

# dossier

XIX Legislatura

12 marzo 2024

## Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

A.C. n. 1717



Senato  
della Repubblica



Camera  
dei deputati



SERVIZIO STUDI

TEL. 06 6706-2451 - [stud1@senato.it](mailto:stud1@senato.it) - [@SR\\_Studi](https://www.instagram.com/SR_Studi)

Dossier n. 257



SERVIZIO STUDI

Dipartimento Istituzioni

Tel. 06 6760-9475 - [✉ st\\_istituzioni@camera.it](mailto:st_istituzioni@camera.it) - [@CD\\_istituzioni](https://www.instagram.com/CD_istituzioni)

Dipartimento Giustizia

Tel. 06 6760-9148 - [✉ st\\_giustizia@camera.it](mailto:st_giustizia@camera.it) - [@CD\\_giustizia](https://www.instagram.com/CD_giustizia)

Progetti di legge n. 266

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

*AC0225.docx*

## INDICE

### SCHEDE DI LETTURA

▪ Articolo 1 ( <i>Obblighi di notifica di incidenti</i> ) .....	5
▪ Articolo 2 ( <i>Mancato o ritardato adeguamento a segnalazioni dell'Agencia per la cybersicurezza nazionale</i> ).....	8
▪ Articolo 3 ( <i>Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105</i> ) .....	10
▪ Articolo 4 ( <i>Disposizioni in materia di Nucleo per la cybersicurezza</i> ).....	13
▪ Articolo 5 ( <i>Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agencia per la cybersicurezza nazionale</i> ) .....	16
▪ Articolo 6 ( <i>Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza</i> ) .....	19
▪ Articolo 7 ( <i>Funzioni dell'Agencia per la cybersicurezza nazionale in materia di intelligenza artificiale</i> ).....	22
▪ Articolo 8 ( <i>Procedimento sanzionatorio per le violazioni in materia di cybersicurezza di competenza dell'Agencia</i> ).....	25
▪ Articolo 9 ( <i>Disposizioni in materia di personale dell'Agencia per la cybersicurezza nazionale</i> ) .....	28
▪ Articolo 10 ( <i>Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici</i> ) .....	29
▪ Articolo 11 ( <i>Modifiche al codice penale</i> ).....	33
▪ Articolo 12 ( <i>Modifiche al codice di procedura penale</i> ).....	64
▪ Articolo 13 ( <i>Modifiche alle norme sui collaboratori di giustizia di cui al decreto-legge n. 8 del 1991</i> ).....	72
▪ Articolo 14 ( <i>Modifiche al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203</i> ).....	78
▪ Articolo 15 ( <i>Modifiche al decreto legislativo 8 giugno 2001, n. 231</i> ).....	80
▪ Articolo 16 ( <i>Modifiche alla legge 11 gennaio 2018, n. 6</i> ) .....	82
▪ Articolo 17 ( <i>Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109</i> ) .....	84
▪ Articolo 18 ( <i>Disposizioni finanziarie</i> ).....	88
▪ La <i>governance</i> della sicurezza cibernetica .....	89



## **Schede di lettura**



## **Articolo 1** *(Obblighi di notifica di incidenti)*

L'**articolo 1** prevede un obbligo di **segnalazione** di alcune tipologie di **incidenti** aventi impatto su reti, sistemi informativi e servizi informatici in carico alle pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni; alle regioni e province autonome di Trento e di Bolzano; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti; alle aziende sanitarie locali; alle società *in house* degli enti fin qui richiamati.

L'articolo 1, al **comma 1**, prevede un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico ai seguenti soggetti:

- pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge di contabilità e finanza pubblica (legge n. 196 del 2009);
- regioni e province autonome di Trento e di Bolzano
- comuni con popolazione superiore a 100.000 abitanti e comunque i comuni capoluoghi di regione;
- le società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti;
- le aziende sanitarie locali;
- le società *in house* degli enti fin qui richiamati.

In termini generali si ricorda che l'articolo 1 del Testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo n. 175 del 2016, definisce come "società *in house*" le società sulle quali un'amministrazione esercita il controllo analogo a quello esercitato sui propri servizi o più amministrazioni esercitano il controllo analogo congiunto; nelle quali la partecipazione di capitali privati avviene solo se prescritta da norme di legge e con modalità tali da non determinare poteri di controllo o di veto e nelle quali oltre l'ottanta per cento del loro fatturato deve essere effettuato nello svolgimento dei compiti a esse affidati dall'ente pubblico o dagli enti pubblici soci.

Il comma 1 specifica che gli incidenti da segnalare sono quelli indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge n.

105 del 2019. Tale disposizione richiama a sua volta gli incidenti di cui all'articolo 1, comma 1, lettera h) del regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici adottato con il DPCM n. 81 del 2021 e cioè "ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici".

Il **comma 2** indica le modalità con le quali effettuare la notifica: una prima segnalazione deve avvenire senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza; entro settantadue ore dal medesimo momento dovrà avvenire la notifica completa di tutti gli elementi informativi disponibili.

Sia la segnalazione che la notifica completa dovranno avvenire utilizzando le procedure disponibili sul sito *internet* dell'Agenzia per la cybersicurezza nazionale.

I **commi 4 e 5** indicano le sanzioni per la violazione dell'obbligo di notifica.

In particolare, il **comma 4** prevede, in caso di inosservanza, la comunicazione da parte dell'Agenzia per la cybersicurezza nazionale all'interessato che la reiterazione dell'inosservanza comporterà l'applicazione delle sanzioni previste dal comma 5. In caso di inosservanza l'Agenzia inoltre può disporre ispezioni. Queste ispezioni avranno anche il compito di verificare l'attuazione da parte dei soggetti interessati di interventi di rafforzamento della loro resilienza rispetto al rischio di incidenti, interventi direttamente indicati dall'Agenzia ovvero previsti da apposite linee guida adottate dall'Agenzia. Le modalità di svolgimento delle ispezioni saranno disciplinate con determinazione del direttore generale dell'Agenzia pubblicata nella "Gazzetta Ufficiale".

Il **comma 5** individua la sanzione amministrativa pecuniaria per la reiterata inosservanza dell'obbligo di notifica da un minimo di 25.000 a un massimo di 125.000 euro. L'applicazione della sanzione avverrà, specifica la disposizione, nel rispetto "dell'articolo 17, comma 4-*quater*, del decreto-legge n. 82 del 2021"; tale comma è introdotto dall'articolo 8 del presente provvedimento, per la sua illustrazione si rinvia alla relativa scheda.

La violazione può comunque anche costituire causa di responsabilità disciplinare e amministrativo-contabile.

In base al **comma 3**, i soggetti indicati al comma 1 possono anche effettuare notifiche volontarie di incidenti ulteriori rispetto a quelli oggetto di obbligo di notifica sopra descritti. In tal caso si applica quanto



previsto per le notifiche volontarie dai commi 3, 4 e 5 del decreto legislativo n. 65 del 2018 (di recepimento della direttiva (UE) 2016/1148 in materia di sicurezza delle reti e dei sistemi informativi dell'Unione) e cioè che le notifiche volontarie sono trattate successivamente alle notifiche obbligatorie (comma 3); le notifiche volontarie sono trattate solo qualora tale trattamento non costituisca un onere sproporzionato o eccessivo (comma 4); la notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica (comma 5).

Il **comma 6** esclude dall'ambito di applicazione dell'articolo:

- gli operatori di servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali in cui la fornitura di tali servizi dipende dalla rete e dai servizi informativi e in cui un incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio, nei settori dell'energia, bancario, finanziario, sanitario, nel settore dell'acqua potabile e nelle infrastrutture digitali (articolo 3, comma 1, lettera g) del decreto legislativo n. 65 del 2018, che a sua volta richiama, per la definizione dei servizi essenziali l'articolo 4, comma 3, e l'allegato II);
- i fornitori di servizi digitali (di cui all'articolo 3, comma 1, lettera i) del decreto legislativo n. 65 del 2018);
- i soggetti ricompresi nel perimetro di sicurezza nazionale cibernetica di cui all'articolo 1, comma 2-bis del decreto-legge n. 105 del 2019;
- organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa della sicurezza militare dello Stato;
- il Dipartimento delle informazioni per la sicurezza (DIS) (art. 4, legge n. 124 del 2007); l'Agenzia di informazione e sicurezza esterna (AISE) (art. 6, legge n. 124 del 2007) e l'Agenzia di informazione e sicurezza interna (AISI) (art. 7, legge n. 124 del 2007).

*Ratio* della disposizione in commento appare quindi essere quella di prevedere un più ampio obbligo di notifica di incidenti rilevanti per la cybersicurezza per soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica istituito dal decreto-legge n. 82 del 2021 (per il quale si rinvia al box presente nella scheda relativa all'articolo 4).

## Articolo 2

### *(Mancato o ritardato adeguamento a segnalazioni dell’Agenzia per la cybersicurezza nazionale)*

L’**articolo 2** prevede che le amministrazioni e gli enti pubblici e altri soggetti che forniscono servizi pubblici, qualora siano oggetto di **segnalazioni dell’Agenzia per la cybersicurezza nazionale** circa **specifiche vulnerabilità** cui essi risultano **potenzialmente esposti**, debbano provvedere tempestivamente all’adozione degli **interventi risolutivi** indicati dalla stessa Agenzia.

In dettaglio, il **comma 1** prevede che l’Agenzia per la cybersicurezza nazionale (ACN) possa segnalare, ad una serie di soggetti pubblici o che forniscono servizi pubblici, **specifiche vulnerabilità cui essi risultano potenzialmente esposti**; inoltre prevede che i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre **15 giorni** dalla comunicazione, all’adozione degli interventi risolutivi indicati dalla stessa Agenzia.

La disposizione si applica, oltre ai soggetti di cui all’articolo 1, comma 1, del provvedimento in commento, ossia quelli tenuti a segnalare all’ACN gli incidenti cibernetici cui sono incorsi (le amministrazioni centrali, le regioni e province autonome, i grandi comuni, le grandi società di trasporto pubblico urbano e le ASL) anche ai seguenti soggetti:

- **soggetti inclusi nel perimetro di sicurezza nazionale**, di cui all’articolo 1, comma *2-bis*, del D.L. 105/2019: ossia le amministrazioni pubbliche, enti e operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l’**esercizio di una funzione essenziale dello Stato**, ovvero la prestazione di un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un **pregiudizio per la sicurezza nazionale**; l’elenco di tali soggetti è contenuta in un atto amministrativo, non soggetto a pubblicazione, adottato dal Presidente del Consiglio, su proposta del Comitato interministeriale per la cybersicurezza - CIC, entro trenta giorni dalla data di entrata in vigore del DPCM che reca modalità e criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica

(sul punto si rinvia al box contenuto nella scheda relativa all'articolo 4);

- **soggetti NIS**, di cui all'articolo 3, comma 1, lettere g) e i), del D.Lgs. 65/2018 (attuazione direttiva *Network and information security* - NIS), ossia:
  - **operatori di servizi essenziali**, ossia i soggetti pubblici o privati, che forniscono un servizio (dipendente dalla rete e dai sistemi informativi) essenziale per il mantenimento di attività sociali e economiche fondamentali (concernenti settori quali l'energia, i trasporti, banche, sanità, acqua potabile e infrastrutture digitali) e che pertanto un incidente nella loro attività avrebbe effetti negativi rilevanti sulla fornitura di tale servizio;
  - **fornitori di servizi digitali**, cioè qualsiasi persona giuridica che fornisce un servizio digitale, ossia un servizio della società dell'informazione prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi;
- **soggetti Tel.Co.**, di cui all'articolo 40, comma 3, alinea, del D.Lgs. 259/2003 (codice delle comunicazioni elettroniche), ossia le **imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica** accessibili al pubblico:

Il **comma 2** prevede l'applicazione di una **sanzione amministrativa pecuniaria** in caso di mancata o ritardata adozione degli interventi risolutivi indicati dall'ACN di cui al comma 1. Si tratta della medesima sanzione per la reiterata inosservanza dell'obbligo di notifica all'ACN degli incidenti cibernetici indicata all'articolo 1, comma 5, del provvedimento in esame: da 25 mila a 125 mila euro. La sanzione è comminata dall'ACN.

La sanzione non si applica nel caso in cui motivate esigenze di natura tecnico-organizzativa, che devono essere tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine di 15 giorni.

### Articolo 3

*(Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105)*

L'**articolo 3** stabilisce che i soggetti inclusi nel Perimetro provvedono, oltre che alla notifica, anche alla **segnalazione degli incidenti** che intervengono su reti, sistemi informativi e servizi informatici che si trovano **al di fuori del Perimetro** (di loro pertinenza), **senza ritardo e comunque al massimo entro ventiquattro ore**, con finalità di coordinamento del D.L. n. 105/2019 (c.d. decreto Perimetro) con le modifiche recate all'articolo 1 del disegno di legge in esame. Con la medesima finalità si prevede altresì l'applicazione della sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 in caso di reiterata inosservanza dell'obbligo di notifica.

L'articolo 3 interviene in particolare **sull'articolo 1 del decreto-legge n. 105 del 2019** (c.d. decreto Perimetro), inserendo **due modifiche al comma 3-bis** di quell'articolo, che ha **esteso** in capo ai **soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica** (P.A., enti e operatori pubblici e privati che svolgono funzioni istituzionali o essenziali per gli interessi dello Stato, individuati con apposito atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la cybersicurezza) **gli obblighi di notifica** già previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica ("beni ICT"), **anche agli incidenti** che intervengono **su reti, sistemi informativi e servizi** informatici che si trovano **al di fuori del Perimetro** (diversi quindi dai beni ICT), ma che sono **di pertinenza di soggetti inclusi nel Perimetro**.

La disposizione che viene ora modificata è stata inserita nel c.d. decreto Perimetro dall'**art. 37-quater, comma 1, D.L. 9 agosto 2022, n. 115**, al fine di rafforzare il sistema di tutela della sicurezza nazionale nello spazio cibernetico posto in essere dal Perimetro di sicurezza nazionale cibernetica e avere un **quadro tecnico più aggiornato e completo** sugli **attacchi e incidenti** cibernetici che si verificano ai danni delle reti, sistemi informativi e servizi informatici dei soggetti istituzionali e di interesse nazionale che rientrano nel Perimetro.

Ai sensi del citato articolo 1, comma 3-bis del decreto Perimetro, la **tassonomia degli incidenti** su reti, sistemi informativi e servizi informatici che

si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), è **stabilita con determinazioni tecniche** del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale, che possono dettare specifiche modalità di notifica. Al riguardo, è intervenuta la **determinazione 3 gennaio 2023**, che ha classificato, in categorie, gli incidenti, indicando, per ciascuna tipologia di incidente, un codice identificativo e la corrispondente categoria, accompagnata dalla descrizione di ciascuna tipologia di incidente.

Si ricorda inoltre che non rientrano nel nuovo obbligo di notifica introdotto con il D.L. 115/2022 i beni aventi impatto sulle reti, i sistemi informativi e i sistemi informatici del Ministero della difesa. A questi si applicano i principi e le modalità di cui all'articolo 528, comma 1, lettera d) del codice dell'ordinamento della difesa (decreto legislativo n. 66 del 2010)<sup>1</sup>.

Le modifiche introdotte sono finalizzate, come evidenziato anche nella relazione illustrativa, al raccordo e al coordinamento delle disposizioni del citato D.L. 105/2019 con quelle recate dal provvedimento in esame, segnatamente all'articolo 1 (su cui, si rinvia, *supra*, alla relativa scheda di lettura).

Con la prima modifica, di cui alla **lettera a)** – che sostituisce il secondo periodo del richiamato art. 1, co. 3-*bis*, D.L. 105/2019, si prevede, anche per i c.d. soggetti Perimetro, **l'applicazione della medesima procedura** – che consta delle due **distinte fasi della segnalazione e della notifica** – nonché degli stessi termini, introdotti dall'articolo 1 del disegno di legge in esame, in relazione alle ipotesi di notifica già previste per gli stessi soggetti Perimetro dal richiamato comma 3-*bis*, e cioè in relazione agli incidenti aventi impatto su reti, sistemi informativi e servizi informatici, di pertinenza di tali soggetti, diversi da quelli inseriti nel Perimetro.

Pertanto, il nuovo secondo periodo stabilisce che i soggetti inclusi nel Perimetro devono effettuare la **segnalazione degli incidenti** che intervengono su reti, sistemi informativi e servizi informatici che si trovano **al di fuori del Perimetro** (di loro pertinenza), **senza ritardo e comunque al massimo entro ventiquattro ore**, nonché, come già previsto, provvedono alla **notifica entro settantadue ore**.

---

<sup>1</sup> Tale disposizione prevede che all'informatizzazione del Ministero della difesa si applichino le procedure previste dal codice dell'amministrazione digitale (decreto legislativo n. 82 del 2005) con le limitazioni dell'articolo 2, comma 6 (esclusione dall'applicazione del codice dell'amministrazione digitale per le attività di difesa e sicurezza nazionale); dell'articolo 75, comma 2 (partecipazione alle attività del sistema pubblico di connettività) e dell'articolo 17, comma 1-*bis* (svolgimento dei compiti previsti dal Codice dell'amministrazione digitale da parte di agenzie, forze armate e forze di polizia mediante propri uffici, senza incrementare le dotazioni complessive).

Con la seconda modifica, di cui alla **lettera b)** del comma unico dell'articolo in commento, si prevede, aggiungendo un ultimo periodo al richiamato comma *3-bis* dell'art. 1 del decreto Perimetro, l'applicazione delle medesime **sanzioni** introdotte dall'articolo 1 del disegno di legge per i casi di **reiterata inosservanza dell'obbligo di notifica**, ossia la sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000.

**Restano vigenti le ulteriori disposizioni contenute nel citato comma 3-bis**, in base alle quali, in quanto compatibili, per la decorrenza del termine e per le modalità di notifica si applicano le disposizioni dell'[articolo 3](#), comma 4, secondo e terzo periodo, del regolamento di cui al d.P.C.m. 14 aprile 2021, n. 81, in base al quale i termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza, a seguito delle evidenze ottenute, anche mediante le attività di monitoraggio, test e controllo sulla base delle misure di sicurezza (di cui all'allegato B) di un incidente riconducibile a una delle tipologie individuate nell'allegato. Il comma *3-bis* richiama altresì le disposizioni di cui all'[articolo 4](#), commi 2 e 4, del citato regolamento, in materia di notifica volontaria degli incidenti, in base ai quali le notifiche volontarie sono trattate dal CSIRT Italia in subordine a quelle obbligatorie e qualora tale trattamento non costituisca un onere sproporzionato o eccessivo. Il comma 4 prevede che i soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui alla sottocategoria 2.1.4 (ID.AM-6) dell'[allegato B](#), ed in particolare all'incaricato e al referente tecnico di cui alla medesima sottocategoria.

## **Articolo 4** *(Disposizioni in materia di Nucleo per la cybersicurezza)*

L'**articolo 4** prevede la possibilità di far partecipare alle riunioni del **Nucleo per la cybersicurezza** ulteriori soggetti quali rappresentanti della **Direzione nazionale antimafia e antiterrorismo** e rappresentanti della **Banca d'Italia**, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese.

### • *Il Nucleo per la cybersicurezza*

Il decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, all'articolo 8 ha disposto che, presso la medesima Agenzia, venisse costituito in via permanente il Nucleo per la cybersicurezza, adibito a supportare il Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento (comma 1).

Secondo quanto disposto al comma 2, il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), di ciascuno dei Ministeri rappresentati nel Comitato interministeriale per la Cybersicurezza (CIC) e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza.

In relazione alle materie oggetto di trattazione, i componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni e

possono essere chiamati a partecipare anche rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza (comma 3).

Al comma 4 si prevede che il Nucleo, anche relativamente ai compiti di gestione delle crisi che coinvolgono aspetti di cybersicurezza, possa essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati.

Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati (comma 4-bis).

In particolare, disponendo l'introduzione, dopo il comma 4 dell'articolo 8 del decreto-legge n. 82 del 2021, di un nuovo comma, si prevede per l'appunto che, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia<sup>2</sup>, il Nucleo possa essere convocato nella composizione di cui al medesimo comma 4 – e, dunque, con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati –, di volta in volta estesa alla partecipazione:

- di un rappresentante della Direzione nazionale antimafia e antiterrorismo,
- della Banca d'Italia,
- di uno o più operatori – di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019, indicato nella norma come “decreto-legge perimetro”, in coerenza con la definizione recata dall'articolo 1 del decreto-legge n. 82 del 2021 che qui si novella – inseriti nel cosiddetto perimetro di sicurezza nazionale cibernetica,
- nonché di eventuali altri soggetti, interessati alle stesse questioni.

#### • *Il Perimetro di sicurezza nazionale cibernetica*

Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una **funzione essenziale dello Stato**, ovvero la prestazione di un **servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato** e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un **pregiudizio per la sicurezza nazionale**, è stato adottato il **decreto-legge n. 105 del 2019** con il quale è stato istituito un **perimetro di sicurezza nazionale cibernetica** e sono state introdotte misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

All'articolo 1, comma 2-bis, il citato decreto-legge stabilisce che l'elencazione di tali soggetti sia contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la cybersicurezza (CIC). L'atto amministrativo in questione, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco.

---

<sup>2</sup> di cui all'articolo 9, comma 1, lettera a), del decreto-legge n. 82 del 2021



L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità.

Dando seguito all'art. 1, comma 2, lettera b), del citato decreto-legge, è stato adottato il **Regolamento** in materia di **notifiche degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici ([DPCM n. 81 del 2021](#)).

In base a quanto disposto dall'art. 3 del DPCM, i soggetti pubblici e privati che abbiano ricevuto la comunicazione di inclusione all'interno del perimetro provvedono a notificare al CSIRT italiano (*Computer Security Incident Response Team* – gruppo di intervento per la sicurezza informatica in caso di incidente) le tipologie di incidenti previste nell'allegato A del medesimo DPCM che impattino sui beni ICT di propria pertinenza. Tale obbligo di notifica è esteso, dal comma 3 del medesimo articolo, anche agli incidenti che impattino su beni “contigui” a quelli ICT.

La notifica deve essere effettuata **entro sei ore**, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A (meno grave), ed **entro un'ora**, qualora si tratti di un incidente individuato nella tabella 2 del medesimo allegato (più grave). Tali termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza di un incidente riconducibile a una delle tipologie individuate nell'allegato A.

A fronte dell'esigenza di garantire la conoscenza delle informazioni relative agli incidenti anche laddove questi non colpiscano i beni ICT o quelli ad essi contigui, nell'art. 1 del decreto-legge n. 105 del 2019 è stato inserito il **nuovo comma 3-bis**<sup>3</sup>, il quale per l'appunto stabilisce che l'obbligo di notifica di cui si è detto sorga anche in presenza di incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici di pertinenza del soggetto “diversi” dai beni ICT. In questi casi la notifica deve essere effettuata **entro il termine di 72 ore**.

La [determina](#) del 3 gennaio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale riporta la tassonomia degli incidenti informatici relativi alla cybersicurezza che hanno un impatto su reti, sistemi informativi e servizi informatici attinenti ai soggetti che sono tenuti alla notifica ai sensi dell'art. 1, comma 3-bis, del decreto-legge n. 105 del 2019.

Si precisa, infine, che le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice.

---

<sup>3</sup> Decreto-legge n.115 del 2022, art. 37-quater, comma 1.

## Articolo 5

### *(Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale)*

L'articolo 5 consente al Presidente del Consiglio dei Ministri di disporre il **differimento degli obblighi informativi e delle attività di resilienza in capo all'Agenzia per la cybersicurezza nazionale** nei casi in cui questo sia considerato strettamente necessario dai servizi di sicurezza della Repubblica.

In particolare, il **comma 1** dell'articolo in esame prevede che, qualora **i servizi di sicurezza della Repubblica**, avuta notizia di un **evento** o di un **incidente informatici**, ritengano **strettamente necessario**, per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica, **il differimento di una o più attività di resilienza** di competenza dell'Agenzia per la cybersicurezza nazionale, per il tramite del Dipartimento delle informazioni per la sicurezza, **ne informino il Presidente del Consiglio dei ministri** o l'Autorità delegata per la sicurezza della Repubblica, ove istituita.

Il **comma 2** dell'articolo in commento dispone che, nei casi di cui al comma 1, il **Presidente del Consiglio dei ministri**, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, **può disporre il differimento degli obblighi informativi** cui è in ogni caso tenuta la citata Agenzia, **nonché il differimento di una o più delle sopra citate attività di resilienza**.

I **servizi di cui agli articoli 6 e 7 [della legge 3 agosto 2007, n. 124](#)**, cui fa esplicito riferimento il comma 1 dell'articolo in esame, sono **l'Agenzia informazioni e sicurezza esterna (AISE)**, cui è affidato il compito di ricercare ed elaborare tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero, e **l'Agenzia informazioni e sicurezza interna (AISI)**, alla quale è affidato il compito di ricercare ed elaborare tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

Il **Sistema di informazione per la sicurezza della Repubblica**, ai sensi dell'articolo 2 della citata legge n. 124 del 2007, è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità delegata per la sicurezza della repubblica, ove istituita, dal Dipartimento delle informazioni per la sicurezza (DIS), dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI).

Per quanto concerne l'**Autorità delegata per la sicurezza della Repubblica**, si ricorda infine che, ai sensi dell'articolo 3 della legge 3 agosto 2007, n. 124, il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni in materia di sicurezza della repubblica e di cybersicurezza, che non sono ad esso attribuite in via esclusiva, **soltanto ad un Ministro senza portafoglio o ad un Sottosegretario di Stato**. Non è richiesto il parere del Consiglio dei ministri per il conferimento delle citate deleghe.

Quanto alle **attività di resilienza di competenza della Agenzia per la cybersicurezza nazionale** di cui l'articolo in esame rende possibile, al comma 1, il differimento, esse sono puntualmente identificate in quelle di cui all'articolo 7, comma 1, lettere *n*) ed *n-bis*) del [decreto-legge 14 giugno 2021, n. 82](#). Ai sensi delle citate lettere, l'Agenzia per la cybersicurezza nazionale esercita le seguenti funzioni:

- sviluppare capacità nazionali di **prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici**, anche attraverso il Gruppo di intervento per la sicurezza informatica in caso di incidente – CSIRT di cui all'articolo 8 del [decreto legislativo 18 maggio 2018, n. 65](#) (cosiddetto decreto legislativo “NIS”), ed anche promuovendo iniziative di partenariato pubblico-privato (lettera *n*));

- nell'ambito delle funzioni appena citate, svolgere ogni **attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi**, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici (lettera *n-bis*)).

In riferimento **agli obblighi informativi** di cui, parimenti, l'articolo in commento rende possibile, al comma 2, il differimento, essi sono quelli di cui all'articolo 17, commi 4 e *4-bis*, del medesimo decreto-legge n. 82 del 2021. Ai sensi di tali commi:

- il personale dell'Agenzia per la cybersicurezza nazionale addetto al CSIRT Italia, in quanto pubblico ufficiale, è tenuto, ai sensi [dell'articolo 331 del codice di procedura penale](#), a **trasmettere le notifiche di incidente informatico ricevute** all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione che, ai sensi del [decreto interministeriale 19](#)

---

[gennaio 1999](#), è stato individuato nel **Servizio di Polizia postale e comunicazioni** (comma 4);

- l'Agenzia per la cybersicurezza nazionale è poi tenuta a **trasmettere al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti** per l'esercizio delle sue funzioni, ai sensi [dell'articolo 371-bis del codice di procedura penale](#) (comma 4-*bis*).

## Articolo 6

### *(Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza)*

L'**articolo 6** istituisce, per le pubbliche amministrazioni indicate nell'**articolo 1, comma 1**, dove non sia già presente, la **struttura preposta alle attività di cyber-sicurezza**, anche all'interno di quelle già presenti a legislazione vigente; al contempo, predispone l'istituzione del **referente per la cyber-sicurezza**, unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale. Precisa, infine, quali soggetti e quali organi dello Stato siano esclusi dall'applicazione dei nuovi obblighi e per cui permane la disciplina precedente.

Il **comma 1** individua, primariamente, i soggetti delle pubbliche amministrazioni coinvolti. Si tratta delle **pubbliche amministrazioni** trattate nell'**articolo 1, comma 1**, del disegno di legge salvo non presentino già la struttura costituenda. In particolare, si tratta di:

- le pubbliche amministrazioni definite come tali a partire dalla ricognizione annuale dell'ISTAT e pubblicata con proprio provvedimento sulla gazzetta ufficiale (art. 1, comma 3, legge n. 196 del 2009);
- le regioni e le province autonome di Trento e Bolzano;
- i comuni con una popolazione superiore ai 100.000 abitanti;
- i comuni capoluoghi di regione;
- le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti;
- le aziende sanitarie locali.

Tali soggetti, qualora non la possiedano ancora, devono dotarsi di una **struttura per la cybersicurezza**, anche fra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Le **lettere da a) a g)** del comma 1 individua i compiti a cui tale struttura dovrà provvedere, in particolare:

- lo sviluppo di politiche e procedure di sicurezza delle informazioni;
- la produzione e l'aggiornamento di un piano per il rischio informatico;

- la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;
- la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, a partire dalla produzione dei piani precedentemente elencati;
- la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
- il monitoraggio e la valutazione continua delle minacce alla sicurezza e alla vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Il **comma 2** istituisce la figura del referente per la cybersicurezza all'interno delle strutture appena descritte nel **comma 1**. Questo in particolare:

- viene individuato in ragione delle **qualità professionali** possedute;
- svolge la funzione di **punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale** in relazione a quanto previsto dalla legge e dalle normative settoriali in materia di cybersicurezza per le amministrazioni;
- il suo **nominativo** deve essere **comunicato** all'Agenzia per la cybersicurezza nazionale.

Il **comma 3** individua i soggetti e gli organi dello Stato a cui non si applicano le disposizioni presenti.

La **lettera a)** specifica l'**esclusione delle amministrazioni pubbliche**, degli enti e degli operatori pubblici e privati, elencati **all'interno del decreto del Presidente del Consiglio dei Ministri n. 131 del 31 luglio 2020**, adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC) (art. 1, co. 2-*bis*, decreto-legge n.105 del 2019, convertito con modificazione nella legge n. 133 del 2019). Si tratta dei soggetti già inclusi nel perimetro di sicurezza nazionale cibernetica e per i quali già risultano in vigore specifici obblighi di sicurezza (si rinvia, al riguardo, alle schede relative agli articoli 2 e 4).

La **lettera b)** specifica l'esclusione per quegli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza, in particolare:

- il Dipartimento delle informazioni per la sicurezza (**DIS**) (art. 4, legge n. 124 del 2007);

- l' Agenzia di informazione e sicurezza esterna (**AISE**) (art. 6, legge n. 124 del 2007);
- l' Agenzia di informazione e sicurezza interna (**AISI**) (art. 7, legge n. 124 del 2007).

## Articolo 7

### *(Funzioni dell’Agenzia per la cybersicurezza nazionale in materia di intelligenza artificiale)*

L’**articolo 7** inserisce tra le funzioni dell’Agenzia per la cybersicurezza nazionale – ACN la valorizzazione dell’**intelligenza artificiale** per il **rafforzamento della cybersicurezza nazionale**.

A tal fine, modifica il D.L. 82/2021, che ha definito l’architettura della cybersicurezza nazionale e ha istituito e disciplinato l’ACN, ed in particolare il comma 1 dell’articolo 7 che individua puntualmente le funzioni dell’agenzia. Attraverso l’inserimento della nuova lettera *m-quater*), tra le funzioni istituzionali dell’ACN viene ricompresa quella della **promozione e sviluppo** di ogni iniziativa, anche di partenariato tra soggetti pubblici e privati, per la valorizzazione dell’intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale; ciò anche al fine di favorire un **uso etico e corretto** dei sistemi basati sulla IA.

#### • *L’intelligenza artificiale e la sicurezza cibernetica*

È in via di definitiva adozione da parte del Parlamento europeo e del Consiglio la proposta di regolamento, presentata dalla Commissione europea il 21 aprile 2021, recante un quadro giuridico in materia di intelligenza artificiale (*Artificial Intelligence Act*). Per approfondire si veda il tema dell’attività parlamentare del Servizio Studi della Camera su [L’intelligenza artificiale](#).

Il regolamento ha l’obiettivo di migliorare il funzionamento del mercato interno e promuovere l’adozione di un’intelligenza artificiale affidabile, garantendo, nel contempo, un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dell’UE, compresa la democrazia, lo Stato di diritto e la tutela dell’ambiente dagli effetti dannosi dei sistemi di intelligenza artificiale nell’Unione, nonché sostenendo l’innovazione.

In particolare, il nuovo regolamento introduce: a) regole armonizzate per l’immissione sul mercato, la messa in servizio e l’uso dei sistemi di intelligenza artificiale nell’Unione; b) il divieto di determinate pratiche di intelligenza artificiale; c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; d) regole di trasparenza armonizzate per alcuni sistemi di IA; e) regole armonizzate specifiche per l’immissione sul mercato di modelli di IA di uso generale; f) regole sul monitoraggio del mercato, sulla governance e sull’applicazione della vigilanza del mercato stesso; g) misure a sostegno dell’innovazione, con particolare attenzione alle PMI, comprese le start-up.



Per quanto qui di interesse, il regolamento considera ad alto rischio i sistemi di IA che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali. Quindi, prima di immettere un sistema di IA ad alto rischio sul mercato dell'UE, o di farlo entrare in servizio, i fornitori dovranno sottoporlo a una valutazione della conformità. Dovranno dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza).

Inoltre, i fornitori di modelli che comportano rischi sistemici saranno pertanto tenuti a valutare e attenuare i rischi, a segnalare incidenti gravi, a condurre prove e valutazioni dei modelli all'avanguardia, a garantire la cibersicurezza e a fornire informazioni sul consumo energetico dei loro modelli.

A livello nazionale, si segnala la promozione dell'Intelligenza Artificiale all'interno della PA proposta dalla [Strategia italiana sull'AI](#) – elaborata alla fine del novembre 2021 dal Ministero dello Sviluppo Economico, il Ministero dell'innovazione tecnologica e della transizione digitale e quello dell'università e della ricerca, al fine di delineare le politiche da implementare nel triennio 2022-2024 per potenziare il sistema IA in Italia. Tra i principi guida del documento vi è necessità di implementare l'IA in modo responsabile e trasparente, affinché possa rispondere alle sfide della società garantendo sicurezza in tutti i settori.

A tal fine, l'Italia ha aderito alle [Linee guida etiche per un programma di orientamento e attuazione affidabile dell'IA](#) definito dall'*High Level Expert Group on AI*. La sicurezza nazionale è uno dei settori prioritari considerati nella strategia: “L'importanza dell'IA per la sicurezza nazionale di un Paese è cresciuta costantemente negli ultimi cinque anni. Pertanto, l'Italia è pienamente impegnata a investire in applicazioni di intelligenza artificiale che garantiscano la sicurezza dei suoi cittadini. Ciò include la sicurezza informatica individuale e nazionale, in cui l'IA ha contribuito con lo sviluppo di software di rilevamento e risoluzione di nuova generazione”.

Anche il [Piano triennale per l'informatica nella pubblica amministrazione 2024-2026](#) pubblicato dall'AGID del dicembre 2023 affronta il tema dell'intelligenza artificiale. Si prevede che gli acquisti di innovazione, nel prossimo triennio, saranno indirizzati prioritariamente alla sperimentazione di modelli di commercializzazione ed acquisto di sistemi di intelligenza artificiale ed alla crescita di capacità industriali nel settore, anche attraverso collaborazioni internazionali. Il Dipartimento per la trasformazione digitale, l'ACN e l'AGID si impegnano, pertanto, a promuovere l'obiettivo di innalzare i livelli di cybersecurity dell'Intelligenza Artificiale per assicurare che sia progettata, sviluppata e impiegata in maniera sicura, anche in coerenza con le linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale. Dunque, la cibersicurezza è considerata una pre-condizione essenziale dell'IA e serve per garantire resilienza, privacy, correttezza ed affidabilità dei sistemi. Per questo motivo, l'Agenzia per la cibersicurezza nazionale ha aderito alle [Linee guida per uno sviluppo sicuro dell'Intelligenza Artificiale](#), promosse dal

*National Cyber Security Centre del Regno Unito.* Il documento, reso pubblico il 27 novembre 2023, è stato sottoscritto da 23 Agenzie di 18 Paesi ed è rivolto a tutti i fornitori di sistemi che utilizzano l'Intelligenza Artificiale, sia creati da zero sia costruiti su servizi o strumenti forniti da altri.

## **Articolo 8**

*(Procedimento sanzionatorio per le violazioni in materia di cybersicurezza di competenza dell’Agenzia)*

L’articolo 8 definisce **tempi e modalità per l’adozione del regolamento** che stabilisce 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. Prevede che nelle more dell’adozione del regolamento, trovi applicazione il capo I, sezioni I e II, della legge sulle sanzioni amministrative (n. 689/1981).

A tal fine, la disposizione in commento introduce un nuovo **comma 4-quater all’articolo 17 del decreto-legge n. 82 del 2021**, che ha definito l’architettura nazionale di cybersicurezza ed istituito l’Agenzia per la cybersicurezza nazionale.

La disposizione così introdotta stabilisce che la **disciplina del procedimento sanzionatorio** amministrativo dell’Agenzia per la cybersicurezza nazionale è **definita con regolamento** adottato con decreto del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la cybersicurezza.

La disposizione precisa che il regolamento può essere adottato **anche in deroga all’articolo 17 della legge 23 agosto 1988, n. 400**.

Il regolamento dovrà definire i termini e le modalità per l’**accertamento**, la **contestazione** e la **notificazione delle violazioni** della normativa in materia di cybersicurezza e l’**irrogazione delle relative sanzioni** che sono di competenza dell’Agenzia ai sensi del citato D.L. n. 82/2021 e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all’Agenzia.

In proposito, si ricorda che il D.L. n. 82/2021 ha stabilito (art. 7), tra le diverse competenze, che l’Agenzia per la cybersicurezza nazionale:

- a) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi ed è competente all’accertamento delle violazioni e all’irrogazione delle **sanzioni amministrative previste dal decreto legislativo NIS** (D.Lgs. n. 65/2018);
- b) è Autorità nazionale di certificazione della cybersicurezza e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già

attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni;

- c) assume tutte le funzioni in materia di cybersicurezza **già attribuite al Ministero dello sviluppo economico**, tra cui le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del **decreto-legge perimetro** e quelle relative all'**accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste** dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;
- d) assume tutte le funzioni **già attribuite alla Presidenza del Consiglio dei ministri** in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto (D.L. 105/2019).

L'articolo 17 del medesimo D.L. 82/2021, al comma 1, prevede che per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, attribuite all'Agenzia, essa possa avvalersi "dell'ausilio" del personale dell'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni (previsto dall'articolo 7-bis del decreto-legge n. 144 del 2005; ossia il Servizio di polizia postale e delle comunicazioni del Dipartimento della pubblica sicurezza).

**Il regolamento è adottato entro novanta giorni dalla data di entrata in vigore della legge.**

La disposizione stabilisce infine che **nelle more** dell'entrata in vigore di tale regolamento, ai procedimenti sanzionatori si applicano, per ciascuna delle richiamate fasi procedurali (accertamento, contestazione e notificazione delle violazioni e irrogazione delle relative sanzioni), le disposizioni contenute nel capo I, sezioni I e II, della **legge 24 novembre 1981, n. 689**.

In base alla legge 689/1981 l'applicazione della sanzione amministrativa pecuniaria avviene secondo il seguente procedimento:

- accertamento, contestazione-notifica al trasgressore;
- pagamento in misura ridotta o inoltro di memoria difensiva all'autorità amministrativa: archiviazione o emanazione di ordinanza ingiunzione di pagamento da parte dell'autorità amministrativa;
- eventuale opposizione all'ordinanza ingiunzione davanti all'autorità giudiziaria (giudice di pace o tribunale);
- accoglimento dell'opposizione, anche parziale, o rigetto (sentenza ricorribile per cassazione);
- eventuale esecuzione forzata per la riscossione delle somme.

Dal punto di vista procedimentale, occorre innanzitutto che la violazione sia accertata dagli organi di controllo competenti o dalla polizia giudiziaria (art. 13).

La violazione deve essere immediatamente contestata o comunque notificata al trasgressore entro 90 giorni (art. 14); entro i successivi 60 giorni l'autore può conciliare pagando una somma ridotta pari alla terza parte del massimo previsto o pari al doppio del minimo (cd. oblazione o pagamento in misura ridotta, art. 16). In caso contrario, egli può, entro 30 giorni, presentare scritti difensivi all'autorità competente; quest'ultima, dopo aver esaminato i documenti e le eventuali memorie presentate, se ritiene sussistere la violazione contestata determina l'ammontare della sanzione con ordinanza motivata e ne ingiunge il pagamento (cd. ordinanza-ingiunzione, art. 18).

Entro 30 giorni dalla sua notificazione l'interessato può presentare opposizione all'ordinanza ingiunzione (che, salvo eccezioni, non sospende il pagamento), inoltrando ricorso all'autorità giudiziaria competente (artt. 22, 22-bis). In base all'art. 6 del decreto-legislativo 150/2011, l'autorità giudiziaria competente sulla citata opposizione è il giudice di pace a meno che, per il valore della controversia (sanzione pecuniaria superiore nel massimo a 15.493 euro) o per la materia trattata (tutela del lavoro, igiene sui luoghi di lavoro e prevenzione degli infortuni sul lavoro; previdenza e assistenza obbligatoria; tutela dell'ambiente dall'inquinamento, della flora, della fauna e delle aree protette; igiene degli alimenti e delle bevande; materia valutaria; antiriciclaggio), non sussista la competenza del tribunale. L'esecuzione dell'ingiunzione non viene sospesa e il giudizio che con esso si instaura si può concludere o con un'ordinanza di convalida del provvedimento o con sentenza di annullamento o modifica del provvedimento. Il giudice ha piena facoltà sull'atto, potendo o annullarlo o modificarlo, sia per vizi di legittimità che di merito. In caso di condizioni economiche disagiate del trasgressore, l'autorità che ha applicato la sanzione può concedere la rateazione del pagamento (art. 26). Decorso il termine fissato dall'ordinanza ingiunzione, in assenza del pagamento, l'autorità che ha emesso il provvedimento procede alla riscossione delle somme dovute con esecuzione forzata in base alle norme previste per l'esazione delle imposte dirette (art. 27). Il termine di prescrizione delle sanzioni amministrative pecuniarie è di 5 anni dal giorno della commessa violazione (art. 28).

**Articolo 9**  
*(Disposizioni in materia di personale dell’Agenzia per la cybersicurezza nazionale)*

L’articolo 9 stabilisce un **divieto**, della durata di due anni, **di assunzione**, anche di incarichi, **presso soggetti privati** finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i **dipendenti** appartenenti al ruolo del personale dell’**Agenzia per la cybersicurezza nazionale** che abbiano partecipato, nell’interesse e a spese dell’Agenzia stessa, a specifici **percorsi formativi di specializzazione**. Sono tuttavia previste delle specifiche **cause di esclusione** dall’applicazione del richiamato divieto.

Più nel dettaglio, introducendo il nuovo comma 8-ter all’articolo 12 del decreto-legge 14 giugno 2021, n. 82, l’articolo in esame dispone che i dipendenti appartenenti al ruolo del personale dell’Agenzia che abbiano partecipato, nell’interesse e a spese dell’Agenzia stessa, a specifici percorsi formativi di specializzazione, **per due anni a decorrere dalla data di completamento dell’ultimo dei predetti percorsi formativi** non possono essere assunti, né assumere incarichi, presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza, pena la nullità dei contratti eventualmente stipulati in violazione di quanto disposto.

**Tale divieto non si applica** al personale che sia cessato dal servizio presso l’Agenzia in caso di:

- collocamento a riposo d’ufficio al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia;
- cessazione a domanda per inabilità;
- dispensa dal servizio dovuta a motivi di salute.

I percorsi formativi di specializzazione che danno luogo al predetto divieto di assunzione sono individuati con determinazione del direttore generale dell’Agenzia sulla base della particolare qualità dell’offerta formativa, dei costi, della durata e del livello di specializzazione che consegue alla frequenza dei medesimi.

**Articolo 10**  
*(Disciplina dei contratti pubblici di beni e servizi informatici  
impiegati in un contesto connesso alla tutela degli interessi  
nazionali strategici)*

L'articolo 10 introduce alcuni **criteri di cybersicurezza** nella disciplina dei **contratti pubblici**: nel caso di **approvvigionamento di beni e servizi informatici**, le pubbliche amministrazioni, le società pubbliche e i soggetti privati compresi nel perimetro di sicurezza cibernetica, devono tenere in considerazione gli **elementi essenziali di cybersicurezza** individuati da un DPCM da emanarsi entro 120 giorni. Si prevedono poi che, nell'ambito di tali contratti, una serie di obblighi e facoltà in capo alle **stazioni appaltanti**, incluse le centrali di committenza, sempre in relazione agli elementi essenziali di cybersicurezza.

In dettaglio, il **comma 1** prevede l'adozione di un **decreto del Presidente del Consiglio dei ministri**, entro 120 giorni dalla data di entrata in vigore del provvedimento in esame, su proposta dell'Agenzia per la cybersicurezza nazionale e previo parere del Comitato interministeriale per la cybersicurezza (CIC), con cui sono individuati gli **elementi essenziali di cybersicurezza** da tenere in considerazione in relazione alle **attività di approvvigionamento di beni e servizi informatici** impiegati in un contesto connesso alla tutela degli **interessi nazionali strategici**.

Si precisa, inoltre, che per elementi essenziali di cybersicurezza si intende "l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela" degli interessi nazionali strategici.

I soggetti tenuti a rispettare tali elementi essenziali nell'acquisto di beni ICT sono quelli indicati nell'articolo 2, comma 2, del codice dell'amministrazione digitale (D.Lgs. 82/2005), ossia:

- le **pubbliche amministrazioni**, comprese le autorità di sistema portuale e le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
- i **gestori di servizi pubblici**, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
- le **società a controllo pubblico**, escluse le società quotate a meno che non gestiscano servizi di pubblico interesse.

Inoltre, rientrano nel campo di applicazione della disposizione di cui sopra anche i **sogetti privati**, non compresi tra quelli di cui sopra, ma rientranti nel **perimetro di sicurezza nazionale cibernetica (PSNC)** di cui all'articolo 1, comma 2-*bis*, del D.L. 105/2019. Si tratta dei soggetti aventi una sede nel territorio nazionale, da cui dipende l'**esercizio di una funzione essenziale dello Stato**, ovvero la prestazione di un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un **pregiudizio per la sicurezza nazionale**; l'elenco di tali soggetti è contenuta in un atto amministrativo, non soggetto a pubblicazione, adottato dal Presidente del Consiglio, su proposta del Comitato interministeriale per la cybersicurezza - CIC, entro trenta giorni dalla data di entrata in vigore del DPCM che reca modalità e criteri procedurali di individuazione dei soggetti inclusi nel PSNC (**comma 3**).

Il **comma 2** prevede, nell'ambito dei contratti di approvvigionamento di beni e servizi informatici di cui al comma 1, una serie di **obblighi e facoltà in capo alle stazioni appaltanti**, incluse le centrali di committenza, **in relazione agli elementi essenziali di cybersicurezza** individuati dal comma precedente.

Nel dettaglio viene previsto che le stazioni appaltanti, incluse le centrali di committenza:

- possono esercitare la **facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del D.Lgs. 36/2023** (Codice dei contratti pubblici), se accertano che l'offerta non tiene conto degli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;

In base al disposto dell'art. 107, comma 2, del Codice dei contratti pubblici, la stazione appaltante può decidere di non aggiudicare l'appalto all'offerente che ha presentato l'offerta economicamente più vantaggiosa se ha accertato che l'offerta non soddisfa gli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali di diritto del lavoro.

L'art. 108, comma 10, del medesimo Codice, dispone invece che le stazioni appaltanti possono decidere di non procedere all'aggiudicazione se nessuna offerta risulti conveniente o idonea in relazione all'oggetto del contratto. Tale facoltà, che va indicata espressamente nel bando di gara o invito nelle procedure senza bando, può essere esercitata non oltre il termine di trenta giorni dalla conclusione delle valutazioni delle offerte.



- **considerano sempre gli elementi essenziali di cybersicurezza** di cui al comma 1 nella valutazione dell'elemento qualitativo, **ai fini dell'individuazione del miglior rapporto qualità/prezzo** per l'aggiudicazione;
- nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del Codice dei contratti pubblici, inseriscono gli **elementi di cybersicurezza** di cui al comma 1 **tra i requisiti minimi dell'offerta**;

L'art. 108, comma 3, del Codice consente l'utilizzazione del criterio del minor prezzo per i servizi e le forniture con caratteristiche standardizzate o le cui condizioni sono definite dal mercato.

Nella recente giurisprudenza del Consiglio di Stato è stato evidenziato che “per la giurisprudenza (da ultimo, Cons. Stato, V, 27 ottobre 2022, n. 9249), le caratteristiche indefettibili (ossia i requisiti minimi) delle prestazioni o del bene previste dalla *lex specialis* di gara costituiscono una condizione di partecipazione alla procedura selettiva” ([sentenza n. 10577/2022](#)) e che “secondo l'indirizzo sostenuto dalla giurisprudenza prevalente, l'operatore economico che offre una prestazione o un prodotto privo dei requisiti minimi di carattere tecnico deve essere escluso dalla procedura di gara” ([sentenza n. 423/2023](#)).

- nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa (**OEPV**), ai sensi dell'articolo 108, comma 4, del Codice dei contratti pubblici, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un **tetto massimo per il punteggio economico entro il limite del 10%**.

Il richiamato comma 4 dell'art. 108 del Codice dei contratti pubblici dispone che i documenti di gara stabiliscono i criteri di aggiudicazione dell'offerta, pertinenti alla natura, all'oggetto e alle caratteristiche del contratto. In particolare, l'OEPV, individuata sulla base del miglior rapporto qualità/prezzo, è valutata sulla base di criteri oggettivi, quali gli aspetti qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto. La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. Il quarto periodo del comma 4 dispone poi che “nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici”, mentre il successivo periodo

dispone che “nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento”.

Le disposizioni introdotte dall’articolo in esame si inseriscono in un sistema normativo di **approvvigionamento di beni ICT** disciplinato principalmente dall’articolo 1 del D.L. 105/2019, relativo al PSNC. Le disposizioni in materia di approvvigionamento di prodotti, processi, servizi per tecnologie dell’informazione e delle telecomunicazioni e associate infrastrutture destinati alle reti, ai sistemi informativi e all’espletamento dei servizi informatici di cui al comma 2, lettera *b*), del medesimo articolo 1 del D.L. 105/2019 sono espressamente richiamate e fatte salve dal **comma 4** dell’articolo in esame.

Ai sensi della disposizione da ultimo citata, i soggetti rientranti nel PSNC sono tenuti a predisporre, e aggiornare almeno annualmente, un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, da cui dipendono funzioni o servizi essenziali e il cui malfunzionamento può arrecare pericoli per la sicurezza nazionale.

Gli elenchi, predisposti secondo i criteri elaborati dal Tavolo interministeriale per l’attuazione del perimetro di sicurezza nazionale cibernetica, sono trasmessi all’Agenzia per la cybersicurezza nazionale.

Nel sistema di approvvigionamento dei beni ICT dei soggetti inclusi nel PSNC un ruolo centrale è svolto dal Centro di valutazione e certificazione nazionale (CVCN), organismo operante presso l’Agenzia per la cybersicurezza nazionale, disciplinato dall’articolo 1 del D.L. 105/2019. Il CVCN ha il compito di valutare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del PSNC e appartenenti alle categorie individuate dal [DPCM 15 giugno 2021](#). I soggetti rientranti nel PSNC che intendono procedere, anche tramite le centrali di committenza, all’affidamento di beni ICT sono tenuti a darne comunicazione al CVCN per le opportune verifiche che possono prevedere anche specifici *test software e hardware*.

I fornitori di beni ICT a loro volta, sono tenuti ad assicurare al CVCN la collaborazione per l’effettuazione di *test*.

Il CVCN, inoltre, contribuisce all’elaborazione delle misure di sicurezza, definisce le metodologie di verifica e *test* ed elabora gli schemi di certificazione cibernetica.

Il Ministero dell’interno e quello della difesa utilizzano propri centri di valutazione in luogo del centro nazionale.

## **Articolo 11** *(Modifiche al codice penale)*

**L'articolo 11** reca modifiche al codice penale in materia di **prevenzione e contrasto dei reati informatici**.

Il **comma 1, lett. a)**, modifica l'art. 615-ter c.p. (*Accesso abusivo a un sistema informatico o telematico*).

L'art. 615-ter c.p. nel testo attualmente vigente punisce con la **reclusione fino a 3 anni** chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo (primo comma).

Il secondo comma prevede quali circostanze aggravanti punite con la **reclusione da 1 a 5 anni**:

- la commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da parte di un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (n. 1);
- la commissione del fatto con violenza sulle cose o sulle persone o se il colpevole è palesemente armato (n. 2);
- la distruzione o il danneggiamento del sistema, l'interruzione totale o parziale, la distruzione o il danneggiamento di dati, informazioni o programmi (n. 3).

Il terzo comma prevede quale ulteriore aggravante, parimenti punita con la **reclusione da 1 a 5 anni**, la commissione del fatto su **sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico**.

Il medesimo terzo comma prevede che qualora concorrano l'aggravante di cui al comma stesso e taluna di quelle di cui al secondo comma la pena sia della **reclusione da 3 a 8 anni**.

Il delitto è punibile a querela nel caso previsto dal primo comma; negli altri casi si procede d'ufficio.

Le modifiche introdotte dalla disposizione in commento sono volte ad **ampliare l'ambito di applicazione della fattispecie** e a inasprire il trattamento sanzionatorio **elevando le pene previste**.

Sotto il primo profilo:

- l'aggravante di cui al secondo comma, n. 2, è prevista non soltanto se il colpevole per commettere il fatto usa violenza sulle cose o sulle persone, ma anche se usa **minaccia (n. 1, 1.2)**;
- l'aggravante di cui al secondo comma, n. 3, è prevista anche se dal fatto deriva la **sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare, dei dati (n. 1, 1.3)**.

Sotto il profilo dell'inasprimento delle pene:

- nella fattispecie aggravata ai sensi del secondo comma è prevista la pena della **reclusione da 2 a 10 anni** (attualmente è da 1 a 5 anni) (**n. 1, 1.1**);
- nella fattispecie aggravata ai sensi del terzo comma è prevista la pena della **reclusione da 3 a 10 anni** (attualmente è da 1 a 5 anni) (**n. 2, 2.1**);
- nella fattispecie pluriaggravata in cui ricorrono l'aggravante di cui al terzo comma nonché taluna delle aggravanti di cui al secondo comma è prevista la pena della **reclusione da 4 a 12 anni** (attualmente è da 3 a 8 anni) (**n. 2, 2.1**);
- qualora concorrano le aggravanti di cui al secondo comma, n. 3, e al terzo comma (vale a dire se il fatto è commesso su un sistema di interesse militare o relativo all'ordine pubblico, alla sicurezza pubblica, alla sanità o alla protezione civile e se ne deriva la distruzione o il danneggiamento del sistema o la sottrazione dei dati) è previsto il **divieto di equivalenza o prevalenza delle attenuanti** (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo previste dall'introducendo art. 623-*quater*, su cui *vedi infra*) e che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti (**n. 2, 2.1**).

In riferimento al **divieto di prevalenza delle attenuanti sulle aggravanti**, si ricorda che, di recente, la Corte costituzionale con la sentenza 197/2023 ha dichiarato l'illegittimità costituzionale dell'art. 577, terzo comma, del codice penale nella parte in cui vieta al giudice, in caso di omicidio commesso in danno di un ascendente, discendente, coniuge o convivente, ai sensi del medesimo art. 577, primo comma, n. 1), di comminare la pena a seguito del giudizio di bilanciamento, *ex art. 69 c.p.*, tra circostanze aggravanti ed attenuanti, in particolare operando una valutazione circa la possibile prevalenza di queste ultime, con specifico riguardo a quelle di cui agli artt. 62, primo comma, numero 2) (attenuante della provocazione), e 62-*bis*, del codice penale (attenuanti generiche).

Nelle motivazioni la Corte, citando la propria sentenza n. 73 del 2020, ricorda che la pena deve essere «adeguatamente calibrata non solo al concreto contenuto di offensività del fatto di reato per gli interessi protetti, ma anche al disvalore soggettivo espresso dal fatto medesimo», e che quest'ultimo «dipende in maniera determinante non solo dal contenuto della volontà criminosa (dolosa o colposa) e dal grado del dolo o della colpa, ma anche dalla eventuale presenza di fattori che hanno influito sul processo motivazionale dell'autore, rendendolo più o meno rimproverabile».

In questo senso, il «flessibile strumento del bilanciamento tra le circostanze» può essere considerato espressione diretta dei principi costituzionali di proporzionalità e individualizzazione della pena desumibili dagli artt. 3 e 27, terzo comma, Cost.»

Derogare al regime del bilanciamento – afferma la Corte - è certamente consentito al legislatore nell'esercizio della propria discrezionalità, purché la deroga sia conforme ai principi costituzionali.

La Corte ha ritenuto che il divieto di prevalenza di cui all'art. 577, terzo comma, c.p., violasse l'art. 3 Cost., rilevando fra l'altro la «intrinseca irragionevolezza» della previsione per cui «una sola circostanza aggravante [...] abbia l'effetto di impedire un giudizio di prevalenza di una pluralità di circostanze attenuanti».

**Il comma 1, lett. b), modifica l'art. 615-*quater* c.p. (*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*).**

L'art. 615-*quater* c.p. nel testo attualmente vigente punisce con la reclusione fino a 2 anni e con la multa fino a euro 5.164 chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Ai sensi del secondo comma si applica la reclusione da 1 a 3 anni e la multa da euro 5.164 a euro 10.329 se il fatto è commesso in danno di un **sistema utilizzato dallo Stato, da un ente pubblico o da un'impresa che esercita servizi pubblici o di pubblica necessità**, da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da un **investigatore privato** anche abusivo, o con abuso della qualità di **operatore di sistema**.

La disposizione in commento modifica, in primo luogo, la definizione della fattispecie delittuosa, ampliando il dolo specifico previsto per la configurabilità della fattispecie operando la sostituzione della nozione di

“profitto” prevista dal testo vigente con quella, più ampia, di “vantaggio” (n. 1).

Inoltre, vengono ridefinite le aggravanti, prevedendo:

- la pena della **reclusione da 2 a 6 anni** (anziché da 1 a 3 anni) se il fatto è commesso da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da parte di un **investigatore privato** anche abusivo, o con abuso della qualità di **operatore di sistema** (n. 2);
- la pena della **reclusione da 3 a 8 anni** se il fatto è commesso su **sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico** (tale definizione, operata mediante rinvio all'art. 615-ter, terzo comma, primo periodo, sostituisce quella della commissione del fatto in danno di un sistema utilizzato dallo Stato o da enti pubblici o da imprese esercenti servizi pubblici prevista dal testo vigente<sup>4</sup>) (n. 3).

Il **comma 1, lett. d**, interviene sull'art. 617-bis c.p. (*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche e telefoniche*).

L'art. 617-bis nel testo vigente punisce con la **reclusione da 1 a 4 anni** chiunque, fuori dei casi consentiti dalla legge, al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti o parti di apparati o di strumenti idonei a intercettare, impedire o interrompere le predette comunicazioni o conversazioni.

È prevista la circostanza aggravante affetto speciale, con l'applicazione della **reclusione da 1 a 5 anni**, della commissione del fatto **in danno di un pubblico ufficiale** nell'esercizio o a causa delle sue funzioni o **da parte di un pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri o da un **investigatore privato** anche abusivo (secondo comma).

---

<sup>4</sup> Secondo quanto precisato nella relazione illustrativa con riferimento alla modifica di analogo tenore introdotta dalla lett. e) al quarto comma dell'art. 617-quater c.p., si tratta di un “riallineamento, di natura sistematica (...) al sistema delle aggravanti previste per l'accesso abusivo a sistema informatico”.

La disposizione in commento dopo il primo comma dell'art. 617-*bis* inserisce un ulteriore comma volto a prevedere una **circostanza aggravante**, con l'applicazione della **reclusione da 2 a 6 anni**, qualora ricorra taluna delle circostanze di cui all'art. 615-*ter*, secondo comma, n. 1, vale a dire la **commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da un **investigatore privato** anche abusivo, o con abuso della qualità di **operatore di sistema**.

Tale circostanza aggravante assorbe pertanto parzialmente la fattispecie prevista dal vigente secondo comma (terzo comma a seguito delle modifiche introdotte dalla disposizione in commento), che viene conseguentemente modificato al fine di coordinare le due disposizioni.

Il testo risultante dalle modifiche prevede, dunque, l'aggravante, con reclusione da 2 a 6 anni, se il fatto è commesso da determinate categorie di soggetti (pubblico ufficiale, investigatore privato, operatore di sistema), e l'aggravante, con reclusione da 1 a 5 anni, per la commissione del fatto in danno di un pubblico ufficiale.

Il **comma 1, lett. e)**, interviene sull'art. 617-*quater* c.p. (***Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche***).

L'art. 617-*quater* c.p. nel testo attualmente vigente punisce con la **reclusione da 1 anno e 6 mesi a 5 anni** chiunque fraudolentemente **intercetta** comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le **impedisce** o le **interrompe**, e chiunque, salvo che il fatto costituisca più grave reato, rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni (primo e secondo comma). Il reato è punibile a querela (terzo comma).

Si procede d'ufficio e si applica la pena della **reclusione da 3 a 8 anni** se il fatto è commesso in danno di un **sistema utilizzato dallo Stato, da un ente pubblico o da un'impresa che esercita servizi pubblici o di pubblica necessità**, da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, con abuso della qualità di **operatore di sistema** o da chi esercita **abusivamente** la professione di **investigatore privato** (quarto comma).

La disposizione in commento reca, in primo luogo, alcune **modifiche** al quarto comma in materia di **aggravanti**, concernenti:

- l'innalzamento della pena prevista per le fattispecie aggravate, con la previsione della **reclusione da 4 a 10 anni** (anziché da 3 a 8 anni) (**n. 1, 1.1**);

- la previsione dell'aggravante della commissione del fatto su **sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico** (tale definizione, operata mediante rinvio all'art. 615-ter, terzo comma, primo periodo, sostituisce quella della commissione del fatto in danno di un sistema utilizzato dallo Stato o da enti pubblici o da imprese esercenti servizi pubblici prevista dal testo vigente<sup>5</sup>) (**n. 1, 1.2**);
- la previsione dell'aggravante della commissione del fatto **in danno di un pubblico ufficiale** nell'esercizio o a causa delle sue funzioni (in aggiunta a quella, già prevista, della commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri o da chi esercita abusivamente la professione di investigatore privato anche abusivo) (**n. 1, 1.3 e 1.4**);
- l'introduzione del **divieto di equivalenza o prevalenza delle attenuanti** (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo, su cui *vedi infra*, previste dall'introducendo art. 623-quater) sull'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, prevedendo che le diminuzioni di pena si operino sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Sulla giurisprudenza costituzionale in materia di divieto di prevalenza delle attenuanti si veda *sopra*.

Il **comma 1, lett. f)**, interviene sull'art. 617-quinquies c.p. (***Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche***).

L'art. 617-quinquies c.p. nel testo attualmente vigente punisce con la **reclusione da 1 a 4 anni** chiunque fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere

---

<sup>5</sup> Secondo quanto precisato nella relazione illustrativa, si tratta di un "riallineamento, di natura sistematica (...) al sistema delle aggravanti previste per l'accesso abusivo a sistema informatico".



comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi (primo comma).

Si applica – in virtù del richiamo al quarto comma dell’art. 617-*quater* - la pena della **reclusione da 1 a 5 anni** se il fatto è commesso in danno di un **sistema utilizzato dallo Stato, da un ente pubblico o da un’impresa che esercita servizi pubblici o di pubblica necessità**, da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, con abuso della qualità di **operatore di sistema** o da chi esercita **abusivamente** la professione di **investigatore privato** (secondo comma).

La disposizione in commento reca **modifiche alla disciplina delle aggravanti**, innalzando le pene e ridefinendo le fattispecie, analogamente a quanto previsto dalla lett. *e*) per l’art. 617-*quater*.

In particolare, si prevede:

- la previsione – mediante rinvio all’art. 617-*quater*, quarto comma, n. 2, come modificato dalla lett. *e*) - dell’aggravante, con applicazione della **reclusione da 2 a 6 anni**, della commissione del fatto **in danno di un pubblico ufficiale** nell’esercizio o a causa delle sue funzioni (in aggiunta a quella, già prevista, della commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri o da chi esercita abusivamente la professione di investigatore privato anche abusivo) (**n. 1**);
- la previsione dell’aggravante, con applicazione della **reclusione da 3 a 8 anni**, della commissione del fatto su **sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico** (tale definizione è operata mediante rinvio all’art. 617-*quater*, quarto comma, n. 1, come modificato dalla lett. *e*)<sup>6</sup>) (**n. 2**);
- l’introduzione del **divieto di equivalenza o prevalenza delle attenuanti** (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo previste dall’introducendo art. 623-*quater*, su cui *vedi infra*,) sull’aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse

<sup>6</sup> Secondo quanto precisato nella relazione illustrativa con riferimento alla modifica di analogo tenore introdotta dalla lett. *e*) al quarto comma dell’art. 617-*quater* c.p., si tratta di un “riallineamento, di natura sistematica (...) al sistema delle aggravanti previste per l’accesso abusivo a sistema informatico”.

pubblico, prevedendo che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Sulla giurisprudenza costituzionale in materia di divieto di prevalenza delle attenuanti *vedi sopra*.

Il **comma 1, lett. g)**, interviene sull'art. 617-*sexies* c.p. (***Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche***).

L'art. 617-*sexies* c.p. nel testo attualmente vigente punisce con la **reclusione da 1 a 4 anni** chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi (primo comma).

Si applica – in virtù del richiamo al **quarto comma dell'art. 617-*quater*** - la pena della **reclusione da 1 a 5 anni** se il fatto è commesso in danno di un **sistema utilizzato dallo Stato, da un ente pubblico o da un'impresa che esercita servizi pubblici o di pubblica necessità**, da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, con abuso della qualità di **operatore di sistema** o da chi esercita **abusivamente** la professione di **investigatore privato** (secondo comma).

La fattispecie non aggravata è punibile a querela (terzo comma).

La disposizione in commento prevede:

- l'**innalzamento della pena** per la fattispecie aggravata, per la quale si prevede la **reclusione da 3 a 8 anni** (anziché da 1 a 5 anni) (**n. 1**);
- la contestuale **ridefinizione della medesima fattispecie aggravata**, in virtù delle modifiche introdotte dalla lett. *e*), n. 1, del disegno di legge in esame al quarto comma dell'art. 617-*quater* (sulle quali *vedi sopra*), in quanto il richiamo contenuto nel secondo comma dell'art. 617-*sexies* non viene modificato (**n. 2**);
- l'introduzione del **divieto di equivalenza o prevalenza delle attenuanti** (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo previste dall'introducendo art. 623-*quater*, su cui *vedi infra*.) sull'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, prevedendo che le diminuzioni di pena si operano sulla

quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Sulla giurisprudenza costituzionale in materia di divieto di prevalenza delle attenuanti *vedi sopra*.

Il **comma 1, lett. h)**, reca una **disposizione di coordinamento** volta a modificare la rubrica del capo III-bis del titolo XII del libro secondo del codice penale, ora denominata “*Disposizioni comuni*”, conseguentemente all'introduzione dell'art. 623-*quater* (*vedi infra*).

Il **comma 1, lett. i)**, prevede l'**inserimento** nel codice penale dell'**art. 623-*quater*** in materia di **circostanze attenuanti** per i delitti di cui agli artt. 615-*ter* (*Accesso abusivo a un sistema informatico 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* (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*) del codice penale.

Sono previste:

- una **circostanza attenuante a effetto comune** (diminuzione della pena fino a un terzo) quando il fatto sia di **lieve entità**, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo (primo comma del nuovo art. 623-*quater*);
- una **circostanza attenuante a effetto speciale** (diminuzione della pena dalla metà a due terzi) in favore di chi **si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze**, anche **aiutando concretamente l'autorità giudiziaria o l'autorità di polizia** nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi (secondo comma del nuovo art. 623-*quater*).

Alle predette attenuanti **non si applica il divieto di prevalenza** sancito dall'art. 69, quarto comma, c.p. (terzo comma del nuovo art. 623-*quater*).

Ai sensi dell'art. 69, quarto comma, c.p., vi è divieto di prevalenza delle attenuanti sulle circostanze aggravanti di cui all'art. 99 (recidiva), 111 (determinazione al reato di persona non imputabile o non punibile) e 112, primo comma, n. 4 (aggravanti previste nel caso di concorso: partecipazione di 5 o più persone, per i promotori od organizzatori, per chi ha determinato a commettere il reato persone sottoposte alla propria autorità o vigilanza o responsabilità genitoriale).

**Il comma 1, lett. l), aggiunge un comma all'art. 629 c.p. (*Estorsione*).**

L'art. 629 c.p. punisce con la reclusione da 5 a 10 anni e con la multa da euro 1.000 a euro 4.000 chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno.

La pena è della reclusione da 7 a 20 anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze aggravanti del delitto di rapina.

Il comma aggiuntivo introdotto dalla disposizione in commento prevede la fattispecie del delitto di **estorsione mediante reati informatici**, realizzata dalla costrizione di taluno a fare o ad omettere qualche cosa, procurando a sé o ad altro un ingiusto profitto, **mediante le condotte, o la minaccia di compierle**, di cui ai seguenti reati: artt. 615-ter (*Accesso abusivo ad un sistema informatico o telematico*), 617-*quater* (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*), 617-*sexies* (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*), 635-*bis* (*Danneggiamento di informazioni, dati e programmi informatici*), 635-*quater* (*Danneggiamento di sistemi informatici o telematici*) e 635-*quinquies* (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*).

Si prevede che la nuova fattispecie delittuosa sia punita con la **reclusione da 6 a 12 anni** e con la **multa da euro 5.000 a euro 10.000**.

Si prevede la **reclusione da 8 a 22 anni** e la **multa da euro 6.000 a euro 18.000** se ricorre taluna delle circostanze "indicate nell'ultimo capoverso dell'articolo precedente".

Tale rinvio va presumibilmente interpretato come riferito al vigente terzo comma dell'art. 628, in considerazione del fatto che l'identico rinvio contenuto nel secondo comma dell'art. 629 è stato costantemente interpretato dalla giurisprudenza, anche dopo l'aggiunta di commi successivi, come riferito al terzo comma dell'art. 628, che enumera le circostanze aggravanti del delitto di rapina.

Si ricorda che ai sensi dell'art. 628 c.p. sono circostanze aggravanti del delitto di rapina l'aver commesso il fatto: con armi, da persona travisata, o da più persone riunite; ponendo taluno in stato di incapacità di volere o di agire; da parte di appartenenti a un'associazione mafiosa; nei confronti di persona ultrasessantacinquenne; nonché (ma si tratta di ipotesi difficilmente configurabili per il delitto di estorsione) in un luogo di privata dimora, all'interno di mezzi di pubblico trasporto, nei pressi di banche, uffici postali e bancomat nei confronti di chi abbia fruito dei relativi servizi.

*Si rileva come il richiamo all' "ultimo capoverso dell'articolo precedente", pur riproducendo quello di cui al vigente secondo comma dell'art. 629 c.p., appare non pienamente conforme ai criteri indicati dalla [Guida alla redazione dei testi normativi](#) di cui alla Circolare della Presidenza del Consiglio dei ministri 2 maggio 2001, ai sensi della quale "Per le citazioni e le "novelle" relative ai codici penali si utilizzano, anche nel virgolettato, la denominazione "comma" o "periodo". Non sono pertanto utilizzate le denominazioni originariamente in uso in tali testi ("prima parte" e "capoverso")" (punto 3.3). Inoltre, "va evitato l'uso delle espressioni "precedente" e "successivo". Tali espressioni sono superflue, stante la necessità di citare sempre il numero degli articoli e dei commi, e d'altra parte possono determinare problemi di coordinamento e dubbi di individuazione in caso di modifiche successive al testo" (punto 1.91., lett. d).*

*Si valuti, pertanto, l'opportunità di sostituire il richiamo all' "ultimo capoverso dell'articolo precedente" con un richiamo puntuale al comma e all'articolo cui si intende fare riferimento, nel rispetto dei criteri indicati dalla Guida alla redazione dei testi normativi sopra menzionati.*

**Il comma 1, lett. m,** interviene sull'art. 635-*bis* c.p. (**Danneggiamento di informazioni, dati e programmi informatici**).

L'art. 635-*bis* c.p. punisce con la reclusione da 6 mesi a 3 anni, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. Il delitto è punibile a querela (primo comma).

Il secondo comma prevede quali circostanze aggravanti, con l'applicazione della reclusione da 1 a 4 anni, la commissione del fatto con violenza alla persona o con minaccia o con abuso della qualità di operatore del sistema.

La disposizione in commento prevede:

- **l'innalzamento della pena** per la fattispecie semplice, prevedendo la **reclusione da 2 a 6 anni** (anziché da 6 mesi a 3 anni);

- l'ampliamento della fattispecie aggravata, prevedendo che essa ricorra se il fatto è commesso:
  - **da parte di un pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da un **investigatore privato** anche abusivo (oltre che con abuso della qualità di operatore di sistema, come già previsto dal testo vigente);
  - usando **violenza o minaccia** o da parte di **persona palesemente armata** (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata);
- l'**innalzamento della pena** per la fattispecie aggravata, prevedendo la **reclusione da 3 a 8 anni** (anziché da 1 a 4 anni).

Il **comma 1, lett. n**, interviene sull'art. 635-ter c.p. (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*).

L'art. 635-ter c.p., nel testo attualmente vigente, punisce con la reclusione da 1 a 4 anni, salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

E' prevista la circostanza aggravante, con l'applicazione della reclusione da 3 a 8 anni, della distruzione, deterioramento, cancellazione, alterazione o soppressione delle informazioni, dei dati o dei programmi (secondo comma).

È altresì prevista la circostanza aggravante a effetto comune (aumento della pena fino a un terzo) della commissione del fatto con violenza o minaccia o con abuso della qualità di operatore di sistema (terzo comma).

La disposizione in commento interviene, in primo luogo, sulla **definizione della fattispecie delittuosa**, prevedendo che i fatti descritti debbano essere diretti a distruggere, deteriorare, cancellare, alterare o sopprimere **informazioni, dati o programmi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico (n. 1)**.

Tale definizione, mutuata dal vigente art. 615-ter, terzo comma - relativo alle circostanze aggravanti del delitto di accesso abusivo a un sistema informatico o telematico - sostituisce quella della commissione del fatto in danno di un sistema utilizzato dallo Stato o da enti pubblici o da imprese esercenti servizi pubblici prevista dal testo vigente. Viene conseguentemente modificata anche la **rubrica** dell'articolo (**n. 3**).

La disposizione in commento interviene, inoltre, sulle circostanze aggravanti, sostituendo il secondo comma dell'articolo<sup>7</sup> (**n. 2**).

Sono previste quali circostanze aggravanti, con l'applicazione della pena della **reclusione da 3 a 8 anni**:

- la commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (il testo vigente fa riferimento solo all'abuso della qualità di operatore di sistema e prevede l'aumento della pena fino a un terzo) (nuovo secondo comma, n. 1);
- l'uso di violenza o minaccia o la commissione del fatto da parte di persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata ed è inasprito il trattamento sanzionatorio, prevedendo il testo vigente l'aumento della pena fino a un terzo) (nuovo secondo comma, n. 2);
- la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi (rispetto al testo vigente, l'aggravante è estesa alle ipotesi di sottrazione o inaccessibilità dei dati o dei programmi) (nuovo secondo comma, n. 3).

La disposizione in commento sostituisce altresì il terzo comma dell'articolo prevedendo, nel caso di **concorso** di taluna delle **circostanze di cui ai nn. 1 e 2** del secondo comma e della **circostanza di cui al n. 3**:

- la pena della reclusione da 4 a 12 anni;
- il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo previste dall'introducendo art. 623-*quater*, su cui *vedi infra*), prevedendo inoltre che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Sulla giurisprudenza costituzionale in materia di divieto di prevalenza delle attenuanti *vedi sopra*.

---

<sup>7</sup> Secondo quanto precisato nella relazione illustrativa, l'intervento è finalizzato a uniformare l'elencazione delle aggravanti a quella recata dall'art. 615-*ter*, secondo comma.

Il **comma 1, lett. o)**, interviene sull'art. 635-*quater* c.p.p. (***Danneggiamento di sistemi informatici o telematici***).

L'art. 635-*quater* c.p., nel testo attualmente vigente, punisce con la reclusione da 1 a 5 anni, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-*bis* (*vedi sopra*) ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento (primo comma).

È prevista la circostanza aggravante a effetto comune (aumento della pena fino a un terzo) della commissione del fatto con violenza o minaccia o con abuso della qualità di operatore di sistema (secondo comma).

La disposizione in commento prevede (con modifiche analoghe a quelle previste per l'art. 635-*bis*, *vedi sopra*):

- l'**innalzamento della pena** per la fattispecie semplice, prevedendo la **reclusione da 2 a 6 anni** (anziché da 1 a 5 anni);
- l'ampliamento della fattispecie aggravata, prevedendo che essa ricorra se il fatto è commesso:
  - **da parte di un pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da un **investigatore privato** anche abusivo (oltre che con abuso della qualità di operatore di sistema, come già previsto dal testo vigente);
  - usando **violenza o minaccia** o da parte di **persona palesemente armata** (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata);
- la ridefinizione della pena per la fattispecie aggravata, prevedendo la **reclusione da 3 a 8 anni** (anziché l'aumento fino a un terzo previsto dal testo vigente).

Il **comma 1, lett. p)**, introduce nel codice penale l'art. 635-*quater.1* (***Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico***).

Il primo comma del nuovo articolo riproduce il vigente art. 615-*quinquies* c.p.<sup>8</sup> (che viene contestualmente abrogato dalla **lett. c)**: è punito con la **reclusione fino a 2 anni** e con la **multa fino a euro 10.329**

---

<sup>8</sup> La relazione illustrativa riporta che l'intervento risponde ad esigenze di riordino sistematico, giacché la disposizione viene ricollocata nel più appropriato contesto dei delitti di danneggiamento.



chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Il secondo e il terzo comma prevedono quali circostanze aggravanti:

- la commissione del fatto da parte di un **pubblico ufficiale o incaricato di pubblico servizio** con abuso dei poteri o con violazione dei doveri, da un **investigatore privato** anche abusivo, o con abuso della qualità di **operatore di sistema (reclusione da 2 a 6 anni)**, previsione operata tramite il rinvio alle circostanze di cui all'art. 615-ter, secondo comma, n. 1;
- la commissione del fatto su **sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico (reclusione da 3 a 8 anni)**, previsione operata tramite il rinvio all'articolo 615-ter, terzo comma, primo periodo.

Il **comma 1, lett. q)**, sostituisce l'art. 635-quinquies c.p. (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*).

L'art. 635-quinquies c.p. nel testo attualmente vigente punisce con la reclusione da 1 a 4 anni chiunque commette i fatti di cui all'art. 635-quater al fine di distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento (primo comma).

Il secondo comma prevede la reclusione da 3 a 8 anni se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

Il terzo comma prevede la circostanza aggravante a effetto comune (aumento della pena fino a un terzo) se il fatto è commesso con violenza alla persona o minaccia o con abuso della qualità di operatore di sistema.

Il **nuovo art. 635-quinquies**, come sostituito dalla disposizione in commento, reca la rubrica: *Danneggiamento di sistemi informatici o telematici di pubblico interesse*.

Il primo comma punisce – salvo che il fatto costituisca più grave reato – con la **reclusione da 2 a 6 anni**, chiunque, mediante le condotte di cui all'art. 635-bis (*vedi sopra*) ovvero mediante l'introduzione o la

trasmissione di dati, informazioni o programmi compie atti diretti a **distruggere, danneggiare, rendere**, in tutto o in parte, **inservibili sistemi informatici o telematici di pubblico interesse** ovvero ad **ostacolarne gravemente il funzionamento**.

Rispetto al testo vigente si prevede, dunque, l'**innalzamento della pena** e la sostituzione della nozione di servizi informatici o telematici di pubblica utilità con quella di **servizi informatici o telematici di pubblico interesse**.

Quanto alle modalità della condotta la disciplina vigente non è sostanzialmente innovata, in quanto - secondo quanto precisato nella relazione illustrativa - la nuova formulazione si limita a riprodurre estensivamente la descrizione della fattispecie che, nel testo vigente, è operata mediante rinvio all'art. 635-*quater*.

Il secondo comma disciplina le circostanze aggravanti, prevedendo quali circostanze aggravanti, con l'applicazione della pena della **reclusione da 3 a 8 anni**:

- la commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (il testo vigente fa riferimento solo all'abuso della qualità di operatore di sistema e prevede l'aumento della pena fino a un terzo) (n. 1);
- l'uso di violenza o minaccia o la commissione del fatto da parte di persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata ed è inasprito il trattamento sanzionatorio, prevedendo il testo vigente l'aumento della pena fino a un terzo) (n. 2);
- la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni dei dati o dei programmi (il testo vigente prevede l'aggravante nel caso di distruzione, danneggiamento o inservibilità del sistema) (n. 3).

Il terzo comma prevede, nel caso di **concorso** di taluna delle **circostanze di cui ai nn. 1 e 2** del secondo comma e di taluna delle **circostanze di cui al n. 3**:

- la pena della reclusione da 4 a 12 anni;
- il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve

entità e del recesso attivo previste dall'introducendo art. 639-ter, su cui *vedi infra*), specificando che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Sulla giurisprudenza costituzionale in materia di divieto di prevalenza delle attenuanti *vedi sopra*.

Il **comma 1, lett. r)**, prevede l'inserimento nel codice penale dell'art. 639-ter in materia di circostanze attenuanti per i delitti di cui agli artt. del codice penale 629, terzo comma, introdotto dalle lett. l) (*Estorsione mediante reati informatici, vedi sopra*), 635-ter (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), 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, come modificato alla lett. q) (*Danneggiamento di sistemi informatici o telematici di pubblico interesse*).

Sono previste:

- una **circostanza attenuante a effetto comune** (diminuzione della pena fino a un terzo) quando il fatto sia di **lieve entità**, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo (primo comma del nuovo art. 639-ter);
- una **circostanza attenuante a effetto speciale** (diminuzione della pena dalla metà a due terzi) in favore di chi **si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze**, anche **aiutando concretamente l'autorità giudiziaria o l'autorità di polizia** nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi (secondo comma del nuovo art. 639-quater).

Alle predette attenuanti **non si applica il divieto di prevalenza** sancito dall'art. 69, quarto comma, c.p. (terzo comma del nuovo art. 639-quater).

Ai sensi dell'art. 69, quarto comma, c.p., vi è divieto di prevalenza delle attenuanti sulle circostanze aggravanti di cui all'art. 99 (recidiva), 111 (determinazione al reato di persona non imputabile o non punibile) e 112, primo comma, n. 4 (aggravanti previste nel caso di concorso: partecipazione di 5 o più persone, per i promotori od organizzatori, per chi ha determinato a commettere il reato persone sottoposte alla propria autorità o vigilanza o responsabilità genitoriale).

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
Art. 615-ter (Accesso abusivo ad un sistema informatico o telematico)	Art. 615-ter (idem)
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.	<i>Identico</i>
	<i>[Art. 11, co. 1, lett. a), n. 1]</i>
La pena è della reclusione da <b>uno a cinque</b> anni:  1) se il fatto è 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;  2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;  3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.	La pena è della reclusione da <b>due a dieci</b> anni:  <i>Identico</i>  2) se il colpevole per commettere il fatto usa <b>minaccia o</b> violenza sulle cose o alle persone, ovvero se è palesemente armato;  3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento <b>ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare</b> dei dati, delle informazioni o dei programmi in esso contenuti.
	<i>[Art. 11, co. 1, lett. a), n. 2]</i>
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza	Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
<p>pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione <b>da uno a cinque anni e da tre a otto anni.</b></p>	<p>pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione <b>da tre a dieci anni e da quattro a dodici anni.</b></p> <p><b>Nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-quater non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.</b></p>
<p>Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.</p>	<p><i>Identico</i></p>
<p>Art. 615-quater (<i>Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici</i>)</p>	<p>Art. 615-quater (<i>idem</i>)</p>
	<p>[Art. 11, co. 1, lett. b), n. 1]</p>
<p>Chiunque, al fine di procurare a sé o ad altri un <b>profitto</b> o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.</p>	<p>Chiunque, al fine di procurare a sé o ad altri un <b>vantaggio</b> o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.</p>

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
	<i>[Art. 11, co. 1, lett. b), n. 2]</i>
<b>La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-<i>quater</i>.</b>	<b>La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-<i>ter</i>, secondo comma, numero 1).</b>
	<i>[Art. 11, co. 1, lett. b), n. 3]</i>
	<b>La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-<i>ter</i>, terzo comma, primo periodo.</b>
	<i>[Art. 11, co. 1, lett. c)]</i>
<i>Art. 615-<i>quinqüies</i> (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)</i>	<i>Art. 615-<i>quinqüies</i> (idem)</i>
<b>Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.</b>	<b><i>Abrogato</i></b>

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
Art. 617-bis <i>(Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche)</i>	Art. 617-bis <i>(idem)</i>
Comma 1 <i>Omissis.</i>	Comma 1 <i>Omissis.</i>
	<i>[Art. 11, co. 1, lett. d), n.1]</i>
	<b>La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).</b>
	<i>[Art. 11, co. 1, lett. d), n.2]</i>
La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni <b>ovvero 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 servizio o da chi esercita anche abusivamente la professione di investigatore privato.</b>	<b>La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni.</b>
Art. 617-quater <i>(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)</i>	Art. 617-quater <i>(idem)</i>
Commi da 1 a 3 <i>Omissis</i>	Commi da 1 a 3 <i>Omissis</i>
	<i>[Art. 11, co. 1, lett. e), n.1]</i>
Tuttavia si procede d'ufficio e la pena è della reclusione da <b>tre a otto</b> anni se il fatto è commesso:  <b>1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da</b>	Tuttavia si procede d'ufficio e la pena è della reclusione da <b>quattro a dieci</b> anni se il fatto è commesso:  <b>1) in danno di taluno dei sistemi informatici o telematici indicati</b>

Codice penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
<p>altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;</p> <p>2) <b>da un pubblico ufficiale</b> o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, <b>ovvero</b> con abuso della qualità di operatore del sistema;</p> <p>3) <b>da chi esercita anche abusivamente la professione di investigatore privato.</b></p>	<p>nell'articolo 615-ter, terzo comma, primo periodo;</p> <p>2) <b>in danno di un pubblico ufficiale, nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale</b> o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, <b>o da chi esercita, anche abusivamente, la professione di investigatore privato,</b> o con abuso della qualità di operatore del sistema;</p> <p><b>Abrogato</b></p>
	<i>[Art. 11, co. 1, lett. e), n.2]</i>
	<p><b>Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-<i>quater</i>, concorrenti con l'aggravante di cui al quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.</b></p>
<p>Art. 617-<i>quinqüies</i> (<i>Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche</i>)</p>	<p>Art. 617-<i>quinqüies</i> (<i>idem</i>)</p>
Comma 1 <i>Omissis</i>	Comma 1 <i>Omissis</i>
	<i>[Art. 11, co. 1, lett. f), n.1]</i>
<p><b>La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-<i>quater</i>.</b></p>	<p><b>Quando ricorre taluna delle circostanze di cui all'articolo 617-<i>quater</i>, quarto comma, numero 2), la pena è della reclusione da due a sei</b></p>



Codice penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
	anni
	<i>[Art. 11, co. 1, lett. f), n.2]</i>
	<p>Quando ricorre taluna delle circostanze di cui all'articolo 617-<i>quater</i>, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.</p> <p>Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-<i>quater</i>, concorrenti con l'aggravante di cui all'articolo 617-<i>quater</i>, quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.</p>
Art. 617- <i>sexies</i> (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)	Art. 617- <i>sexies</i> ( <i>idem</i> )
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.	<i>Identico</i>
	<i>[Art. 11, co. 1, lett. g), n. 1]</i>
La pena è della reclusione da <b>uno a cinque</b> anni nei casi previsti dal quarto comma dell'articolo 617- <i>quater</i> .	La pena è della reclusione da <b>tre a otto</b> anni nei casi previsti dal quarto comma dell'articolo 617- <i>quater</i> .

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
	<i>[Art. 11, co. 1, lett. g), n. 2]</i>
	<b>Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-<i>quater</i>, concorrenti con l'aggravante di cui all'articolo 617-<i>quater</i>, quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta circostanza aggravante.</b>
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.	<i>Identico</i>
	<i>[Art. 11, co. 1, lett. h)]</i>
<b>Capo III-<i>bis</i></b> <i>(Disposizioni comuni sulla procedibilità)</i>	<b>Capo III-<i>bis</i></b> <i>(Disposizioni comuni)</i>
	<i>[Art. 11, co. 1, lett. i)]</i>
	<b>Art. 623-<i>quater</i></b> <i>(Circostanze attenuanti)</i>
	<b>Le pene comminate per i delitti di cui agli articoli 615-<i>ter</i>, 615-<i>quater</i>, 617-<i>quater</i>, 617-<i>quinquies</i> e 617-<i>sexies</i> sono diminuite quando, per la natura, la specie, i mezzi, le modalità o circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità. Le pene previste per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel</b>

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
	<p>recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.</p> <p>Non si applica il divieto di cui all'articolo 69, quarto comma.</p>
Art. 629 ( <i>Estorsione</i> )	Art. 629 ( <i>idem</i> )
Commi 1 e 2 <i>Omissis</i>	Comma 1 e 2 <i>Omissis</i>
	[Art. 11, co. 1, lett. l)]
	<p><b>Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente</b></p>
Art. 635-bis ( <i>Danneggiamento di informazioni, dati e programmi informatici</i> )	Art. 635-bis ( <i>idem</i> )
	[Art. 11, co. 1, lett. m)]
Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da <b>sei mesi a tre anni</b> .	Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da <b>due a sei anni</b> .
<b>Se il fatto è commesso con violenza alla persona o con minaccia ovvero con</b>	<b>La pena è della reclusione da tre a otto anni:</b>

Codice penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.	<p>1) se il fatto è 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;</p> <p>2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.</p>
	<i>[Art. 11, co. 1, lett. n), n.3]</i>
Art. 635-ter <i>(Danneggiamento di informazioni, dati e programmi informatici <b>utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità</b>)</i>	Art. 635-ter <i>(Danneggiamento di informazioni, dati e programmi informatici <b>pubblici o di interesse pubblico</b>)</i>
	<i>[Art. 11, co. 1, lett. n), n.1]</i>
Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici <b>utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità</b> , è punito con la reclusione da uno a quattro anni.	Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici <b>di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico</b> , è punito con la reclusione da due a sei anni.
	<i>[Art. 11, co. 1, lett. n), n.2]</i>
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.	<p>La pena è della reclusione da tre a otto anni:</p> <p>1) se il fatto è 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</p>

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
	<p><b>investigatore privato, o con abuso della qualità di operatore del sistema;</b></p> <p><b>2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;</b></p> <p><b>3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.</b></p>
<p><b>Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.</b></p>	<p><b>La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3); in tal caso, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 639-ter non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.</b></p>
<p><i>Art. 635-quater (Danneggiamento di sistemi informatici o telematici)</i></p>	<p><i>Art. 635-quater (Danneggiamento di sistemi informatici o telematici)</i></p>
	<p><i>[Art. 11, co. 1, lett. o), n. 1]</i></p>
<p>Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il</p>	<p>Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il</p>

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
funzionamento è punito con la reclusione da <b>uno a cinque</b> anni.	funzionamento è punito con la reclusione da <b>due a sei</b> anni.
	<i>[Art. 11, co. 1, lett. o), n. 2]</i>
<b>Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.</b>	<p><b>La pena è della reclusione da tre a otto anni:</b></p> <p>1) se il fatto è 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;</p> <p>2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.</p>
	<i>[Art. 11, co. 1, lett. p)]</i>
	<p><b>Art. 635-quater.1</b>  <i>(Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)</i></p>
	<p><b>Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.</b></p>

Codice penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
	<p>La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).</p> <p>La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma, primo periodo.</p>
<p>Art. 635-quinquies (Danneggiamento di sistemi informatici o telematici di <b>pubblica utilità</b>)</p>	<p>Art. 635-quinquies (Danneggiamento di sistemi informatici o telematici di <b>pubblico interesse</b>)</p>
	<p>[Art. 11, co. 1, lett. q)]</p>
<p>Se il fatto di cui all'articolo 635-<i>quater</i> è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.</p>	<p>Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-<i>bis</i> ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.</p>
<p>Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.</p>	<p>La pena è della reclusione da tre a otto anni:</p> <ol style="list-style-type: none"> <li>1) se il fatto è 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;</li> <li>2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se</li> </ol>

Codice penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
	<p>è palesemente armato;</p> <p>3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.</p>
<p>Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.</p>	<p>La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3); in tal caso, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 639-ter non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.</p>
	<i>[Art. 11, co. 1, lett. r)]</i>
	<p><b>Art. 639-ter</b> <i>(Circostanze attenuanti)</i></p>
	<p>Le pene comminate per i delitti di cui agli articoli 629, terzo comma, 635-ter, 635-quater.1 e 635-quinquies sono diminuite quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità.</p>
	<p>Le pene comminate per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel</p>



---

<b>Codice penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
	<b>recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.</b>
	<b>Non si applica il divieto di cui all'articolo 69, quarto comma.</b>

## **Articolo 12** *(Modifiche al codice di procedura penale)*

L'**articolo 12** reca modifiche al codice di procedura penale finalizzate a recepire gli interventi in materia di prevenzione e contrasto dei reati informatici introdotte dal precedente articolo 11.

Per tali reati si prevedono: l'attribuzione della competenza sulle indagini alla **procura distrettuale**; la **deroga al regime ordinario per la proroga delle indagini preliminari**; termini di **durata** massima delle **indagini preliminari** pari a **2 anni**.

L'articolo 12, composto di un unico comma, ripartito in 3 lettere, introduce **modifiche** di natura procedurale **conseguenziali a quelle introdotte nel codice penale** dal precedente articolo 11.

La **lettera a)** interviene sull'art. 51, comma 3-*quinquies*, c.p.p., in materia di fattispecie delittuose di **competenza della procura distrettuale**, al fine di eliminare il riferimento al soppresso articolo 615-*quinquies* c.p. e di inserirvi tre nuove fattispecie delittuose ovvero:

- la detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, di cui all'art. 635-*quater*.1 c.p.;
- il danneggiamento di sistemi informatici o telematici di pubblico interesse, di cui all'art. 635-*quinquies* c.p.;
- la comunicazione di dati, informazioni o elementi di fatto falsi tesa a ostacolare o condizionare la formazione e trasmissione dell'elenco di reti, sistemi informatici e informativi da parte degli operatori compresi nel perimetro di sicurezza cibernetica, le procedure di affidamento delle forniture di strumenti destinati ai servizi e sistemi informatici, o le attività ispettive o di vigilanza su reti, sistemi informatici e servizi informatici, di cui all'articolo 1, comma 11, del decreto-legge n. 105 del 2019, convertito, con modificazioni, dalla legge n. 133 del 2019.

La **lettera b)** reca una modifica all'art. 406, comma 5-*bis*, c.p.p., volta ad includere i reati informatici contenuti nel numero 7-*ter* dell'articolo 407, comma 2, lettera *a)*, c.p.p., introdotto dalla successiva lettera *c)*, nell'ambito di applicazione della **deroga** ivi prevista **all'ordinario regime per la concessione della proroga** dei termini per lo svolgimento **delle indagini preliminari**.

Il **comma 5-bis** dell'art. 406 c.p.p. prevede infatti un regime semplificato per la concessione della proroga del termine per la conclusione delle indagini preliminari per i delitti di cui agli articoli 51, comma 3-*bis* c.p.p. e 407, comma 2, lettera *a*), numeri 4) e 7-*bis*), c.p.p. cui **si provvede con ordinanza del giudice entro 10 giorni dalla presentazione della richiesta**.

Il **regime ordinario** per la concessione della proroga del termine per le indagini preliminari, di cui ai commi 3, 4 e 5 del citato art. 406, comma 5-*bis*, c.p.p., prevede invece la **notifica della richiesta** alla persona sottoposta alle indagini nonché alla persona offesa dal reato che, nella notizia di reato o successivamente alla sua presentazione, abbia dichiarato di voler esserne informata, con l'avviso della **facoltà di presentare memorie** entro 5 giorni. Il giudice provvede quindi entro 10 giorni dalla scadenza del termine per la presentazione delle memorie: nel caso intenda concedere la proroga, emette **ordinanza in camera di consiglio** senza intervento del pubblico ministero e dei difensori, altrimenti **fissa la data dell'udienza in camera di consiglio** e ne fa notificare avviso al pubblico ministero, alla persona sottoposta alle indagini ed eventualmente alla persona offesa dal reato che abbia dichiarato di voler esserne informata.

La **lettera c)** modifica l'articolo 407 c.p.p., che dispone in ordine ai termini di durata massima delle indagini preliminari. In particolare, si interviene sulla lettera *a)* del comma 2, nell'ambito della quale sono elencate le tipologie di delitti per i quali il termine di **durata massima delle indagini preliminari** è stabilito in **2 anni**<sup>9</sup>, con l'inserimento del nuovo numero 7-*ter*), al fine di riconoscere l'estensione del termine ivi prevista anche alle indagini concernenti taluni delitti informatici<sup>10</sup>. Nello specifico i reati indicati al numero 7-*ter*) sono:

- accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.);

<sup>9</sup> Ai sensi del comma 1 del medesimo art. 407 c.p.p., la durata ordinaria delle indagini preliminari non può superare i 18 mesi per i delitti e un anno per le contravvenzioni.

<sup>10</sup> I numeri da 1 a 7-*bis*) della lettera *a)* contengono un **ampio elenco di reati gravi** (tra cui, a titolo di esempio, si citano omicidio, sequestro di persona, delitti commessi nell'ambito di associazioni di tipo mafioso, delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale, violenza sessuale di gruppo, reato di favoreggiamento dell'ingresso illegale all'interno del territorio dello Stato, nelle ipotesi aggravate, e reato di morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina). Ulteriori ipotesi di durata massima di 2 anni delle indagini preliminari sono previste nel caso di notizie di reato che rendono **particolarmente complesse le investigazioni** per la molteplicità di fatti tra loro collegati ovvero per l'elevato numero di persone sottoposte alle indagini o di persone offese (lett. *b*); di indagini che richiedono il **compimento di atti all'estero** (lett. *c*); di procedimenti in cui è indispensabile mantenere il **collegamento tra più uffici del pubblico ministero** (lett. *d*).

- detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater*);
- falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-*ter* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.);
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-*sexies* c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-*quater.1* c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.).

In relazione a tali delitti, l'estensione dei termini delle indagini preliminari opera qualora il fatto sia **commesso in danno di sistemi informatici o telematici**:

- di interesse militare;
- o relativi all'ordine pubblico, alla sicurezza pubblica, alla sanità, alla protezione civile;
- o che siano comunque di interesse pubblico.

<b>Codice di procedura penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
Art. 51 <i>(Uffici del pubblico ministero. Attribuzioni del procuratore della Repubblica distrettuale)</i>	Art. 51 <i>(idem)</i>
Commi da 1 a 3- <i>quater Omissis</i>	Commi da 1 a 3- <i>quater Omissis</i>
	<i>[Art. 12, co. 1, lett. a)]</i>
3- <i>quinqies</i> . Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414- <i>bis</i> , 600- <i>bis</i> , 600- <i>ter</i> , 600- <i>quater</i> , 600- <i>quater</i> .1, 600- <i>quinqies</i> , 609- <i>undecies</i> , 615- <i>ter</i> , 615- <i>quater</i> , <b>615-<i>quinqies</i></b> , 617- <i>bis</i> , 617- <i>ter</i> , 617- <i>quater</i> , 617- <i>quinqies</i> , 617- <i>sexies</i> , 635- <i>bis</i> , 635- <i>ter</i> , 635- <i>quater</i> , 640- <i>ter</i> e 640- <i>quinqies</i> del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.	3- <i>quinqies</i> . Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414- <i>bis</i> , 600- <i>bis</i> , 600- <i>ter</i> , 600- <i>quater</i> , 600- <i>quater</i> .1, 600- <i>quinqies</i> , 609- <i>undecies</i> , 615- <i>ter</i> , 615- <i>quater</i> , 617- <i>bis</i> , 617- <i>ter</i> , 617- <i>quater</i> , 617- <i>quinqies</i> , 617- <i>sexies</i> , 635- <i>bis</i> , 635- <i>ter</i> , 635- <i>quater</i> , <b>635-<i>quater</i>.1</b> , <b>635-<i>quinqies</i></b> , 640- <i>ter</i> e 640- <i>quinqies</i> del codice penale, <b>o per il delitto di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133</b> , le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.
Art. 406 <i>(Proroga dei termini)</i>	Art. 406 <i>(idem)</i>
Commi 1 e 2 <i>Omissis</i>	Commi 1 e 2 <i>Omissis</i>
Commi 2- <i>bis</i> e 2- <i>ter</i> <i>Abrogati</i>	Commi 2- <i>bis</i> e 2- <i>ter</i> <i>Abrogati</i>
3. La richiesta di proroga è notificata, a cura del giudice, con l'avviso della facoltà di presentare memorie entro cinque giorni dalla notificazione, alla persona sottoposta alle indagini nonché alla persona offesa dal reato che, nella notizia di reato o successivamente alla sua	<i>Identico</i>

<b>Codice di procedura penale</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
presentazione, abbia dichiarato di volere esserne informata. Il giudice provvede entro dieci giorni dalla scadenza del termine per la presentazione delle memorie.	
4. Il giudice autorizza la proroga del termine con ordinanza emessa in camera di consiglio senza intervento del pubblico ministero e dei difensori.	<i>Identico</i>
5. Qualora ritenga che allo stato degli atti non si debba concedere la proroga, il giudice, entro il termine previsto dal comma 3 secondo periodo, fissa la data dell'udienza in camera di consiglio e ne fa notificare avviso al pubblico ministero, alla persona sottoposta alle indagini nonché, nella ipotesi prevista dal comma 3, alla persona offesa dal reato. Il procedimento si svolge nelle forme previste dall'articolo 127.	<i>Identico</i>
	<i>[Art. 12, co. 1, lett. b)]</i>
5-bis. Le disposizioni dei commi 3, 4 e 5 non si applicano se si procede per taluno dei delitti indicati nell'articolo 51 comma 3-bis e nell'articolo 407, comma 2, lettera a), numeri <b>4 e 7-bis</b> . In tali casi, il giudice provvede con ordinanza entro dieci giorni dalla presentazione della richiesta, dandone comunicazione al pubblico ministero.	5-bis. Le disposizioni dei commi 3, 4 e 5 non si applicano se si procede per taluno dei delitti indicati nell'articolo 51 comma 3-bis e nell'articolo 407, comma 2, lettera a), numeri <b>4), 7-bis) e 7-ter)</b> . In tali casi, il giudice provvede con ordinanza entro dieci giorni dalla presentazione della richiesta, dandone comunicazione al pubblico ministero.
Commi da 6 a 8 <i>Omissis</i>	Commi da 6 a 8 <i>Omissis</i>
Art. 407 <i>(Termine di durata massima delle indagini preliminari)</i>	Art. 407 <i>(idem)</i>
1. Salvo quanto previsto all'articolo 393 comma 4, la durata delle indagini	<i>Identico</i>

Codice di procedura penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
preliminari non può comunque superare diciotto mesi o, se si procede per una contravvenzione, un anno.	
<p>2. La durata massima è tuttavia di due anni se le indagini preliminari riguardano:</p> <p>a) i delitti appresso indicati:</p> <p>1) delitti di cui agli articoli 285, 286, 416-<i>bis</i> e 422 del codice penale, 291-<i>ter</i>, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-<i>quater</i>, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43;</p> <p>2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale;</p> <p>3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-<i>bis</i> del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;</p> <p>4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma e 306, secondo comma, del codice penale;</p> <p>5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine</p>	

Codice di procedura penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110;	
6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni;  7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza;  7-bis) dei delitti previsto dagli articoli 600, 600-bis, primo comma, 600-ter, primo e secondo comma, 601, 602, 609-bis nelle ipotesi aggravate previste dall'articolo 609-ter, 609-quater, 609-octies del codice penale, nonché dei delitti previsti dagli articoli 12, comma 3, e 12-bis del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni;	<i>Identico</i>
	<i>[Art. 12, co. 1, lett. c)]</i>
	<b>7-ter) delitti previsti dagli articoli 615-ter, 615-quater, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 635-quater.1 e 635-quinquies del codice penale, quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o</b>



Codice di procedura penale	
Testo previgente	Modificazioni apportate dall'A.C. 1717
	<b>alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.</b>
<p>b) notizie di reato che rendono particolarmente complesse le investigazioni per la molteplicità di fatti tra loro collegati ovvero per l'elevato numero di persone sottoposte alle indagini o di persone offese;</p> <p>c) indagini che richiedono il compimento di atti all'estero;</p> <p>d) procedimenti in cui è indispensabile mantenere il collegamento tra più uffici del pubblico ministero a norma dell'articolo 371.</p>	<i>Identiche</i>
<p>3. Salvo quanto previsto dall'articolo 415-<i>bis</i>, non possono essere utilizzati gli atti di indagine compiuti dopo la scadenza del termine per la conclusione delle indagini preliminari stabilito dalla legge o prorogato dal giudice.</p>	<i>Identico</i>
<i>3-bis Abrogato</i>	

### Articolo 13

#### *(Modifiche alle norme sui collaboratori di giustizia di cui al decreto-legge n. 8 del 1991)*

L'**articolo 13** reca alcune modifiche alle disposizioni relative ai soggetti che collaborano con la giustizia, di cui al decreto-legge n. 8 del 1991, volte ad estendere il campo di applicazione della relativa disciplina agli autori dei reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

L'articolo 13 composto di un unico comma, ripartito in 3 lettere, apporta modifiche al decreto-legge n. 8 del 1991, convertito, con modificazioni, dalla legge n. 82 del 1991, recante “nuove norme in materia di sequestri di persona a scopo di estorsione e per la protezione dei testimoni di giustizia, nonché per la protezione e il trattamento sanzionatorio di coloro che collaborano con la giustizia”.

In particolare, la **lettera a)** interviene sul comma 2 dell'articolo 9 del citato decreto-legge, relativo alle condizioni di applicabilità delle **speciali misure di protezione** per i collaboratori di giustizia, prevedendo l'**estensione** dell'applicazione di tali misure anche nei confronti degli autori dei **reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.**

Nello specifico, il comma 4-*bis* dell'art. 371-*bis* c.p.p., introdotto dall'articolo 2-*bis*, comma 3, lettera *b)*, del decreto-legge n. 105 del 2023, individua i seguenti **gravi delitti informatici**, in relazione ai quali al procuratore nazionale antimafia e antiterrorismo sono riconosciute funzioni di impulso nei confronti dei procuratori distrettuali:

- 615-*ter*, terzo comma, c.p. (accesso abusivo a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità);
- 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche);

- 617-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche);
- 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche del codice penale).

Si ricorda, inoltre, che il citato decreto-legge n. 8 del 1991 prevede **speciali misure di protezione**, nonché la possibilità di adottare uno speciale programma di protezione, nei confronti di coloro che versano in grave e attuale pericolo per effetto della collaborazione o delle dichiarazioni rese nel corso di un procedimento penale per delitti commessi per finalità di terrorismo o di eversione ovvero ricompresi fra quelli di competenza della procura distrettuale di cui all'art. 51, c. 3-*bis*, c.p.p.<sup>11</sup> nonché per i delitti di violenza sessuale, pedopornografia e prostituzione minorile. Le misure possono essere estese anche ai conviventi nonché a coloro che versano in grave e attuale pericolo a causa delle relazioni intrattenute con il destinatario della protezione. La collaborazione deve avere carattere di intrinseca attendibilità, novità e completezza o deve comunque rivestire notevole importanza ai fini investigativi (art. 9).

Per l'applicazione e la definizione delle misure di protezione è istituita con decreto del Ministro dell'interno, di concerto del Ministero della giustizia, una commissione centrale presieduta da un sottosegretario di Stato e composta da un avvocato dello Stato, da due magistrati e da cinque funzionari e ufficiali con specifica esperienza (art. 10).

Il procedimento di ammissione alle misure di protezione e gli impegni che devono essere assunti dal destinatario sono disciplinati dagli artt. 11 e 12.

L'art. 13 disciplina il contenuto delle misure di protezione, ivi compreso il rilascio delle identità di copertura, mentre l'art. 13-*quater* disciplina la revoca e la modifica delle misure.

All'attuazione e alla specificazione delle modalità esecutive del programma speciale di protezione deliberato dalla commissione centrale provvede il **Servizio centrale di protezione** istituito, nell'ambito del Dipartimento della pubblica sicurezza, con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze. Il Servizio centrale di protezione è articolato, secondo quanto previsto dall'art. 14, in almeno due divisioni dotate di personale e strutture differenti e autonome, in modo da assicurare la

---

<sup>11</sup> Il comma 3-*bis* dell'art. 51 c.p.p. richiama l'associazione a delinquere finalizzata alla commissione di delitti concernenti schiavitù, tratta, traffico di organi, prostituzione minorile, pedopornografia, violenza sessuale, immigrazione clandestina, contraffazione, associazione di tipo mafioso, scambio elettorale politico-mafioso, il traffico illecito di rifiuti; il sequestro di persona a scopo di estorsione; i delitti commessi avvalendosi del vincolo associativo di tipo mafioso; i delitti commessi al fine di agevolare l'attività dell'associazione di tipo mafioso; l'associazione finalizzata al traffico di stupefacenti; l'associazione finalizzata al contrabbando di tabacchi. Il comma 3-*quater* richiama i delitti per finalità di terrorismo.

trattazione separata delle posizioni dei collaboratori di giustizia e dei testimoni di giustizia.

L'art. 15 prevede che nell'ambito dello speciale programma di protezione possa essere autorizzato, con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, il cambiamento delle generalità, garantendone la riservatezza anche in atti della pubblica amministrazione.

La **lettera b)**, invece, interviene sul comma 2 dell'articolo 11 del citato decreto-legge n. 8 del 1991, relativo alla **proposta di ammissione** alle speciali misure di protezione in favore del collaboratore di giustizia, prevedendo che anche per i reati informatici di cui al citato articolo 371-*bis*, comma 4-*bis* c.p.p., sia effettuata la comunicazione della **proposta di ammissione** alle speciali misure di protezione al procuratore nazionale antimafia e antiterrorismo.

Infine, la **lettera c)**, interviene modificando l'art. 16-*nonies* del citato decreto-legge n. 8 del 1991, in materia di disciplina speciale dei **benefici penitenziari** riservati dalla legge ai soggetti che collaborano con la giustizia, estendendo il campo di applicazione della relativa disciplina anche agli autori dei reati informatici di cui al citato articolo 371-*bis*, comma 4-*bis*, c.p.p.

In particolare, si ricorda che il citato articolo 16-*nonies* prevede che nei confronti delle persone condannate per un delitto commesso per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'articolo 51, comma 3-*bis*, del codice di procedura penale, che abbiano prestato condotte di collaborazione, il tribunale o il magistrato di sorveglianza, se ritiene che ne sussistano i presupposti, su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo, può concedere la liberazione condizionale, la concessione dei permessi premio e l'ammissione alla misura della detenzione domiciliare prevista dall'articolo 47-*ter* della legge 26 luglio 1975, n. 354.

<b>Decreto-legge 15 gennaio 1991, n. 8</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
Art. 9 <i>(Condizioni di applicabilità delle speciali misure di protezione)</i>	Art. 9 <i>(idem)</i>
1. Alle persone che tengono le condotte o che si trovano nelle condizioni previste dai commi 2 e 5 possono essere applicate, secondo le disposizioni del presente Capo, speciali misure di protezione idonee ad assicurarne l'incolumità provvedendo, ove necessario, anche alla loro assistenza.	<i>Identico</i>
	<i>[Art. 13, co. 1, lett. a)]</i>
2. Le speciali misure di protezione sono applicate quando risulta la inadeguatezza delle ordinarie misure di tutela adottabili direttamente dalle autorità di pubblica sicurezza o, se si tratta di persone detenute o internate, dal Ministero della giustizia - Dipartimento dell'amministrazione penitenziaria e risulta altresì che le persone nei cui confronti esse sono proposte versano in grave e attuale pericolo per effetto di talune delle condotte di collaborazione aventi le caratteristiche indicate nel comma 3 e tenute relativamente a delitti commessi per finalità di terrorismo o di eversione dell'ordine costituzionale ovvero ricompresi fra quelli di cui all'articolo 51, comma 3-bis, del codice di procedura penale e agli articoli 600-bis, 600-ter, 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, e 600-quinquies del codice penale.	2. Le speciali misure di protezione sono applicate quando risulta la inadeguatezza delle ordinarie misure di tutela adottabili direttamente dalle autorità di pubblica sicurezza o, se si tratta di persone detenute o internate, dal Ministero della giustizia - Dipartimento dell'amministrazione penitenziaria e risulta altresì che le persone nei cui confronti esse sono proposte versano in grave e attuale pericolo per effetto di talune delle condotte di collaborazione aventi le caratteristiche indicate nel comma 3 e tenute relativamente a delitti commessi per finalità di terrorismo o di eversione dell'ordine costituzionale ovvero ricompresi fra quelli di cui all'articolo 51, comma 3-bis, <b>o all'articolo 371-bis, comma 4-bis</b> , del codice di procedura penale e agli articoli 600-bis, 600-ter, 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, e 600-quinquies del codice penale.
Commi da 3 a 6 <i>Omissis</i>	Commi da 3 a 6 <i>Omissis</i>
Art. 11	Art. 11

<b>Decreto-legge 15 gennaio 1991, n. 8</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
<i>(Proposta di ammissione)</i>	<i>(idem)</i>
Comma 1 <i>Omissis</i>	Comma 1 <i>Omissis</i>
	<i>[Art. 13, co. 1, lett. b)]</i>
2. Quando le dichiarazioni indicate nel comma 1 attengono a procedimenti per taluno dei delitti previsti dall'articolo 51, commi 3- <i>bis</i> e 3- <i>quater</i> , del codice di procedura penale, in relazione ai quali risulta che più uffici del pubblico ministero procedono a indagini collegate a norma dell'articolo 371 dello stesso codice, la proposta è formulata da uno degli uffici procedenti d'intesa con gli altri e comunicata al procuratore nazionale antimafia e antiterrorismo; nel caso di mancata intesa il procuratore nazionale antimafia e antiterrorismo risolve il contrasto.	2. Quando le dichiarazioni indicate nel comma 1 attengono a procedimenti per taluno dei delitti previsti dall'articolo 51, commi 3- <i>bis</i> e 3- <i>quater</i> , <b>o all'articolo 371-<i>bis</i>, comma 4-<i>bis</i></b> , del codice di procedura penale, in relazione ai quali risulta che più uffici del pubblico ministero procedono a indagini collegate a norma dell'articolo 371 dello stesso codice, la proposta è formulata da uno degli uffici procedenti d'intesa con gli altri e comunicata al procuratore nazionale antimafia e antiterrorismo; nel caso di mancata intesa il procuratore nazionale antimafia e antiterrorismo risolve il contrasto.
Commi da 3 a 8 <i>Omissis</i>	Commi da 3 a 8 <i>Omissis</i>
<i>Art. 16-<i>nonies</i></i> <i>(Benefici penitenziari)</i>	<i>Art. 16-<i>nonies</i></i> <i>(idem)</i>
	<i>[Art. 13, co. 1, lett. c)]</i>
1. Nei confronti delle persone condannate per un delitto commesso per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'articolo 51, comma 3- <i>bis</i> , del codice di procedura penale, che abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione che consentono la concessione delle circostanze attenuanti previste dal codice penale o da disposizioni speciali, la liberazione condizionale, la concessione dei permessi premio e l'ammissione alla misura della	1. Nei confronti delle persone condannate per un delitto commesso per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'articolo 51, comma 3- <i>bis</i> , <b>o all'articolo 371-<i>bis</i>, comma 4-<i>bis</i></b> , del codice di procedura penale, che abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione che consentono la concessione delle circostanze attenuanti previste dal codice penale o da disposizioni speciali, la liberazione condizionale, la concessione dei permessi

<b>Decreto-legge 15 gennaio 1991, n. 8</b>	
<b>Testo previgente</b>	<b>Modificazioni apportate dall'A.C. 1717</b>
detenzione domiciliare prevista dall'articolo 47- <i>ter</i> della legge 26 luglio 1975, n. 354, e successive modificazioni, sono disposte su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo.	premio e l'ammissione alla misura della detenzione domiciliare prevista dall'articolo 47- <i>ter</i> della legge 26 luglio 1975, n. 354, e successive modificazioni, sono disposte su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo.
Commi da 2 a 8- <i>bis Omissis</i>	Commi da 2 a 8- <i>bis Omissis</i>

## Articolo 14

*(Modifiche al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203)*

**L'articolo 14** estende la disciplina delle **intercettazioni** prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo.

Più nel dettaglio **l'articolo 14** - nella prospettiva del potenziamento degli strumenti investigativi - introduce nell'articolo 13 del decreto-legge 13 maggio 1991, n. 152 (conv. legge n. 203 del 1991), il nuovo comma *3-bis*.

L'**articolo 13 del decreto-legge n. 152 del 1991** reca una **deroga alla disciplina contenuta nell'art. 267 c.p.p.**, stabilendo un allargamento delle possibilità di **ricorso alle intercettazioni** per indagini relative a **delitti di criminalità organizzata** o di **minaccia con il mezzo del telefono**. In queste ipotesi, infatti, l'autorizzazione all'intercettazione è soggetta a **limiti meno stringenti**, potendo essere concessa:

- quando sussistono **"sufficienti indizi"** di reato (anziché gravi indizi);
- quando è **"necessaria per lo svolgimento delle indagini"** (anziché assolutamente indispensabile).

Nelle stesse ipotesi le **intercettazioni ambientali** sono consentite nel domicilio o altro luogo di dimora privata anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. La relativa durata è di **40 giorni**, prorogabile per periodi successivi di 20 giorni.

Nei casi di urgenza, alla proroga provvede direttamente il pubblico ministero, con decreto che viene immediatamente comunicato al giudice per le indagini preliminari, il quale entro quarantotto ore decide sulla convalida.

È appena il caso di rammentare che la disciplina dettata dall'articolo 13, per effetto dell'articolo 1 del decreto-legge n. 105 del 2023 (conv. legge n. 137 del 2023) trova applicazione anche nei procedimenti per i delitti, consumati o tentati, di **attività organizzate per il traffico illecito di rifiuti** (art. 452-*quaterdecies* c.p.) e **sequestro di persona a scopo di estorsione** (art. 630 c.p.), ovvero commessi **con finalità di terrorismo o avvalendosi delle condizioni previste dall'articolo 416-bis c.p.** (forza di intimidazione del vincolo associativo e condizione di assoggettamento e di omertà che ne derivano) o per agevolare l'attività delle associazioni previste dallo stesso articolo (associazioni di tipo mafioso).

Ai sensi del nuovo comma *3-bis* la disciplina derogatoria in materia di intercettazioni nell'ambito di procedimenti per delitti di criminalità



organizzata (dettata dai commi 1, 2 e 3 dell'art. 13 del decreto legge n. 152) si applica anche quando si procede in relazione a uno dei gravi delitti informatici (tentati o consumati) rimessi ai sensi dell'articolo 371-*bis*, comma 4- *bis*, c.p.p. al coordinamento del procuratore nazionale antimafia e antiterrorismo

Si tratta in particolare dei seguenti delitti contenuti nel codice penale:

- 615-*ter*, terzo comma c.p. (accesso abusivo a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche);
- 617-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche);
- 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche);
- 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità);

È appena il caso di segnalare che i sopracitati articoli del codice penale sono oggetto di modifica da parte dell'art. 11 del presente disegno di legge. *Si rinvia alla relativa scheda di lettura.*

L'art. 371-*bis* c.p.p., rubricato attività di coordinamento del procuratore nazionale antimafia e antiterrorismo, delinea il quadro dei poteri e delle prerogative del procuratore medesimo. In particolare, ai sensi del comma 2, specificamente richiamato dal nuovo comma 3-*bis*, il procuratore nazionale antimafia e antiterrorismo esercita funzioni di impulso nei confronti dei procuratori distrettuali al fine di rendere effettivo il coordinamento delle attività di indagine, di garantire la funzionalità dell'impiego della polizia giudiziaria nelle sue diverse articolazioni e di assicurare la completezza e tempestività delle investigazioni.

## **Articolo 15** *(Modifiche al decreto legislativo 8 giugno 2001, n. 231)*

**L'articolo 15** interviene sul catalogo dei **reati presupposto della responsabilità amministrativa degli enti**, contemplato dall'articolo 24-*bis* del decreto legislativo n. 231 del 2001.

Più nel dettaglio **l'articolo 15** apporta una serie di modifiche all'articolo 24-*bis* del decreto legislativo n. 231 del 2001.

L'articolo 24-*bis*, introdotto nell'ordinamento dalla legge n. 48 del 2008 di ratifica della Convenzione di Budapest sulla cybercriminalità, nella sua **formulazione vigente**, prevede una serie di sanzioni per gli enti, quando i reati informatici sono commessi da una persona fisica esercitante poteri direttivi nel loro ambito.

Ai sensi del comma 1 dell'articolo 24-*bis* si applica all'ente la **sanzione pecuniaria da cento a cinquecento quote** in relazione alla commissione dei delitti di cui agli articoli 615-*ter* (Accesso abusivo ad un sistema informatico o telematico), 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), 635-*bis* (Danneggiamento di informazioni, dati e programmi informatici e telematici), 635-*ter* (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), 635-*quater* (Danneggiamento di sistemi informatici e telematici) e 635-*quinquies* (Danneggiamento di sistemi informatici e telematici di pubblica utilità) del codice penale.

In relazione alla commissione dei delitti di cui agli articoli 615-*quater* (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici) e 615-*quinquies* (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) del codice penale, si applica all'ente, invece **la sanzione pecuniaria sino a trecento quote** (comma 2).

Il disegno di legge:

- **aumenta le sanzioni** previste al comma 1 (che passano da un arco edittale compreso tra cento e cinquecento quote, ad un arco compreso tra duecento e settecento quote),

- introduce nell'articolo 24-*bis* il nuovo comma 1-*bis*, ai sensi del quale si applica all'ente la **sanzione pecuniaria da trecento a ottocento quote** in relazione alla commissione della nuova fattispecie di **estorsione informatica** di cui all'articolo 629, terzo comma, del codice penale (*si veda la lett. l) del comma 1 dell'art. 11 del presente ddl*). Nei casi di condanna è prevista anche l'applicazione **delle sanzioni interdittive** previste dall'articolo 9, comma 2 del medesimo decreto legislativo 8 giugno 2001, n. 231, per una durata non inferiore a due anni;

Le sanzioni interdittive sono: a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.

- modifica il comma 2 dell'articolo 24-*bis*, **elevando** la sanzione pecuniaria ivi prevista **sino a quattrocento quote** (attualmente è "fino a trecento quote") e sostituendo tra i reati presupposti per i quali è prevista l'applicazione all'ente della sanzione pecuniaria suddetta il riferimento all'articolo 615-*quinquies* c.p. (*abrogato dall'articolo 11, lettera c) del presente ddl*) con il richiamo al nuovo delitto di **detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'articolo 635-*quater*.1.**

## **Articolo 16** *(Modifiche alla legge 11 gennaio 2018, n. 6)*

**L'articolo 16** interviene sul procedimento di applicazione delle speciali misure di protezione per i **testimoni di giustizia** e per gli altri protetti, prevedendo che la Commissione centrale debba richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, anche nel caso dei gravi delitti informatici indicati nell'articolo 371-*bis*, comma 4- *bis*, c.p.p.

Più nel dettaglio **l'articolo 16** modifica il comma 2 dell'articolo 11 della legge 11 gennaio 2018, n. 6.

Tale articolo disciplina la **proposta di ammissione** alle speciali **misure di protezione per i testimoni di giustizia**. Attualmente la Commissione centrale è tenuta a richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, nel caso in cui la testimonianza riguardi delitti di mafia, terrorismo ed altri delitti di particolare allarme sociale (articolo 51, commi 3-*bis*, *ter* e *quater*, c.p.p.)

È appena il caso di rammentare che le speciali misure di protezione dei testimoni di giustizia si sostanziano in:

- misure di tutela (fisica);
- misure di sostegno economico;
- misure di reinserimento sociale e lavorativo.

Il disegno di legge prevede che il parere debba essere richiesto anche nel caso di delitti di cui all'articolo 371-*bis*, comma 4-*bis* c.p.p.

Si tratta in particolare dei seguenti delitti contenuti nel codice penale:

- 615-*ter*, terzo comma (accesso abusivo a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- 635-*quinquies* (danneggiamento di sistemi informatici o telematici di pubblica utilità);
- 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);
- 617-*sexies* (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche del codice penale).

È appena il caso di segnalare che i sopracitati articoli del codice penale sono oggetto di modifica da parte dell'art. 11 del presente disegno di legge. *Si rinvia alla relativa scheda di lettura.*

Occorre ricordare inoltre che l'articolo 13, comma 1, lett. c) del presente disegno di legge, estende alle persone condannate per i reati informatici attribuiti al coordinamento del procuratore nazionale antimafia e antiterrorismo, la disciplina speciale dei benefici penitenziari riservati dalla legge ai soggetti che **collaborano con la giustizia** (*Si rinvia alla relativa scheda di lettura.*)

**Articolo 17**

*(Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)*

**L'articolo 17** disciplina i rapporti tra l'Agenzia per la cybersicurezza nazionale (ACN), il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero.

Più nel dettaglio **l'articolo 17** modifica il decreto legge n. 82 del 2021 (conv. in legge n. 109 del 2021), il quale ha definito l'architettura nazionale della cybersicurezza e ha istituito l'ACN.

L'**Agenzia per la cybersicurezza nazionale** (ACN) – come anticipato- è stata istituita dal decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Tra i principali compiti dell'Agenzia c'è l'attuazione della [Strategia Nazionale di Cybersicurezza](#), adottata dal Presidente del Consiglio, che contiene gli obiettivi da perseguire entro il 2026.

L'Agenzia inoltre assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione, promuove iniziative di partenariato pubblico-privato, onde rendere effettive le capacità di prevenzione e rilevamento e risposta ad incidenti ed attacchi informatici, sostiene negli ambiti di competenza lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche, assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisca competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare.

Essa, inoltre, assume compiti in precedenza attribuiti a diversi soggetti, quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza, l'Agenzia per l'Italia digitale.

Ad esempio, all'ACN sono stati trasferiti i compiti già dell'AgID relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (art. 6, comma 1, del D.Lgs n. 259/2003, come modificato dal D.Lgs. 207/2021, di recepimento della direttiva UE 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche).

In primo luogo, il **comma 1, lett. a)** modifica il comma 4 dell'articolo 17 prevedendo che la **trasmissione** delle notifiche di incidente da parte

del personale dell’Agenzia addetto al CSIRT Italia all’organo centrale del Ministero dell’interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all’articolo 7-*bis* del decreto legge n. 144 del 2005 (conv. legge n. 155 del 2005), debba essere **immediata**. E’ confermato il riconoscimento al personale dell’Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, della qualifica di pubblico ufficiale. La trasmissione delle notifiche di incidente, che rientra tra i compiti del CSIRT, rimane inquadrata tra gli obblighi di denuncia fissati dall’articolo 331 del codice di procedura penale, concernente appunto la denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio.

L’acronimo CSIRT sta per *Computer Security Incident Response Team* (gruppo di gestione degli incidenti di sicurezza informatica). Tale soggetto originariamente istituito presso il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio è stato successivamente trasferito presso l’Agenzia. I suoi compiti sono: 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; l’intervento in caso di incidente; l’analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT (che interloquisce con l’Agenzia dell’Unione europea per la cybersicurezza).

La **lett. b)** del **comma 1** dell’articolo 17 introduce poi nell’articolo 17 del decreto-legge n. 82 del 2021, **quattro ulteriori commi** (commi da 4-*bis.1* a 4-*bis.4*). Ai sensi del nuovo comma 4-*bis.1* l’Agenzia deve procedere alle attività di cui all’articolo 7, comma 1, lett. n) e n-*bis*) e informare senza ritardo il procuratore nazionale antimafia e antiterrorismo nei casi in cui ha notizia di un attacco ai sistemi informatici o telematici di cui all’articolo 371-*bis*, comma 4-*bis* c.p.p., e, in ogni caso quando risulti interessato taluno dei soggetti di cui:

- all’articolo 1, comma 2-*bis* del decreto-legge n. 105 del 2019 ovvero i soggetti rientranti nel Perimetro di sicurezza nazionale;
- all’articolo 3, comma 1, lett. g) e i) del decreto legislativo n. 65 del 2018. Si tratta in particolare degli operatori di servizi essenziali e dei fornitori di servizio digitale.
- all’articolo 40, comma 3 del decreto legislativo n. 259 del 2003, ovvero le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

L’articolo 7 del decreto-legge n. 82 elenca le funzioni attribuite all’Agenzia. Ai sensi della lett. n) l’Agenzia “sviluppa capacità nazionali di prevenzione,

monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia promuovendo anche iniziative di partenariato pubblico-privato per rendere effettive tali capacità. Come precisa la lett. n-*bis*), nell'ambito della funzione di sviluppo della capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli **incidenti di sicurezza informatica** e gli **attacchi informatici** l'Agenzia svolge anche ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici.

L'art. 371-*bis* c.p.p., rubricato attività di coordinamento del procuratore nazionale antimafia e antiterrorismo, delinea il quadro dei poteri e delle prerogative del procuratore medesimo. In particolare, ai sensi del comma 2, specificamente richiamato dal comma 4-*bis*, il procuratore nazionale antimafia e antiterrorismo esercita **funzioni di impulso** nei confronti dei procuratori distrettuali al fine di rendere effettivo il **coordinamento** delle attività di indagine, di garantire la **funzionalità** dell'impiego della polizia giudiziaria nelle sue diverse articolazioni e di assicurare la **completezza e tempestività delle investigazioni**.

Il **comma 4-*bis*** riconosce le predette funzioni di impulso al procuratore nazionale antimafia e antiterrorismo nei procedimenti relativi ad alcuni **gravi delitti informatici**. Si tratta dei seguenti delitti:

- 615-*ter*, terzo comma c.p. (accesso abusivo a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità);
- 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche);
- 617-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche);
- 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche).

È appena il caso di segnalare che i sopracitati articoli del codice penale sono oggetto di modifica da parte dell'art. 11 del presente disegno di legge. *Si rinvia alla relativa scheda di lettura.*



Corrispondentemente il PM – quando acquisisce la notizia dei gravi delitti informatici indicati nell'articolo 371-bis, comma 4-*bis* c.p.p.– deve darne **tempestiva informazione** all'ACN assicurando anche il **raccordo informativo con l'organo del Ministero dell'interno** per la sicurezza e la regolarità dei servizi di telecomunicazione. (comma 4-*bis*.2 dell'articolo 17).

Il PM, in ogni caso, ricevuta la notizia di reato e, assunta la direzione delle indagini, è chiamato ad impartire le disposizioni necessarie ad assicurare che gli **accertamenti urgenti** si svolgano tenendo conto delle attività di ripristino svolte dall'Agenzia e può eventualmente disporre il differimento di una o più delle attività, con motivato provvedimento adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini (comma 4-*bis*.3 dell'articolo 17):

Viene, infine, introdotta la facoltà per l'ACN, in caso di **accertamenti tecnici irripetibili** per i delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'**incidente probatorio** (comma 4-*bis*.4).

È appena il caso di rammentare che nell'ambito del diritto processuale penale gli accertamenti tecnici non ripetibili, disciplinati principalmente dall'art 360 c.p.p. e dall'art. 391-*decies* c.p.p., sono gli accertamenti che hanno ad oggetto persone, cose o luoghi il cui stato è soggetto a modificazione per cause naturali o a causa della stessa attività accertativa e che, data la loro irripetibilità, sono destinati ad acquisire a tutti gli effetti valore di prova.

## **Articolo 18** *(Disposizioni finanziarie)*

**L'articolo 18, comma 1, reca la clausola di invarianza finanziaria.**

**Il comma 2 dispone che i proventi delle sanzioni** previste nei casi di reiterata inosservanza dell'obbligo di notifica degli incidenti di sicurezza informatica e degli attacchi informatici, siano destinati alle **entrate dell'Agenzia per la cybersicurezza nazionale.**

Il **comma 1** dell'articolo 18 reca la **clausola di invarianza finanziaria**, secondo cui dall'attuazione della legge non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni competenti provvedono agli adempimenti previsti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Il **comma 2** precisa che i proventi delle **sanzioni amministrative pecuniarie** (articolo 1, comma 5) comminate a seguito di violazioni conseguenti alla reiterata inosservanza degli obblighi di notifica degli incidenti indicati nella tassonomia della normativa in materia di Perimetro di sicurezza nazionale cibernetica, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale.

## La governance della sicurezza cibernetica

La materia della sicurezza cibernetica è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. **direttiva NIS - Network and Information Security**) che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea. La direttiva è stata recepita nell'ordinamento interno con il **decreto legislativo n. 65 del 18 maggio 2018**, che costituisce la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

La normativa europea è stata aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. **direttiva NIS 2**) che ha sostituito il quadro di riferimento in materia, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cibersicurezza. L'aggiornamento della direttiva mira inoltre ad eliminare le ampie divergenze tra gli Stati membri che hanno attuato gli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione, stabiliti dalla direttiva NIS in modi significativamente diversi a livello nazionale, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno. La delega per la trasposizione della direttiva nel diritto interno è contenuta nella **di legge di delegazione europea 2022-2023** (L. 15/2024).

Successivamente alla attuazione della NIS 1, il **decreto-legge n. 105 del 2019** è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle **amministrazioni pubbliche**, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un **perimetro di sicurezza nazionale cibernetica (PNSC)** e la previsione di misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019.

Con il **decreto-legge n. 82 del 2021**, si è proceduto alla definizione dell'**architettura nazionale di cibersicurezza** e all'istituzione dell'**Agenzia per la cibersicurezza nazionale**, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (**PNRR**): la sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal

PNRR nell'ambito della trasformazione digitale della p.a. e della digitalizzazione del Paese (vedi oltre).

La *governance* del sistema di sicurezza cibernetica ha al suo vertice il **Presidente del Consiglio dei ministri**, al quale è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza nonché l'adozione della relativa strategia nazionale e - previa deliberazione del Consiglio dei ministri - la nomina e la revoca dei vertici dell'Agenzia per la cybersicurezza nazionale; i tali nomine sono preventivamente informati il COPASIR e le competenti Commissioni parlamentari. Il Presidente del Consiglio dei ministri può delegare all'**Autorità delegata per il sistema di informazione per la sicurezza della Repubblica**, ove istituita, le funzioni in materia di sicurezza cibernetica che non sono a lui attribuite in via esclusiva.

Presso la Presidenza del Consiglio dei ministri è istituito il **Comitato interministeriale per la cybersicurezza (CIC)**, organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

L'**Agenzia per la cybersicurezza nazionale (ACN)** è istituita a tutela degli interessi nazionali nel campo della cybersicurezza. L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale ha il coordinamento tra i soggetti pubblici coinvolti nella cybersicurezza a livello nazionale; promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore. Essa predispose la **strategia nazionale di cybersicurezza**. Ai sensi del nuovo Codice europeo delle comunicazioni elettroniche, svolge anche i compiti relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (D.Lgs. 8 novembre 2021, n. 207, art. 6, comma 3 e artt. 40 e 41). Presso l'Agenzia per la cybersicurezza nazionale è prevista la costituzione di un **Nucleo per la cybersicurezza**, per profili attinenti a eventuali situazioni di crisi.

Il Presidente del Consiglio dei ministri trasmette al Parlamento (entro il 30 aprile di ogni anno) una **relazione** sull'attività svolta dall'Agenzia nell'anno precedente. Così come trasmette al COPASIR (entro il 30 giugno di ogni anno) una relazione sulle attività svolte nell'anno

precedente dall'Agenzia concernenti la tutela della sicurezza nazionale nello spazio cibernetico per i profili di competenza del Comitato.

Nell'ambito del **PNRR** la Cybersecurity è uno dei 7 investimenti afferenti alla Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo".

L'investimento (**investimento 1.5**) è volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica; ad esso sono destinati 622 milioni di euro di cui:

- 241 per la creazione di una infrastruttura per la cybersicurezza (attuata con la creazione della ACN);
- 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC;
- 150 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, ministero della Difesa, Guardia di Finanza, ministero della Giustizia e Consiglio di Stato.

L'intervento si articola in 4 aree principali:

- rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio verso la PA e le imprese di interesse nazionale;
- consolidamento delle capacità tecniche di valutazione e *audit* della sicurezza dell'*hardware* e del *software*;
- potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del crimine informatico;
- implementazione degli *asset* e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

L'investimento è finalizzato a garantire il funzionamento dell'intero sistema di digitalizzazione della p.a. che prevede in primo luogo la creazione di infrastrutture digitali per la p.a. anche attraverso la realizzazione del Polo strategico nazionale (investimento 1.1). Si tratta di un ambiente *cloud* destinato ad ospitare la Piattaforma digitale nazionale dati ove confluiranno le informazioni provenienti da tutte le amministrazioni, consentendo l'interoperabilità dei dati (investimento 1.3). L'obiettivo finale è di sviluppare, attraverso la piattaforma, un'offerta integrata e armonizzata di servizi digitali per i cittadini (investimento 1.4). In tutte queste fasi è necessario garantire la sicurezza cibernetica delle infrastrutture e dei dati.

Il traguardo intermedio previsto dal PNRR, del dicembre 2022, è stato raggiunto con la istituzione dell’Agenzia per la cibersecurity nazionale – ACN e con il dispiego iniziale dei servizi nazionali di cibersecurity.

L’obiettivo finale è previsto nel dicembre 2024 con il dispiego integrale dei servizi nazionali di cibersecurity, l’attivazione delle squadre di pronto intervento informatico (CERT); la piena operatività dei servizi di gestione dei rischi di cibersecurity, compresi quelli per l’analisi della catena di approvvigionamento e i servizi di assicurazione contro i rischi informatici; il completamento della rete di laboratori e dei centri per la valutazione e certificazione della cibersecurity; la piena operatività dell’unità centrale di audit.

