ALERT MEMORANDUM

L'entrata in vigore della Legge sulla Cybersicurezza

25 luglio 2024

Il 17 luglio u.s. è entrata in vigore la Legge n. 90/2024 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (c.d. "**Legge sulla Cybersicurezza**").

La novella rappresenta un passo in avanti verso il rafforzamento della *cybersicurezza* nazionale, considerato l'allarmante aumento di attacchi informatici registrato nell'ultimo anno[1].

Infatti, la Legge sulla Cybersicurezza, fra l'altro:

(i) mira ad incrementare la resilienza delle pubbliche amministrazioni, degli operatori soggetti all'applicazione della normativa in materia di Perimetro di Sicurezza Nazionale Cibernetica ("**Perimetro**"), dei destinatari del D.lgs. n. 65/2018 (decreto di recepimento della Direttiva UE 2016/1148 ("**NIS 1**") e degli operatori che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (i "**soggetti Tel.co.**"), stabilendo anche precise regole per la contrattualizzazione pubblica di beni e servizi informatici cruciali per la protezione degli interessi strategici nazionali;

(ii) prescrive nuovi obblighi di notifica degli incidenti informatici;

(iii) potenzia il ruolo dell'Agenzia per la Cybersicurezza Nazionale ("**ACN**");

(iv) rafforza le misure di sicurezza dei dati istituendo il Centro nazionale di crittografia; e

(v) opera una stretta significativa in materia di contrasto ai reati informatici, inasprendo le pene per i delitti esistenti e introducendo nuove fattispecie di reato, con effetti tanto per le persone fisiche quanto per gli enti, ai sensi del D.lgs. 231/2001 ("**Decreto 231**").

La Legge sulla Cybersicurezza si integra e coordina con la normativa *cybersecurity* vigente, tra cui la normativa in materia di Perimetro (D.L. n. 105/2019) [2], il Regolamento DORA (Regolamento UE 2022/2554) e il D.lgs. n. 65/2018, di recepimento della Direttiva NIS 1[3].

Per domande relative ai temi discussi in questa nota, potete contattare qualsiasi avvocato del nostro studio con cui siete abitualmente in contatto o gli autori di seguito indicati.

ROMA

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

Andrea Mantovani
+39 06 6952 2804
amantovani@cgsh.com

Bernardo Massella Ducci Teri
+39 06 6952 2290
bmassella@cgsh.com

Federica Mammì Borruto
+39 06 6952 2826
fmammiborruto@cgsh.com

Marco Accorroni
+39 06 6952 2320
maccorroni@cgsh.com

Paola Maria Onorato
+39 06 6952 2654
ponorato@cgsh.com

MILANO

Giulia Checcacci
+39 02 7260 8224
gcheccacci@cgsh.com

Elena Galimberti
+39 02 7260 8670
egalimberti@cgsh.com

[1] Secondo il Rapporto pubblicato dall'Associazione Italiana per la Sicurezza Informatica CLUSIT 2024, nel 2023 gli attacchi sono aumentati dell'11% a livello globale e del 65% a livello italiano.

[2] Unitamente ai relativi decreti attuativi: DPCM 30 luglio 2020, n. 131, DPR 5 febbraio 2021, n. 54, DPCM 14 aprile 2021, n. 81, D.L. 14 giugno 2021, n. 82, DPCM 15 giugno 2021, DPCM 18 maggio 2022, n. 92 e alla Determina ACN del 3 gennaio 2023.

[3] La Legge sulla Cybersicurezza non fa invece specifico riferimento alla Direttiva NIS 2 (Direttiva UE 2022/2055), che gli Stati Membri sono obbligati a recepire entro il 17 ottobre 2024.

1. AMBITO DI APPLICAZIONE

Principali destinatari degli obblighi introdotti dalla Legge sulla Cybersicurezza sono le Pubbliche Amministrazioni [4] nonché le società *in house* che forniscono alle Pubbliche Amministrazioni servizi informatici, servizi di trasporto, servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali e servizi di gestione dei rifiuti ("**Soggetti Pubblici**"). In particolare, l'inclusione delle società *in house* tra i destinatari della legge mostra la crescente attenzione prestata dal legislatore nei loro confronti, quali infrastrutture critiche e parti indispensabili della *supply chain*, le cui vulnerabilità possono incidere sull'intera catena di approvvigionamento di beni e servizi.

Inoltre, la novella legislativa estende alcuni degli obblighi introdotti anche agli operatori di servizi essenziali e ai fornitori di servizi digitali, così come definiti nella direttiva NIS 1 (articolo 3, comma 1, lettere g) e i), recepita in Itala con il D.lgs. n. 65/2018) (i "**Soggetti NIS 1**"), ai soggetti Tel.co. nonché agli operatori inclusi nel Perimetro.

2. OBBLIGO DI NOTIFICA

L'art. 1 della Legge sulla Cybersicurezza introduce obblighi di notifica degli incidenti informatici in capo ai Soggetti Pubblici.

Questi sono tenuti a segnalare all'ACN tutti gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici indicati nella tassonomia di cui alla determina dell'ACN del 3 gennaio 2023 [5].

Una prima segnalazione deve avvenire entro 24 ore dal momento in cui i Soggetti Pubblici sono venuti a conoscenza dell'incidente e la notifica deve essere completata entro il termine massimo di 72 ore, a decorrere dal medesimo momento, con tutte le informazioni disponibili, utilizzando i canali di cui al sito internet dell'ACN.

I Soggetti Pubblici possono inoltre effettuare notifiche volontarie aventi ad oggetto tipologie di incidenti non inclusi nella tassonomia. In tal caso, le notifiche sono trattate in subordine rispetto a quelle obbligatorie e solo se il loro trattamento da parte del Computer Security Incident Response Team Italia presso l'ACN non costituisce un onere sproporzionato o eccessivo. Tali notifiche volontarie non possono, in ogni caso, imporre al soggetto notificante alcun obbligo a cui lo stesso non sarebbe stato sottoposto in assenza di tale notifica [6].

In caso di inosservanza dell'obbligo di notifica, il comma 5 dell'articolo in commento prevede l'invio da parte dell'ACN di apposita comunicazione al Soggetto Pubblico volta ad informarlo che la reiterazione dell'inosservanza nell'arco di 5 anni comporterà l'applicazione della sanzione amministrativa pecuniaria da €25.000 a €125.000. Inoltre, l'ACN potrà effettuare ispezioni nei 12 mesi successivi all'accertamento del ritardo o dell'omissione anche per verificare che i Soggetti Pubblici interessati abbiano attuato interventi di rafforzamento della resilienza rispetto al rischio di incidenti.

L'obbligo di notifica in commento è applicabile a decorrere dalla data di entrata in vigore della Legge sulla Cybersicurezza alle pubbliche amministrazioni centrali incluse nell'elenco ISTAT, alle regioni e province autonome di Trento e di Bolzano nonché alle città metropolitane. Per tutti gli altri Soggetti Pubblici, l'obbligo sarà applicabile a decorrere dal 180° giorno dall'entrata in vigore della Legge sulla Cybersicurezza.

È importante sottolineare che, con l'introduzione della disposizione in esame, l'obbligo di notifica viene esteso anche a soggetti ulteriori rispetto a quelli già ricompresi nel Perimetro e, attraverso la modifica apportata al comma 3-*bis* dell'art. 1 del D.L. 105/2019 (istitutivo del Perimetro), le modalità e i tempi di notifica di cui alla Legge sulla Cybersicurezza (segnalazione entro 24 ore e notifica entro 72 ore) vengono estesi anche agli incidenti che impattano su reti, sistemi anche informativi e servizi informatici diversi dai beni ICT [7] ma che sono comunque di

[4] In particolare, nel contesto della Legge sulla Cybersicurezza, sono considerate pubbliche amministrazioni: le pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni; le regioni e 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; 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.

[5] Cfr. https://www.gazzettaufficiale.it/eli/id/2023/01/10/23A00114/sg.

[6] Cfr. Articolo 18, commi 3, 4 e 5 del D.lgs. 65/2018.

[7] Definiti, ai sensi dell'art. 1. lett. m) del DPCM 131/2020 come un "*insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura, considerato unitariamente ai fini dello svolgimento di*

pertinenza di soggetti inclusi nel Perimetro stesso.

Sono esclusi dall'applicazione della disposizione in commento i Soggetti NIS 1, i soggetti inclusi nel Perimetro per quanto riguarda gli incidenti impattanti sui beni ICT (per cui rimane applicabile quanto previsto nella normativa sul Perimetro) nonché gli organi statali preposti alla sicurezza pubblica e militare, il Dipartimento delle informazioni per la sicurezza, e le Agenzie di informazione e sicurezza esterna e interna.

3. RISOLUZIONE DELLE VULNERABILITÀ SEGNALATE DALL'ACN

La Legge sulla Cybersicurezza definisce le modalità di gestione delle segnalazioni di specifiche vulnerabilità comunicate dall'ACN ai seguenti soggetti (elencati nell'art. 2): i Soggetti Pubblici, i soggetti inclusi nel Perimetro, i Soggetti NIS 1 e i soggetti Tel.co.

In particolare, l'ACN può segnalare specifiche vulnerabilità cui i soggetti sopra indicati risultano potenzialmente esposti affinché questi provvedano tempestivamente (e, comunque, non oltre 15 giorni) all'adozione degli interventi risolutivi indicati dalla stessa ACN, salvo che motivate esigenze di natura tecnico-organizzativa ne impediscano l'adozione o ne comportino il differimento oltre il termine indicato.

Il mancato rispetto di quanto prescritto nella segnalazione comporta l'applicazione della sanzione amministrativa pecuniaria da €25.000 a €125.000.

4. REFERENTE PER LA CYBERSICUREZZA

I Soggetti Pubblici sono, inoltre, tenuti a dotarsi di una struttura per la *cybersicurezza* e a designare un referente per la *cybersicurezza*, individuato in ragione di specifiche competenze in materia e preposto a fungere quale punto di contatto nei rapporti con l'ACN (il suo nominativo deve essere infatti comunicato all'ACN).

Ulteriori obblighi in proposito ricalcano quelli già previsti per i soggetti inclusi nel Perimetro, es., l'adozione di *policy* e procedure interne di sicurezza delle informazioni, la predisposizione e l'aggiornamento di un piano di gestione del rischio informatico, la definizione di ruoli e responsabilità, la pianificazione e l'attuazione di interventi di potenziamento per la gestione dei rischi informativi, l'attuazione delle misure indicate dalle linee guida che saranno pubblicate dall'ACN nonché l'obbligo di costante monitoraggio delle minacce alla sicurezza e alla vulnerabilità dei sistemi, al fine di provvedere al pronto aggiornamento della sicurezza, ove necessario.

5. RAFFORZAMENTO DELLE MISURE DI SICUREZZA DEI DATI

Per i Soggetti Pubblici, nonché per i soggetti inclusi nel Perimetro e per i Soggetti NIS 1 è previsto l'obbligo di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica utilizzino soluzioni crittografiche conformi alle linee guida sulla crittografia e sulla conservazione delle *password* stabilite dall'ACN e dall'Autorità Garante per la protezione dei dati personali. In particolare, al fine di non rendere accessibili a terzi i dati cifrati, i predetti soggetti devono anche verificare che le applicazioni e i programmi interessati dalla norma non contengano vulnerabilità note.

Per garantire il rispetto di tale obbligo, vengono rafforzati i compiti dell'ACN, chiamata a promuovere l'uso della crittografia attraverso una sezione dedicata della strategia nazionale di *cybersicurezza*. Questo include lo sviluppo e la diffusione di *standard*, linee guida e raccomandazioni per rafforzare la sicurezza dei sistemi informatici, la valutazione della sicurezza dei sistemi crittografici e la gestione di attività informative per promuovere l'utilizzo della crittografia come strumento di sicurezza cibernetica.

A questo scopo, è istituito il Centro nazionale di crittografia presso l'ACN, regolato da provvedimenti del direttore generale dell'ACN.

6. CONTRATTI CON PROVIDER TECNOLOGICI

Nel caso di approvvigionamento di specifiche categorie di beni, sistemi e servizi ICT impiegati in un contesto connesso alla tutela di interessi nazionali strategici, le pubbliche amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico[8], nonché i soggetti inclusi nel Perimetro dovranno tenere in considerazione elementi essenziali di *cybersecurity*, ossia criteri e regole tecniche che i beni e servizi informatici da acquisire devono rispettare per

funzioni essenziali dello Stato o per l'erogazione di servizi essenziali".

[8] Come definite all'art. 2, comma 2 del Codice dell'amministrazione digitale (D.Lgs. 82/2005).

garantire la confidenzialità, l'integrità e la disponibilità dei dati da trattare. Tali elementi essenziali dovranno essere individuati con DPCM da adottarsi entro 120 giorni dall'entrata in vigore della Legge sulla Cybersicurezza.

L'obbligo introdotto si affianca a quello già previsto in materia di approvvigionamento dei beni ICT per i soggetti inclusi nel Perimetro, destinatari dell'obbligo di avviare il processo di valutazione da parte del Centro di Valutazione e Certificazione Nazionale ("**CVCN**"), per verificare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del Perimetro e appartenenti alle categorie individuate dal DPCM del 15 giugno 2021. A seguito dell'entrata in vigore della Legge sulla Cybersicurezza, i soggetti inclusi nel Perimetro dovranno quindi valutare anche gli elementi di *cybersecurity* previsti dal predetto DPCM per quei beni e servizi informatici non soggetti alla valutazione del CVCN.

7. PRECLUSIONI IN MATERIA DI ASSUNZIONE DEL PERSONALE

La Legge sulla Cybersicurezza introduce una serie di preclusioni in materia di assunzione, da parte di soggetti privati, del personale che abbia ricoperto specifici ruoli presso alcune pubbliche amministrazioni centrali, il cui mancato rispetto comporta la nullità del contratto stipulato (artt. 12 e 13).

Ad esempio, la Legge sulla Cybersicurezza prevede che i dipendenti dell'ACN che abbiano partecipato a specifici percorsi formativi di specializzazione nell'interesse e a spese della stessa ACN non possano assumere incarichi presso soggetti privati per svolgere mansioni in materia di *cybersicurezza* per un periodo di due anni decorrenti dall'ultimo percorso formativo.

8. AMPLIAMENTO DELL'AMBITO DI APPLICAZIONE DEL REGOLAMENTO DORA

La Legge sulla Cybersicurezza apporta, infine, modifiche alla legge di delegazione europea per l'adeguamento della normativa nazionale ad alcune disposizioni del Regolamento DORA.

In particolare, viene ampliato il novero dei soggetti interessati dall'applicazione del Regolamento DORA ricomprendendovi, oltre alle "entità finanziare", anche gli intermediari finanziari [9] e Poste Italiane S.p.A. per l'attività del Patrimonio Bancoposta.

Tale modifica è volta a conseguire un elevato livello di resilienza operativa digitale e ad assicurare la stabilità del settore finanziario nel suo complesso. Di conseguenza, nell'esercizio della delega, il Governo dovrà apportare le occorrenti modifiche e integrazioni alla disciplina applicabile ai predetti soggetti, al fine di rendere i presidi in materia di resilienza operativa equivalenti a quelli del Regolamento DORA, tenendo conto del principio di proporzionalità e delle attività svolte dai destinatari, nonché attribuendo a Banca d'Italia l'esercizio nei confronti di questi soggetti di poteri di vigilanza, di indagine e sanzionatori.

9. LE PRINCIPALI MODIFICHE IN MATERIA DI REATI INFORMATICI

Con la Legge sulla Cybersicurezza, il legislatore ha inteso anche rafforzare la lotta alla criminalità informatica, apportando importanti modifiche al codice penale e a quello di procedura penale.

Quanto alle modifiche che interessano il codice penale, giova segnalare:

- il generale inasprimento del trattamento sanzionatorio previsto per i delitti informatici, operato in particolare mediante:
  - un significativo aumento delle pene previste per la quasi totalità dei reati esistenti (tra cui quello di accesso abusivo ai sistemi informatici ai sensi dell'art. 615-ter c.p. e di danneggiamento di informazioni, dati e programmi informatici ex art. 635-bis c.p.);
  - l'introduzione di nuove circostanze aggravanti (come quella applicabile ove il fatto sia commesso "*da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema*", adesso estesa a tutte le fattispecie oggetto di riforma, o la nuova circostanza aggravante prevista per il reato di truffa nei casi in cui il fatto sia

[9] Iscritti all'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al D.lgs. 385/1993.

commesso a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui identificazione [10]) e la ridefinizione (con aumento delle pene) delle circostanze aggravanti già previste;

- l'introduzione di due nuove circostanze attenuanti (artt. 623-*quater* e 639-*ter* c.p.) dal medesimo contenuto ma ciascuna applicabile a specifici reati informatici[11], che prevedono in particolare (i) una diminuzione della pena fino a un terzo, quando il fatto possa considerarsi di lieve entità "*per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo*"; (ii) una diminuzione della pena dalla metà a due terzi, ove il reo si adoperi per evitare che dal reato derivino ulteriori conseguenze, anche fornendo concretamente aiuto alle autorità nella raccolta delle prove o nel recupero dei proventi del reato o degli strumenti utilizzati per commetterlo;

- l'abrogazione del reato di cui all'art. 615-*quinquies* c.p. (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) e la sua sostituzione con il nuovo delitto *ex* art. 635-*quater.*1 c.p.[12];

- l'introduzione del nuovo reato di estorsione informatica (nuovo art. 629, comma 3, c.p.), che punisce con la reclusione da sei a dodici anni e con la multa da 5.000 a 10.000 euro (pene aumentabili in presenza di determinate circostanze aggravanti[13]) chiunque, mediante la commissione di specifici reati informatici[14] o con la minaccia di compierli, costringe taluno a fare o a omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno. La nuova fattispecie potrebbe ad esempio applicarsi in tutti quei in casi in cui un soggetto, dopo aver violato un sistema informatico e aver manipolato e danneggiato informazioni, dati o programmi, richieda un riscatto per il ripristino del sistema stesso e dei relativi dati.

L'accentuato disvalore che la nuova Legge sulla Cybersicurezza intende attribuire ai reati informatici è reso evidente anche dalle modifiche che tale legge apporta al codice di procedura penale, prevedendo in particolare per tali reati: (i) l'attribuzione della competenza delle indagini preliminari alla procura distrettuale; (ii) l'applicazione del regime "semplificato" per la concessione della proroga dei termini per le indagini preliminari[15]; (iii) l'estensione del termine di durata massima per le indagini preliminari a 2 anni.

10. GLI INTERVENTI SUL DECRETO 231 E LE CONSEGUENZE PER LE SOCIETÀ

Le novità più significative per le imprese risiedono senza dubbio nelle modifiche che la Legge sulla Cybersicurezza apporta al Decreto 231, su un duplice fronte:

- da una parte, quello dell'inasprimento delle sanzioni pecuniarie previste nei confronti dell'ente dall'art. 24-*bis* del Decreto 231, dedicato ai reati informatici, che passano (i) per quanto riguarda i reati di cui al comma 1[16], da

[10] Nuovo comma 2-*ter*) dell'art. 640 c.p.

[11] In particolare, l'art. 623-*quater* c.p. si applica ai delitti di cui agli artt. 615-*ter* (Accesso abusivo ad un sistema informativo o telematico), 615-*quater* (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 617-*quater* (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche), 617-*quinquies* (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche) e 617-*sexies* c.p. (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche), mentre l'art. 639-*ter* c.p. trova applicazione per i delitti di cui agli artt. 629, terzo comma (nuova fattispecie di estorsione informatica), 635-*ter* (Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico), 635-*quater.*1 (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) e 635-*quinquies* c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità).

[12] Tale nuova fattispecie riporta la medesima rubrica e punisce la medesima condotta prevista e punita dal previgente art. 615-*quinquies* c.p., prevedendo altresì le stesse sanzioni, con la sola aggiunta di un aumento di pena nel caso in cui ricorrano le circostanze aggravanti di cui all'art. 615-*ter*, comma 2, n. 1) e comma 3, c.p.

[13] In particolare, è prevista la pena della reclusione da otto a ventidue anni e la multa da 6.000 a 18.000 euro in presenza delle circostanze aggravanti di cui al terzo comma dell'art. 628 c.p. (ovvero le circostanze aggravanti previste per il delitto di rapina) e nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o infermità.

[14] Ovvero quelli di cui agli artt. 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis* (Danneggiamento di informazioni, dati e programmi informatici), 635-*quater* (Danneggiamento di sistemi informatici o telematici) e 635-*quinquies* c.p.

[15] Si tratta, in particolare, del regime previsto dall'art. 406, comma 5-bis), c.p.p., che deroga all'ordinario regime per la concessione della proroga dei termini per lo svolgimento delle indagini preliminari, prevedendo che il giudice provveda con ordinanza entro dieci giorni dalla presentazione della richiesta di proroga. Tale disciplina derogatoria, riservata alle fattispecie di particolare gravità, è volta a consentire un accertamento più tempestivo ed efficace della commissione del reato.

[16] Ovvero le fattispecie di cui agli artt. 615-*ter*, 617-*quater*, 617-*quinquies*,

una cornice edittale ricompresa tra 100 e 500 quote ad una ricompresa tra 200 e 700 quote (per un massimo pari a 1.084.300 euro); (ii) per le fattispecie di cui al comma 2[17], da una sanzione fino a 300 quote ad una fino a 400 quote (per un massimo pari a 619.600 euro)[18];

- dall'altra, quello dell'estensione del catalogo dei reati presupposto della responsabilità degli enti, mediante l'inclusione della nuova fattispecie di estorsione informatica (nuovo art. 24-*bis*, comma 1-*bis*), Decreto 231) punita con sanzione pecuniaria da 300 a 800 quote (per un massimo di 1.239.200 euro) e con le sanzioni interdittive previste dall'art. 9, comma 2, del Decreto 231 (interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la Pubblica Amministrazione; esclusione da agevolazioni, finanziamenti, contributi e sussidi con eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi) per una durata non inferiore a due anni.

Alla luce dell'ampliamento dei reati presupposto della responsabilità degli enti, le imprese dovranno considerare la necessità di aggiornare i propri modelli organizzativi *ex* Decreto 231, valutando l'inserimento di ulteriori e specifici strumenti di controllo in aggiunta a quelli eventualmente già presenti per prevenire la commissione dei reati informatici già inclusi tra i reati presupposto (che astrattamente potrebbero già rappresentare un presidio anche con riferimento alla fattispecie di nuova introduzione). Si pensi, ad esempio, a tutte le misure volte a garantire il corretto utilizzo degli strumenti informatici aziendali, il rispetto degli standard di sicurezza con riguardo all'identità degli utenti e all'integrità e confidenzialità dei dati, il monitoraggio sull'utilizzo della rete aziendale da parte dei dipendenti, nonché le specifiche attività di informazione e formazione in favore della popolazione aziendale.

11. CONCLUSIONI

La nuova Legge sulla Cybersicurezza, pur inserendosi in un complesso quadro normativo che necessiterà di ulteriori modifiche anche nel breve termine (basti considerare, a tal riguardo, che già ad ottobre 2024 dovrà essere data attuazione alla Direttiva NIS 2) rappresenta comunque una concreta risposta al repentino e consistente aumento delle minacce cibernetiche.

In particolare, l'ampliamento degli obblighi di notifica di incidenti anche in capo a nuovi soggetti, nonché l'estensione dei nuovi e più stringenti tempi di notifica anche agli incidenti non impattanti sui beni ICT mira ad estendere e a rafforzare la resilienza e la sicurezza informatica nazionale, per garantire un maggior controllo da parte delle stesse infrastrutture critiche coinvolte.

Anche l'inasprimento delle pene per i reati informatici, l'introduzione di nuove fattispecie di reato e le rilevanti novità in materia di responsabilità degli enti ai sensi del Decreto 231 s'inseriscono nella medesima ottica, mirando in particolare ad arginare – con quale concreta efficacia, è ancora presto per dirlo – il fenomeno dei *cybercrime*.

CLEARY GOTTLIEB

635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* c.p.

[17] Ovvero le fattispecie di cui agli artt. 615-*quater* e 635-*quater.1* c.p.

[18] Restano invece invariate le sanzioni interdittive previste dalla norma per tali fattispecie.