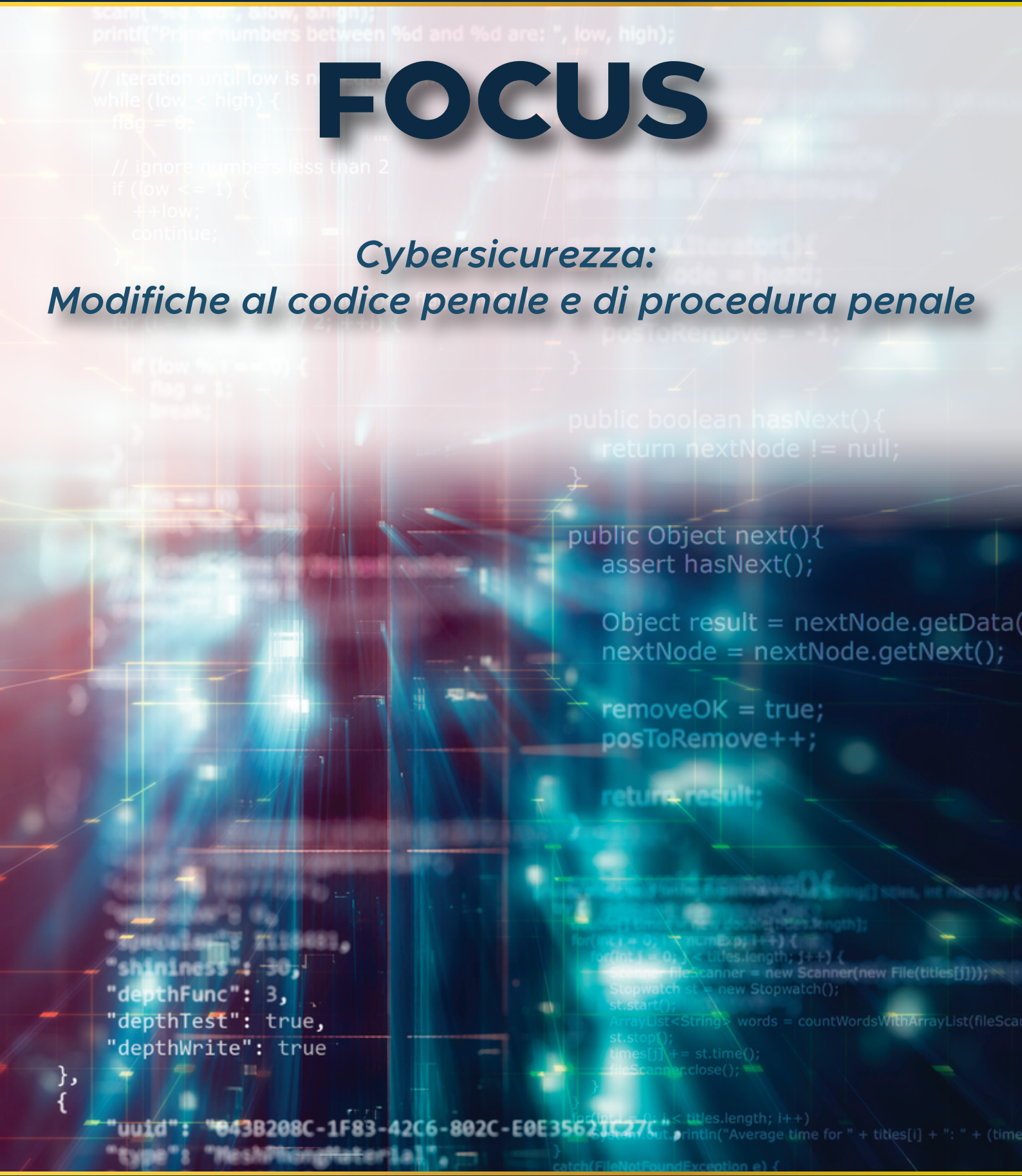
FORNARI E ASSOCIATI

STUDIO LEGALE

FOCUS

Cybersicurezza: Modifiche al codice penale e di procedura penale



fornarieassociati.com

Milano•Roma•Bari

Giugno 2024

PREMESSA.

1.411 sono gli attacchi *cyber* rilevati nel 2023 e trattati dall'Agenzia per la Cybersicurezza Nazionale.

Un dato che indica un incremento del 29% rispetto al 2022.

Questi sono soltanto alcuni dei numeri forniti dalla citata Agenzia nella propria relazione annuale al Parlamento, che ci consentono di tratteggiare una – seppur parziale – panoramica sul fenomeno della criminalità informatica.

Un fenomeno in crescita sia a livello globale sia a livello nazionale, la cui complessità e pericolosità rivela come sia necessario un coordinamento degli interventi – non solo normativi – che permettano di farvi fronte in maniera efficiente ed efficace.

È in questo contesto che si inserisce la c.d. "Legge sulla Cybersicurezza".

Pubblicata sulla Gazzetta Ufficiale n. 153 del 2 luglio 2024, la Legge n. 90 del 2024 persegue uno scopo ben preciso: rafforzare il sistema di cybersicurezza nazionale e prevenire nonché contrastare la commissione di reati informatici.

1. LA LEGGE SULLA CYBERSICUREZZA: IN GENERALE.

Ispirato dal menzionato obiettivo, il provvedimento di recente approvazione si compone complessivamente di 24 articoli, suddivisi in due Capi.

Il primo reca una serie di disposizioni orientate a garantire una migliore capacità di protezione dagli attacchi informatici e a fornire una risposta efficiente dinnanzi a queste emergenze.

In tale ottica, ad esempio, la Legge prevede l'introduzione di obblighi di segnalazione di alcuni tipi di incidenti informatici che abbiano impatto su reti, sistemi informativi e servizi informatici.

Il secondo Capo, che racchiude gli articoli dal 16 al 24, contiene le "*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 di dati in uso presso gli uffici giudiziari*".

In tale sezione trovano, dunque, spazio tutte le modifiche che la Legge ha inteso apportare tanto al Codice Penale, quanto al Codice di Procedura Penale e al D.Lgs. n. 231/2001, al fine di fronteggiare la commissione dei reati informatici.

Volgendo lo sguardo a questo secondo Capo, nei paragrafi che seguono si cercherà di analizzare più dettagliatamente gli interventi della c.d. Legge sulla Cybersicurezza in ambito penalistico.

2. QUALI SONO GLI INTERVENTI AL CODICE PENALE?

Nell'art. 16 sono elencate le novità introdotte dal recente testo di legge al Codice Penale.

Tale disposizione prevede:

- *(i)* l'introduzione di nuove fattispecie di reato, come ad esempio la c.d. "estorsione informatica", disciplinata dall'art. 629, comma 3 c.p.;
- *(ii)* l'aumento delle pene e l'introduzione di circostanze aggravanti ulteriori

rispetto a quanto già previsto dall'attuale Codice Penale.

Sul punto, si può menzionare l'inasprimento del regime sanzionatorio che ha interessato tanto il reato di danneggiamento di informazioni, dati e programmi informatici, tanto quello di accesso abusivo ai sistemi informatici, di cui si dirà meglio a breve.

Se da un lato, dunque, il legislatore – mosso dall'intento di prevenire e contrastare i reati informatici – ha ampliato le fattispecie di reato ovvero aggravato il trattamento sanzionatorio di ipotesi di reato già esistenti, dall'altro lato è intervenuto individuando nuove circostanze attenuanti.

Deputati alla loro disciplina gli articoli 623-*quater* c.p. e 639-*ter* c.p.

Volte ad applicarsi a reati informatici differenti, le norme sopra citate statuiscono che le pene debbano essere diminuite "*quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità*".

Non solo: entrambe le disposizioni prescrivono, altresì, una riduzione della pena dalla metà a due terzi per colui che si adoperi per evitare le conseguenze ulteriori derivanti dall'azione delittuosa, anche fornendo concretamente il proprio aiuto alle autorità; un aiuto che può concretizzarsi nella raccolta di elementi di prova ovvero nell'identificazione degli strumenti utilizzati per la commissione del reato.

2.1 In particolare: l'estorsione informatica.

Come accennato nel paragrafo precedente, al fine di fronteggiare il fenomeno della criminalità informatica, la Legge n. 90/2024 introduce nel Codice Penale nuove fattispecie delittuose.

Tra queste, la c.d. estorsione informatica.

Disciplinata dall'art. 629, comma 3 c.p., la nuova ipotesi di reato punisce l'estorsione posta in essere mediante la commissione di taluni reati informatici ovvero mediante la minaccia di compiere questi ultimi.

Sulla base della fattispecie di nuovo conio, sarà, quindi, punibile con la reclusione da sei a dodici anni e con la multa da euro 5.000 ad euro 10.000, colui che – ad esempio – accedendo abusivamente ad un sistema informatico o telematico, costringa qualcuno a fare o omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con danno altrui.

Il recente provvedimento, dunque, costruisce una nuova fattispecie criminosa, sanzionandola più aspramente dell'estorsione semplice (che è punita oggi con una pena massima di dieci anni di reclusione).

Una cornice edittale che si inasprisce in maniera significativa nel caso in cui sussistano talune circostanze aggravanti.

Basti pensare che, sulla scorta delle nuove prescrizioni dettate dalla Legge, nell'ipotesi in cui la condotta penalmente rilevante venga posta in essere a danno di una persona incapace per età o per infermità, il reato è punito con la reclusione fino a ventidue anni di reclusione.

2.2 In particolare: l'accesso abusivo a sistema informatico.

Accanto alla previsione di nuove ipotesi di reato, la Legge n. 90/2024 ha individuato nell'inasprimento del trattamento sanzionatorio un ulteriore strumento di prevenzione e contrasto alla criminalità informatica.

Come si è fatto brevemente cenno poc'anzi, tra le fattispecie di reato per cui sono stati introdotti considerevoli aumenti di pena, si annovera **l'accesso abusivo a sistema informatico**, disciplinato dall'art. 615-*ter* c.p.

La normativa previgente prevedeva per la fattispecie aggravata ai sensi del secondo comma della disposizione in parola la pena della reclusione da uno a cinque anni.

Le modifiche introdotte dall'art. 16 della Legge prescrivono invece un raddoppio della cornice edittale prevista per la suddetta fattispecie criminosa.

Con la conseguenza che – a valle delle innovazioni normative – nel caso in cui l'accesso abusivo ad un sistema informatico o telematico sia commesso – ad esempio – da un pubblico ufficiale, la pena applicabile è quella della reclusione da due a dieci anni.

3. Quali sono le modifiche al Codice di Procedura Penale?

Gli interventi della Legge sulla Cybersicurezza interessano non soltanto il Codice Penale, ma anche il Codice di Procedura Penale.

L'art. 17 contiene, infatti, l'elenco delle modifiche di carattere procedurale, orientate ad accogliere le novità di natura sostanziale introdotte dall'art. 16 della Legge in parola.

In particolare, la Legge n. 90/2024 ha previsto per i reati informatici:

- **l'attribuzione della competenza delle indagini preliminari alla Procura distrettuale;**
- **la deroga all'ordinario regime per la concessione della proroga dei termini per lo svolgimento delle indagini preliminari.**

  Si tratta di un regime semplificato, sulla base del quale – in applicazione di quanto previsto dall'art. 406, comma 5-*bis* c.p.p. – il giudice provvede con ordinanza entro dieci giorni dalla presentazione della richiesta di proroga;
- **l'estensione del termine di durata massima delle indagini preliminari a 2 anni.**

Dalla breve disamina delle innovazioni apportate al codice di rito emerge con chiarezza il particolare disvalore che – nella percezione del Legislatore e nei fatti – connota le fattispecie di reato oggetto di discussione.

I reati informatici assurgono invero al ruolo di categoria meritevole di una disciplina (spesso) derogatoria, orientata ad accertare tempestivamente e in maniera più efficace la commissione del reato, normalmente riservata a fattispecie delittuose di particolare gravità.

La visione dei reati informatici quali ipotesi di reato particolarmente offensive sembra trovare conferma in una ulteriore modifica prevista dalla Legge sulla Cybersicurezza, relativa alla disciplina delle intercettazioni.

Invero, l'art. 19 del provvedimento oggetto di interesse prevede l'estensione della disciplina

delle **intercettazioni** applicata ai fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo.

In tali casi, dunque, l'autorizzazione all'intercettazione potrà essere concessa qualora:

- sussistano "**sufficienti indizi**" di reato (e non "gravi indizi");
- l'intercettazione sia "**necessaria per lo svolgimento delle indagini**" (anziché "assolutamente indispensabile").

4. Come interviene la Legge n. 90/2024 in materia di responsabilità 231?

La Legge sulla Cybersicurezza dedica, tra i suoi 24 articoli, una disposizione specifica alla disciplina della responsabilità amministrativa degli enti.

In particolare, **l'art. 20 della Legge**, rubricato "*modifiche al decreto legislativo 8 giugno 2001, n. 231*", interviene su due diversi fronti:

(a) da un lato, introduce un **inasprimento delle sanzioni** in capo all'ente che sia ritenuto responsabile dei reati informatici rientranti nel catalogo 231;

(b) dall'altro, **modifica il catalogo dei reati presupposto**;

Queste novità introdotte dal provvedimento di recente approvazione in tema di responsabilità 231 passano attraverso la modifica dell'art. 24-*bis* del D.lgs. n. 231/2001.

Il significativo intervento operato dal legislatore su tale norma, dedicata – appunto – ai delitti informatici e al trattamento illecito di dati, può essere così sintetizzato:

- **vengono innalzate le sanzioni pecuniarie** applicabili all'ente in caso di accertamento della propria responsabilità (commi 1 e 2).

  Ad esempio, con la nuova disciplina, all'ente ritenuto responsabile del reato di accesso abusivo potrà essere applicata una sanzione compresa tra duecento e settecento quote (e non più quella compresa tra cento e cinquecento quote);

- **viene inserito il comma 1-*bis***: riflesso della nuova fattispecie di estorsione c.d. informatica, il nuovo comma prescrive che, in relazione a tale ipotesi delittuosa, l'ente ritenuto responsabile sarà punito con una sanzione pecuniaria compresa tra trecento e ottocento quote;

- ancora con riferimento al reato di estorsione informatica, viene prescritta, in caso di condanna, l'applicazione delle **sanzioni interdittive**, per un periodo non inferiore a due anni (comma 4).

Conclusioni.

Come è stato anticipato nel paragrafo di apertura, la Legge n. 90/2024 rappresenta un provvedimento inteso ad introdurre nell'ordinamento giuridico misure utili per fronteggiare il fenomeno del *cybercrime*.

Nell'ottica di conseguire tale risultato, il legislatore ha anzitutto predisposto strumenti che mirano a rafforzare il sistema di cybersicurezza nazionale, così da incrementare il livello e la capacità di protezione e di risposta dinnanzi ad eventuali attacchi cibernetici.

Percorrendo il medesimo tracciato, al fine di scoraggiare la commissione dei reati informatici, la Legge sulla Cybersicurezza è intervenuta anche sotto il profilo penale: nuove fattispecie di reato, inasprimento del trattamento sanzionatorio di talune fattispecie di reati informatici già previsti, sino all'introduzione di alcune novità in tema di responsabilità 231.

Un complesso di disposizioni, la cui recente introduzione impone di rimandare ad un secondo momento ogni considerazione sui concreti risvolti della stessa.

Nondimeno, è auspicabile che, in prospettiva futura, tale provvedimento si riveli un mezzo utile ed efficace dinnanzi ad un fenomeno così complesso e sempre più pervasivo quale è quello del *cybercrime*.

Un fenomeno che – evidentemente – necessita di strumenti operativi efficienti per fronteggiarlo e, più in generale, di un quadro giuridico che sia in grado di tenere il passo ad un mondo in cui le emergenze cibernetiche sono in costante evoluzione.

La Legge qui in esame, d'altro canto, rappresenta un tassello di un ampio intervento programmatico nell'ambito della normativa sulla cybersicurezza.

Come noto, infatti, nei prossimi mesi l'Italia dovrà recepire la Direttiva europea NIS2, che mira ad accrescere ulteriormente il livello comune di cybersicurezza in tutta l'Unione Europea.

In attesa di tale intervento normativo, che inserirà nel panorama giuridico italiano ulteriori strumenti a tutela della cybersicurezza, non ci resta che attendere di capire quale sarà l'effettiva portata applicativa delle nuove disposizioni.

Contatti

Giuseppe Fornari
Founding Partner

g.fornari@fornarieassociati.com

Martina Pangallo
Associate

m.pangallo@fornarieassociati.com

Eleonora Rocca
Trainee

e.rocca@fornarieassociati.com

Milano
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

Roma
Piazza Adriana 5
T: +39 0622201000
E: roma@fornarieassociati.com

Bari
Via Principe Amedeo 25
T: +39 080 918 4280
E: bari@fornarieassociati.com

Fornari e Associati

www.fornarieassociati.com