosa (articolo 107 comma 2 del Codice degli Appalti), o di non procedere all'aggiudicazione (articolo 108 comma 10 del Codice degli Appalti se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati dal decreto;
- tengono sempre in considerazione tali elementi essenziali nella valutazione dell'elemento qualitativo nell'individuazione del miglior rapporto qualità/prezzo nell'aggiudicazione;
- inseriscono gli elementi essenziali di cybersicurezza tra i requisiti minimi dell'offerta, in caso sia utilizzato il criterio del minor prezzo;
- nel caso del criterio dell'offerta economicamente più vantaggiosa, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità/prezzo stabiliscono un tetto massimo per l'elemento economico entro il 10%;
- prevedono criteri di premialità per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane, EU, NATO o Paesi Terzi tra quelli rientranti in Accordi di collaborazione con Paesi EU o NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Comma 4

Restano ferme le disposizioni previste dal DL 105/2019 nei casi di approvvigionamento di beni, sistemi e servizi ICT destinati ad essere impiegati nelle reti e nei sistemi informativi da parte dei soggetti inseriti nel perimetro di sicurezza nazionale

Dato il perimetro di applicazione, al netto di ulteriori specifiche in sede di decretazione attuativa, non si ritiene che l'articolo si applichi nel concreto agli enti locali, in quanto non interessati dalla gestione diretta di interessi nazionali strategici, né gestori diretti accordi con la NATO o l'Unione Europea per la gestione di informazioni classificate o ancora di ricerca e innovazione.

CAPO II

DISPOSIZIONI PER LA PREVENZIONE E IL CONTRASTO DEI REATI INFORMATICI NONCHÉ IN MATERIA DI COORDINAMENTO DEGLI INTERVENTI IN CASO DI ATTACCHI A SISTEMI INFORMATICI O TELEMATICI E DI SICUREZZA DELLE BANCHE DATI.

Gli articoli da 16 a 23 modificano il Codice penale e di Procedura penale nonché ulteriori norme di settore al fine di potenziare i controlli in materia di cybersicurezza e inasprire le pene e le sanzioni previste in caso di attacco informatico. In generale si tratta di disposizioni perlopiù riferite a

responsabilità individuali e che non hanno un impatto diretto sull'amministrazione comunale, ma, eventualmente, sui singoli.

Art. 24 (Disposizioni finanziarie)

Comma 1

L'articolo sancisce che dall'attuazione delle disposizioni del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le pubbliche amministrazioni adempiono ai compiti sanciti nel decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Comma 2

I proventi dal regime sanzionatorio di cui all'articolo 1 comma 6 confluiranno nelle entrate dell'Agenzia per la Cybersicurezza.