dossier

XIX Legislatura

22 maggio 2024

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

A.S. n. 1143

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO STUDI
TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier n. 257/2

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-9475 - ✉ st_istituzioni@camera.it - @CD_istituzioni

Dipartimento Giustizia
Tel. 06 6760-9148 - ✉ st_giustizia@camera.it - @CD_giustizia

Progetti di legge n. 266/2

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.

I N D I C E

SCHEDE DI LETTURA

- Articolo 1 *(Obblighi di notifica di incidenti)* 3
- Articolo 2 *(Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale)*.....8
- Articolo 3 *(Norme di raccordo con le disposizioni del decreto-legge 21 settembre 2019, n. 105)* 10
- Articolo 4 *(Disposizioni in materia dati relativi a incidenti informatici)* 13
- Articolo 5 *(Disposizioni in materia di Nucleo per la cybersicurezza)*.....14
- Articolo 6 *(Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale)* 17
- Articolo 7 *(Composizione del Comitato interministeriale per la sicurezza della Repubblica)* 20
- Articolo 8 *(Rafforzamento della resilienza delle pubbliche amministrazioni, referente per la cybersicurezza)*.....22
- Articolo 9 *(Rafforzamento delle misure di sicurezza dei dati attraverso la crittografia)*.....26
- Articolo 10 *(Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di crittografia)*.....28
- Articolo 11 *(Procedimento sanzionatorio per le violazioni in materia di cybersicurezza di competenza dell'Agenzia)* 31
- Articolo 12 *(Disposizioni in materia di personale dell'Agenzia per la cybersicurezza nazionale)*.....34
- Articolo 13 *(Disposizioni relative al personale cessato degli organismi di informazione per la sicurezza)*.....36
- Articolo 14 *(Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici)* 38
- Articolo 15 *(Resilienza operativa digitale per il settore finanziario)* 44
- Articolo 16 *(Modifiche al codice penale)*.....49
- Articolo 17 *(Modifiche al codice di procedura penale)*.....81

- Articolo 18 *(Modifiche alle norme sui collaboratori di giustizia di cui al decreto-legge n. 8 del 1991)* 89
- Articolo 19 (*Modifica al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203*).....95
- Articolo 20 (*Modifiche al decreto legislativo 8 giugno 2001, n. 231*).....97
- Articolo 21 (*Modifica alla legge 11 gennaio 2018, n. 6*).....99
- Articolo 22 (*Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109*).....101
- Articolo 23 *(Verifica della sicurezza negli accessi alle banche dati presso gli uffici giudiziari)* 105
- Articolo 24 *(Disposizioni finanziarie)*.....109

Articolo 1
(Obblighi di notifica di incidenti)

L'**articolo 1, modificato dalla Camera dei deputati**, 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; alle città metropolitane; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti; alle società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; alle aziende sanitarie locali; alle società *in house* degli enti fin qui richiamati, attive in alcuni specifici settori.

L'articolo 1, al **comma 1**, così come modificato **dalla Camera dei deputati**, 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;
- città metropolitane (soggetti aggiunti nel corso dell'esame presso la **Camera**);

  Si ricorda che l'articolo 1, comma 5, della legge n. 56 del 2014 ("Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni") individua dieci città metropolitane: Torino, Milano, Venezia, Genova, Bologna, Firenze, Bari, Napoli, Reggio Calabria, a cui si aggiunge la città metropolitana di Roma capitale (art. 1, comma 5, L. n. 56/2014). Le finalità istituzionali generali delle città metropolitane, definite come enti territoriali di area vasta, sono: cura dello sviluppo strategico del territorio metropolitano; promozione e gestione integrata dei servizi, delle infrastrutture e delle reti di comunicazione della città metropolitana; cura delle relazioni istituzionali afferenti al proprio livello, comprese quelle con le città e le aree metropolitane europee. La legge n. 56 del 2014 dispone l'istituzione delle città metropolitane esclusivamente nelle regioni a statuto ordinario. Per quanto riguarda le regioni a statuto speciale, i princìpi della legge valgono come princìpi di grande riforma economica e sociale per la disciplina di città e aree metropolitane, in conformità ai rispettivi statuti,

nelle regioni Sardegna, Sicilia e Friuli-Venezia Giulia (art. 1, comma 5, della L. n. 56/2014). Tali regioni sono tenute ad adeguare i propri ordinamenti interni ai principi della legge n. 56/2014 (art. 1, comma 145 della medesima legge). Finora le città metropolitane istituite dalle regioni a statuto speciale sono: Cagliari, Sassari Catania, Messina e Palermo. In Friuli-Venezia Giulia una modifica dello statuto ha introdotto il nuovo ente della città metropolitana, equiparata al livello di governo comunale (legge costituzionale n. 1 del 2016).

- comuni con popolazione superiore a 100.000 abitanti e comunque i comuni capoluoghi di regione;
- società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane (soggetti aggiunti nel corso dell'esame presso la **Camera**);
- aziende sanitarie locali;
- società *in house* degli enti fin qui richiamati che, come specificato nel corso dell'esame presso la **Camera dei deputati**, siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali ovvero servizi di gestione dei rifiuti.

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.

Con riferimento alle società *in house* che si occupano della raccolta, dello smaltimento o del trattamento delle acque reflue, la disposizione, al fine di definire le "acque reflue", rinvia all'articolo 2, punti 1), 2) e 3) della direttiva 91/271/CEE. Ai sensi di tali disposizioni per "acque reflue urbane" si intendono acque reflue domestiche, acque reflue industriali e/o acque meteoriche di dilavamento; per "acque reflue domestiche" si intendono acque reflue provenienti da insediamenti di tipo residenziale e da servizi, derivanti prevalentemente dal metabolismo umano e da attività domestiche; per "acque reflue industriali" si intendono tutte le tipologie di acque reflue scaricate da edifici in cui si svolgono attività commerciali o industriali, diverse dalle acque reflue domestiche e dalle acque meteoriche di dilavamento.

Relativamente alle società *in house* che si occupano della gestione dei rifiuti, la disposizione, al fine di definire la "gestione dei rifiuti" rinvia all'articolo 3, punto 9), della direttiva 2008/98/CE. In particolare, per "gestione dei rifiuti" si intende la raccolta, il trasporto, il recupero (inclusa la cernita) e lo smaltimento dei rifiuti, compresi la supervisione di tali operazioni effettuate in qualità di commercianti o intermediari.

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.

Il **comma 3**, inserito dalla **Camera dei deputati**, dispone che gli obblighi di notifica indicati ai precedenti commi (segnalazione degli incidenti e modalità per l'effettuazione della notifica) si applichino per alcuni soggetti a decorrere dal centottantesimo giorno dalla data di entrata in vigore del presente provvedimento. Si tratta di:

- i comuni con popolazione superiore a 100.000 abitanti;
- i comuni capoluoghi di regione;
- le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- le aziende sanitarie locali;
- le società *in house* che forniscono servizi informatici, servizi di trasporto descritti come sopra, nonché quelle che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali, ovvero che si occupano della gestione dei rifiuti.

Al riguardo, si segnala che mentre il comma 1 specifica che le società in house *destinatarie degli obblighi di notifica sono quelle che fanno capo agli altri soggetti indicati al comma 1 (attraverso l'utilizzo dell'espressione le "rispettive società* in house"*) tale specificazione non è presente nel comma 3*.

Conseguentemente, gli obblighi di notifica si applicheranno invece a decorrere dalla data di entrata in vigore della presente legge per:

- le pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge n. 196 del 2009;
- le regioni e province autonome di Trento e di Bolzano;
- le città metropolitane.

I **commi 5 e 6** indicano le sanzioni per la violazione dell'obbligo di notifica.

In particolare, il **comma 5**, modificato dalla **Camera dei deputati**, prevede, in caso di inosservanza, la comunicazione da parte dell'Agenzia per la cybersicurezza nazionale all'interessato che la reiterazione dell'inosservanza nell'arco di cinque anni (termine aggiunto presso la **Camera dei deputati**) comporterà l'applicazione delle sanzioni previste dal comma 6. 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 6**, modificato dalla **Camera dei deputati**, individua la sanzione amministrativa pecuniaria per la reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica da un minimo di 25.000 a un massimo di 125.000 euro a carico dei soggetti indicati al comma 1 (già elencati nel relativo commento). 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 11 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 nei confronti, come specificato dalla **Camera dei deputati**, dei funzionari e dei dirigenti responsabili.

In base al **comma 4**, 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 7** 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 5).

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 provincie 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, nell'arco di cinque anni, dell'obbligo di notifica all'ACN degli incidenti cibernetici indicata all'articolo 1, comma 6, 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)[1].

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**.

Con la seconda modifica, di cui alla **lettera *b)*** del comma unico dell'articolo in commento, si prevede, aggiungendo un ultimo periodo al

[1] 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).

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 dati relativi a incidenti informatici)

L'**articolo 4**, introdotto **dalla Camera dei deputati**, prevede che i dati relativi a incidenti informatici sono raccolti, sulla base degli adempimenti di notifica previsti a legislazione vigente, dall'Agenzia per la Cybersicurezza nazionale, che ne cura la pubblicità come dati ufficiali di riferimento degli attacchi informatici.

A tal fine, l'articolo integra, con una nuova lettera m-*ter*), i compiti dell'Agenzia per la Cybersicurezza nazionale descritti dall'articolo 7, comma 1, del decreto-legge n. 82 del 2021.

In particolare, in base all'articolo in commento, spetta all'Agenzia provvedere non solo alla **raccolta**, ma anche alla **elaborazione e classificazione** dei dati relativi alle **notifiche di incidenti informatici**, ricevute dai soggetti a ciò tenuti dalle norme vigenti.

Sono tenuti all'**obbligo di notifica** degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici i soggetti pubblici e privati che abbiano ricevuto la comunicazione di inclusione all'interno del perimetro di sicurezza nazionale cibernetica (art. 1, comma 3-bis, del decreto-legge n. 105 del 2019). Ulteriori obblighi di notifica sono introdotti dall'articolo 1 del disegno di legge in commento (alla cui scheda di lettura, *supra*, si rinvia).

La **pubblicità** dei dati sugli incidenti informatici deve essere assicurata **nell'ambito della relazione** che il Presidente del Consiglio trasmette entro il 30 aprile di ogni anno al Parlamento **sull'attività svolta dall'Agenzia** nell'anno precedente, in materia di cybersicurezza nazionale (art. 14, co. 1, D.L. n. 82/2021).

La disposizione specifica che tali dati rappresentano i **dati ufficiali** di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza.

Da ultimo, si prevede che all'attuazione della disposizione si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Articolo 5
(Disposizioni in materia di Nucleo per la cybersicurezza)

L'**articolo 5** 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[2], 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,

[2] di cui all'articolo 9, comma 1, lettera a), del decreto-legge n. 82 del 2021

comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. 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**[3], 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.

[3] Decreto-legge n.115 del 2022, art. 37-quater, comma 1.

Articolo 6
(Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale)

L'**articolo 6** 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 coma 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 7
(Composizione del Comitato interministeriale per la sicurezza della Repubblica)

L'**articolo 7,** introdotto nel corso dell'esame presso la **Camera dei deputati**, modifica la composizione del Comitato interministeriale per la sicurezza della Repubblica (CISR), disponendo che del Comitato facciano parte anche il Ministro dell'agricoltura, il Ministro delle infrastrutture e dei trasporti e il Ministro dell'università e della ricerca.

Oltre a questo, l'articolo provvede all'aggiornamento delle denominazioni di alcuni ministri già componenti del CISR.

La disposizione modifica l'articolo 5, comma 3, della legge n. 124 del 2007, in materia di sistema di informazione per la sicurezza della Repubblica.

Il richiamato comma 3 prevede che il Comitato sia presieduto dal Presidente del Consiglio. Gli altri componenti sono l'Autorità delegata in materia di sicurezza della Repubblica, ove istituita (attualmente un Sottosegretario alla Presidenza del Consiglio), il Ministro degli esteri, il Ministro dell'interno, il Ministro della difesa, il Ministro della giustizia, il Ministro dell'economia, il Ministro dello sviluppo economico (ora delle imprese del Made in Italy) e il Ministro della transizione ecologica (ora Ministro dell'ambiente e della sicurezza energetica).

L'inserimento del Ministro dello sviluppo economico (ora delle imprese del Made in Italy) tra i componenti del CISR è stato previsto dall'articolo 1, comma 21, del decreto-legge n. 85 del 2008, quello del Ministro della transizione ecologica (ora Ministro dell'ambiente e della sicurezza energetica) dall'articolo 2, comma 8-bis, del decreto-legge n. 22 del 2021.

Il successivo comma 4 del citato articolo 5 prevede che il direttore generale del DIS (Dipartimento per le informazioni e la sicurezza) svolga le funzioni di segretario del Comitato; il comma 5 dispone che il Presidente del Consiglio possa chiamare a partecipare alle sedute del Comitato senza diritto di voto, anche a seguito di loro richiesta, altri componenti del Consiglio dei ministri, i direttori dell'AISE (Agenzia informazioni per la sicurezza esterna) e dell'AISI (Agenzia informazioni per la sicurezza interna), nonché altre autorità civili e militari di cui di

volta in volta sia ritenuta necessaria la presenza in relazione alle questioni da trattare.

Il comma 1 del citato articolo 5 attribuisce al CISR funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Il successivo comma 2 attribuisce poi al Comitato questi compiti specifici:

- Elaborazione degli indirizzi generali e degli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza;
- Deliberazione sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza (cioè l'AISE e l'AISI)[4] e i relativi bilanci preventivi e consuntivi.

L'articolo 2, comma 1, della legge n. 124 del 2007 individua nel CISR uno dei componenti del Sistema di informazione per la sicurezza della Repubblica, insieme al Presidente del Consiglio, all'Autorità delegata, se istituita, al DIS, all'AISE e all'AISI.

Tra le altre funzioni del CISR indicate nella legge merita segnalare:

- il parere sulle disposizioni necessarie per l'organizzazione e il funzionamento del Sistema di informazioni per la sicurezza della Repubblica emanate dal Presidente del Consiglio (articolo 1, comma 3);
- il parere sulle direttive del Presidente del Consiglio per rafforzare per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla **protezione cibernetica e alla sicurezza informatica** nazionali (articolo 1, comma 3-*bis*, introdotto nella legge n. 124 della legge n. 133 del 2012);
- il parere sulla nomina del direttore generale del DIS (articolo 4, comma 5);
- il parere sulla nomina del direttore dell'AISE (articolo 6, comma 7) e dell'AISI (articolo 7, comma 7);
- il parere sulle disposizioni regolamentari di attuazione della legge n. 124 (articolo 43, comma 1).

[4] L'articolo 2, comma 2, della legge n. 124 del 2007 precisa che ai fini della legge per "servizi di informazione per la sicurezza" si intendono appunto l'AISE e l'AISI.

Articolo 8
(Rafforzamento della resilienza delle pubbliche amministrazioni, referente per la cybersicurezza)

L'**articolo 8, modificato dalla Camera,** istituisce, per le pubbliche amministrazioni indicate nell'**articolo 1, comma 1**, dove non sia già presente, la **struttura preposta alle attività di cybersicurezza**, anche all'interno di quelle già presenti a legislazione vigente; al contempo, predispone l'istituzione del **referente per la cybersicurezza**, unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale. Precisa, in tal senso, 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;
- le città metropolitane;
- 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 società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- le aziende sanitarie locali;
- le società *in house* di cui al comma 1 dell'articolo 1, che forniscono servizi informatici, quelle che forniscono servizi di trasporto di cui al primo periodo, nonché quelle che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche e industriali.

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 individuano 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 nonché, a seguito di un'integrazione apportata presso la **Camera dei deputati**, di sistemi di analisi preventiva di rilevamento del 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, nel testo risultante dalle modifiche apportate in sede referente, in ragione di **specifiche professionalità e competenze possedute in materia,** nel caso in cui all'interno dei soggetti di cui all'articolo 1, comma 1 non vi siano dipendenti con tali requisiti potrà essere incaricato il **dipendente di un'altra pubblica amministrazione** previa autorizzazione da parte dell'amministrazione di appartenenza ai sensi dell'art. 53 del decreto legislativo n. 165 del 2001 (norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e nell'ambito delle risorse disponibili a legislazione vigente senza determinare nuovi o maggiori oneri per la finanza pubblica;

  Il richiamato articolo 53 disciplina, tra le altre cose, l'autorizzazione, da parte dell'amministrazione di appartenenza, allo svolgimento da parte dei dipendenti di incarichi retribuiti da parte di altre amministrazioni. Ai sensi del comma 10 l'autorizzazione deve essere richiesta all'amministrazione di appartenenza dallo stesso dipendente o dai soggetti che intendono conferire l'incarico. L'amministrazione di appartenenza deve pronunciarsi sulla

richiesta di autorizzazione entro trenta giorni dalla ricezione della stessa. Per il personale che presta servizio presso amministrazioni pubbliche diverse da quelle di appartenenza, l'autorizzazione è subordinata all'intesa tra le due amministrazioni. In tal caso il termine per provvedere è per l'amministrazione di appartenenza di 45 giorni e si prescinde dall'intesa se l'amministrazione presso la quale il dipendente presta servizio non si pronunzia entro 10 giorni dalla ricezione della richiesta di intesa. Decorsi tali termini, l'autorizzazione, se richiesta per incarichi da conferirsi da amministrazioni pubbliche, si intende accordata; in ogni altro caso, si intende definitivamente negata.

- 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**, introdotto dalla **Camera dei deputati**, prevede che la struttura per la cybersicurezza e il referente per la cybersicurezza istituiti dai commi 1 e 2 possano essere individuati nell'ufficio e nel responsabile per la transizione al digitale previsti dall'art. 17 del decreto legislativo n. 82 del 2005 (codice dell'amministrazione digitale).

L'art. 17 del decreto legislativo n. 82 del 2005 prevede al comma 1 che ciascuna pubblica amministrazione affidi a un unico ufficio dirigenziale generale la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione. Il comma 1-*ter* stabilisce che il responsabile dell'ufficio di cui al comma 1 sia individuato in ragione di adeguate competenze tecnologiche, di informatica giuridica e manageriali e che risponda direttamente all'organo di vertice politico.

Il **comma 4**, introdotto dalla **Camera dei deputati**, prevede che i compiti di cui ai commi 1 e 2 possono essere esercitati in **forma associata**, come previsto dall'articolo 17, commi 1-*sexies* e 1-*septies*, del decreto legislativo n. 82 del 2005.

Si tratta della facoltà prevista per le amministrazioni diverse da quelle dello Stato caratterizzate dalla possibilità, nell'ambito della propria autonomia organizzativa, di individuare un responsabile per il digitale tra le proprie posizioni apicali qualora siano prive di un ufficio di livello dirigenziale.

Il **comma 5,** introdotto dalla **Camera dei deputati**, attribuisce all'Agenzia per la cybersicurezza nazionale la possibilità di individuare le modalità e i processi di coordinamento e mutua **collaborazione**, anche di livello regionale, tra le amministrazioni di cui all'articolo 1 comma 1 e tra i referenti per la cybersicurezza al fine di facilitare la resilienza delle amministrazioni pubbliche.

Il **comma 6** individua i soggetti e gli organi dello Stato a cui non si applicano le disposizioni del presente articolo.

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, comma 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).

Si ricorda che in **sede referente** alla Camera erano stati aggiunti i commi da 7 a 11, poi soppressi a seguito dell'approvazione di una proposta emendamenti dall'Assemblea, volti ad introdurre una disciplina per regolare l'accesso alle banche dati delle pubbliche amministrazioni da parte degli addetti tecnici attraverso specifici sistemi di autenticazione.

Articolo 9
(Rafforzamento delle misure di sicurezza dei dati attraverso la crittografia)

L'**articolo 9, introdotto dalla Camera dei deputati,** attribuisce alle strutture preposte alle attività di cybersicurezza nelle pubbliche amministrazioni la funzione di **verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica rispettino le linee guida sulla crittografia** adottate dall'Agenzia per la Cybersicurezza Nazionale e dall'Autorità Garante per la Protezione dei Dati Personali e non contengano vulnerabilità note.

L'articolo 9 prevede che le strutture di cui all'**articolo 8,** preposte alle attività di cybersicurezza, verifichino che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso nelle pubbliche amministrazioni indicate nell'**articolo 1 comma 1**, che impiegano soluzioni crittografiche, rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle *password* adottate dall'Agenzia per la Cybersicurezza Nazionale e dall'Autorità Garante per la Protezione dei Dati Personali.

Le "Linee Guida Funzioni Crittografiche" sono una serie di documenti elaborati dall'Agenzia per la Cybersicurezza Nazionale coerentemente con gli obiettivi della Strategia Nazionale di Cybersicurezza. Si tratta di una serie di documenti che approfondiscono differenti tematiche e ambiti di applicazione relativi all'impiego di crittografia. I primi tre, pubblicati nel dicembre 2023, recano indicazioni rispettivamente riguardo a "Funzioni di Hash", "Codici di autenticazione di messaggi (MAC)" e "Conservazione delle password".

Al fine di non rendere accessibili a terzi i dati cifrati, le strutture preposte verificano che le applicazioni e i programmi interessati dalla norma non contengano vulnerabilità note.

La medesima attività di verifica è attribuita alle strutture che svolgono analoghe funzioni per i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019 n. 105. Si tratta dei soggetti rientranti nel perimetro di sicurezza cibernetica nazionale (sul punto si rinvia al box presente nella scheda relativa all'articolo 5). Tali soggetti sono individuati ai sensi del comma 2, lettera a) del medesimo articolo tra le amministrazioni pubbliche, enti e operatori pubblici e privati con sede nel territorio nazionale e inclusi nel perimetro di sicurezza nazionale

cibernetica e da cui dipende l'esercizio di funzioni o servizi essenziali per il mantenimento di attività fondamentali per gli interessi dello Stato e che dipendono da reti, sistemi informativi e servizi informatici dal cui malfunzionamento potrebbe derivare un pregiudizio per la sicurezza nazionale. L'individuazione avviene seguendo il criterio di gradualità basato sulla gravità del danno che deriverebbe dal malfunzionamento o dall'interruzione dell'attività.

L'articolo incarica, infine, del medesimo compito le analoghe strutture previste per i soggetti individuati dal decreto legislativo n. 65 del 2018. Si tratta degli operatori di servizi essenziali con sede nel territorio nazionale identificati per ciascun settore e sotto settore indicati nell'allegato II dello stesso decreto legislativo dalle autorità competenti NIS con propri provvedimenti. Il decreto legislativo fornisce i criteri per l'identificazione degli operatori di servizi essenziali che vengono individuati tra i soggetti il cui servizio è essenziale per il mantenimento di attività sociali e/o economiche fondamentali la cui fornitura dipende dalla rete e dai sistemi informativi che qualora subissero un danno avrebbero effetti negativi rilevanti sulla fornitura del servizio stesso.

In particolare, a norma del decreto legislativo n. 65 del 2018, gli operatori che prestano attività sanitaria sono individuati con decreto del Ministero della salute di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano mentre coloro che si occupano di fornire e distribuire acque destinate al consumo umano sono individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Inoltre, un elenco nazionale di tutti gli operatori di servizi essenziali è istituito presso il Ministero dello sviluppo economico che lo inoltra al punto di contatto unico e all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. Tale elenco è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni a partire dal 18 maggio 2018.

Articolo 10
(Funzioni dell'Agenzia per la cybersicurezza nazionale in materia di crittografia)

L'**articolo 10, interamente sostituito nel corso dell'esame alla Camera,** valorizza l'utilizzo della **crittografia** quale strumento di difesa cibernetica e istituisce il **Centro nazionale di crittografia** presso l'Agenzia per la cybersicurezza nazionale – ACN.

Nel testo originario, l'articolo inseriva tra le funzioni dell'Agenzia per la cybersicurezza nazionale – ACN la valorizzazione dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale.

L'articolo in esame modifica il D.L. 82/2021, che ha definito l'architettura della cybersicurezza nazionale e ha istituito e disciplinato l'ACN. In particolare, si incide sul comma 1 dell'articolo 7 che individua puntualmente le funzioni dell'agenzia. Attraverso la sostituzione della lettera *m-bis)* del comma 1, viene potenziato e dettagliato quanto tale lettera già prevede in ordine allo sviluppo della crittografia come strumento di cybersicurezza.

Infatti, nel testo attuale, la lettera m-*bis*) prevede che l'ACN assuma le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera *b)*. Il testo vigente prevede anche che l'Agenzia attivi ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.

La disposizione in commento prevede invece, più dettagliatamente, che l'ACN, anche attraverso una apposita sezione della **strategia nazionale di cybersicurezza** – il documento programmatico predisposto dall'Agenzia – debba provvedere a:

- promuovere l'utilizzo della crittografia anche a vantaggio della tecnologia *blockchain*;

La *blockchain* è una tecnologia che consente di creare un archivio elettronico condiviso e accessibile via internet, in cui sono memorizzate in modo sicuro e irreversibile le informazioni inserite liberamente dai partecipanti al network. L'aggiornamento del registro – con riguardo, ad esempio, alle

informazioni relative a transazioni economiche – avviene in modo decentrato, senza ricorrere a un ente terzo fiduciario, come nei sistemi tradizionali (Banca d'Italia, La governance delle *blockchain* e dei sistemi basati sulla tecnologia dei registri distribuiti, in Questioni di economia e finanza, n. 773/2023).

- sviluppare e diffondere ***standard*, linee guida e raccomandazioni** al fine di rafforzare la cybersicurezza dei sistemi informatici;
- valutare la **sicurezza dei sistemi crittografici**;
- organizzare e gestire **attività di divulgazione** finalizzate a promuovere l'utilizzo della crittografia come strumento di cybersicurezza;
- promuovere, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, la **collaborazione** con **università e centri di ricerca** per la valorizzazione dello sviluppo di **nuovi algoritmi proprietari**, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli **organismi esteri** che svolgono analoghe funzioni.

A tal fine, la disposizione istituisce presso l'ACN il **Centro nazionale di crittografia**, con funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ossia non coperto dal segreto. Il funzionamento del centro è disciplinato con provvedimento del direttore generale dell'Agenzia. Viene poi precisato che all'istituzione del Centro si provvede nell'ambito delle risorse umane, strumentali e finanziarie disponibili e senza nuovi oneri a carico della finanza pubblica.

L'articolo in esame fa salve le competenze dell'**Ufficio centrale per la segretezza**.

L'Ufficio centrale per la segretezza (UCSe), è un organo istituito nell'ambito del Dipartimento delle informazioni per la sicurezza (DIS), la struttura di coordinamento dei servizi di informazione; l'Ufficio è disciplinato dall'articolo 9 della legge n. 124 del 2007. All'UCSe competono:

- gli adempimenti istruttori relativi all'esercizio delle funzioni del Presidente del Consiglio dei ministri quale Autorità nazionale per la sicurezza, a tutela del segreto di Stato;
- lo studio e la predisposizione delle disposizioni esplicative volte a garantire la sicurezza di tutto quanto è coperto dalle classifiche di segretezza con riferimento sia ad atti, documenti e materiali, sia alla produzione industriale;
- il rilascio e la revoca dei nulla osta di sicurezza (NOS), e la tenuta dell'elenco di tutti i soggetti muniti di NOS.

La disposizione in esame fa in particolare salve le competenze del'UCSe con riferimento alle informazioni e alle attività finalizzate alla tutela amministrativa del segreto di Stato e delle classifiche di segretezza, previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della citata legge 124/2007 (si ricorda che i regolamenti di attuazione della legge 124/2007 non vengono pubblicati).

Vengono infine fatte salve le competenze del citato Dipartimento per le informazioni per la sicurezza (DIS) e dei due servizi di informazione operativi, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI), di cui agli articoli 4, 6 e 7 della medesima legge 124/2007.

Articolo 11
(Procedimento sanzionatorio per le violazioni in materia di cybersicurezza di competenza dell'Agenzia)

L'**articolo 11,** modificato dalla **Camera dei deputati**, definisce **termini e modalità per l'adozione del regolamento** che stabilisce i criteri, anche temporali, 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. **Nel corso dell'esame presso la Camera dei deputati**, è stato aggiunto nel procedimento anche il **parere delle Commissioni parlamentari** competenti per materia.

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 procedimentali (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 12
(Disposizioni in materia di personale dell'Agenzia per la cybersicurezza nazionale)

L'**articolo 12, modificato dalla Camera,** 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 - ACN** che abbiano partecipato, nell'interesse e a spese dell'Agenzia stessa, a specifici **percorsi formativi di specializzazione**. Sono tuttavia previste specifiche **cause di esclusione** dall'applicazione del richiamato divieto.
Inoltre, con una modifica **introdotta dalla Camera** viene temporaneamente portato da 5 a 3 anni il periodo di permanenza minima nell'Aerea operativa ai fini del **passaggio del personale ACN** all'Area manageriale.

Più nel dettaglio, **il comma 1,** 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.

Si ricorda che il DL 82/2021, che ha istituito l'Agenzia, demanda ad un apposito regolamento la disciplina del contingente di personale addetto all'ACN. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale di ruolo dell'Agenzia, un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia (art. 12 DL 82/2021).

Tale disposizione è stata attuta con il DPCM 9 dicembre 2021, n. 224, recante il regolamento del personale dell'Agenzia per la cybersicurezza nazionale. L'art. 128 del regolamento fa rinvio, per quanto non disciplinato direttamente, alle norme, in quanto applicabili, relative allo stato giuridico dei dipendenti della Banca d'Italia e a quelle del testo unico del pubblico impiego di cui al D.Lgs. 165/2001.

Sulla scorta di tale disposizione è stato adottato il DPCM 23 aprile 2024 (pubblicato nella *Gazzetta Ufficiale* 15 maggio 2024, n. 112) che detta disposizioni in materia di incompatibilità successiva alla cessazione del rapporto alle dipendenze dell'ACN del direttore generale e del vicedirettore generale e del personale di ruolo che nell'ultimo anno di servizio ha ricoperto posizioni dirigenziali di capo servizio, di vice capo servizio, di capo divisione, di capo di altre unità organizzative di pari livello, ovvero di dirigente in *staff* ai Servizi, cui sono attribuite, sulla base delle norme interne, competenze amministrative in materia di certificazione, vigilanza e sanzioni. In particolare, viene esteso a tale personale il divieto di intrattenere direttamente rapporti di collaborazione, di consulenza o di impiego con i soggetti regolati nonché con società controllate da questi ultimi. Si tratta del medesimo divieto previsto per i componenti e dirigenti di CONSOB, Banca d'Italia e Istituto per la vigilanza sulle assicurazioni dall'art. 29-*bis* della L. 262/2005, cui il DPCM 23 aprile 2024 fa rinvio.

Il **comma 2**, **introdotto dalla Camera**, dispone che, fino al 31 dicembre 2026, per il personale dell'ACN il requisito di permanenza minima nell'Area operativa ai fini del passaggio all'Area manageriale e alte professionalità è fissato in tre anni, anziché 5 come previsto in via ordinaria dal regolamento del personale dell'ACN (DPCM 9 dicembre 2021, n. 224).

Il citato DPCM 224/2021 prevede che il ruolo del personale dell'ACN è articolato in nell'Area manageriale e alte professionalità e nell'Area operativa (art. 1). L'accesso ad entrambe le aree avviene tranne pubblico concorso (art. 8). L'accesso all'Area manageriale avviene anche per concorso interno riservato al personale in possesso del requisito di 5 anni di permanenza nell'Area operativa (art. 12).

.

Articolo 13
(Disposizioni relative al personale cessato degli organismi di informazione per la sicurezza)

L'**articolo 13** pone al personale del sistema di informazione per la sicurezza della Repubblica taluni divieti, per un lasso di tre anni dalla cessazione dell'incarico, in ordine allo svolgimento di attività lavorativa o all'esercizio di cariche, presso determinati enti.

Il **comma 1** dispone che coloro abbiano ricoperto la carica di direttore generale e di vice direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE) o dell'Agenzia informazioni e sicurezza interna (AISI), ovvero vi abbiano svolto incarichi dirigenziali di prima fascia di preposizione a strutture organizzative di livello dirigenziale generale, **non possano nei tre anni successivi alla cessazione dell'incarico svolgere – salvo autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata ove istituita – attività lavorativa, professionale o consulenziale, né possano ricoprire cariche, presso soggetti esteri, pubblici o privati, ovvero presso soggetti privati italiani che svolgano attività di rilevanza strategica** (secondo la perimetrazione resa dal decreto-legge n. 21 del 2012).

L'autorizzazione allo svolgimento dell'attività lavorativa o di cariche è concessa, avuto comunque riguardo alle esigenze di protezione del patrimonio informativo acquisito e di evitare pregiudizi per la sicurezza nazionale.

Il **comma 2** pone un divieto – inderogabile – al personale del ruolo unico del personale dei servizi di informazione per la sicurezza e del DIS (ruolo previsto dall'articolo 21 della legge n. 124 del 2007, la quale reca disciplina del sistema di informazione per la sicurezza della Repubblica) di svolgere, nei tre anni successivi alla cessazione dal servizio, attività lavorativa, professionale o consulenziale, ovvero ricoprire cariche, **presso enti o privati titolari di licenza per prestare vigilanza o custodia** (licenza del prefetto, ai sensi dell'articolo 134 del Testo unico di pubblica sicurezza, recato dal r.d. n. 773 del 1931**), o comunque presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa**.

Ed il **comma 3** prevede per quel medesimo personale, qualora abbia partecipato a specifici percorsi formativi di specializzazione nell'interesse e a spese delle DIS, dell'AISE e dell'AISI, un divieto di

assunzione o di assunzione di **incarichi presso soggetti privati, per svolgere le mansioni per le quali abbia beneficiato delle attività formative** medesime. Il divieto ha la durata di tre anni a decorrere dalla data di completamento dell'ultimo dei percorsi formativi.

I contratti conclusi e gli incarichi conferiti in violazione dei divieti posti dai commi sopra ricordati sono nulli, specifica il **comma 4**.

Infine il **comma 5** demanda a regolamento adottato con d.P.C.m previo parere del Comitato parlamentare per la sicurezza della Repubblica e sentito il Comitato interministeriale per la sicurezza della Repubblica (tale il contenuto del rinvio normativo all'articolo 43 della legge n. 124 del 2007) la definizione delle procedure di autorizzazione – per i casi autorizzabili, ai sensi del comma 1 – nonché gli obblighi di dichiarazione e di comunicazione a carico dei dipendenti.

Risulta demandata al medesimo regolamento altresì la determinazione dei "casi in cui *non* si applicano i divieti di cui ai commi *2* e 3" – *secondo formulazione che parrebbe suscettibile di approfondimento, posto che il comma 2 si direbbe lasciare esiguo margine all'individuazione di fattispecie disapplicative* – nonché le modalità di individuazione dei percorsi formativi che determinano il divieto di cui al comma 3.

Articolo 14
(Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici)

L'**articolo 14, modificato dalla Camera,** introduce alcuni **criteri di cybersicurezza** nella disciplina dei **contratti pubblici**: nel caso di **approvvigionamento di** specifiche categorie 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 del **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 sicurezza della Repubblica (CISR)** per l'occasione nella composizione di cui all'art. 10, comma 1, del DL 82/2021, che prevede la partecipazione del Ministro delegato per l'innovazione tecnologica e la transizione digitale e del direttore generale dell'Agenzia, qualora il CISR è convocato in situazioni di crisi cybernetica.

Nella formulazione originaria si prevedeva il parere del Comitato interministeriale per la cybersicurezza (CIC).

Per una disamina del ruolo e delle funzioni del CISR si veda la scheda relativa all'articolo 7 del presente provvedimento.

Con il DPCM di cui sopra sono individuati – per determinate categorie tecnologiche di beni e servizi informatici, **come chiarito nel corso dell'esame della Camera** - 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.

A seguito dell'**approvazione di una proposta emendativa alla Camera**, il DPCM individua anche i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti **criteri di premialità** per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza **italiane** o di Paesi appartenenti all'**Unione europea** o di Paesi aderenti all'Alleanza atlantica (**NATO**) o di **Paesi terzi** individuati con il medesimo DPCM di cui sopra tra quelli che sono **parte di accordi di collaborazione** con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

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 **soggetti 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,** al riguardo si rinvia al box presente nella scheda relativa all'articolo 5).

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".

prevedono – nei casi individuati dal DPCM di cui al comma 1 - criteri di premialità (**introdotti nel corso dell'esame della Camera**) per le proposte o per le offerte che contemplino l'uso di **tecnologie di cybersicurezza italiane** o di **Paesi appartenenti all'Unione europea** o di Paesi aderenti alla **NATO** o di **Paesi terzi** tra quelli che sono parte di **accordi di collaborazione** con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

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 perimetro di sicurezza nazionale cibernetica.

Le disposizioni di approvvigionamento di beni, sistemi e servizi di *information and communication technology* destinati ad essere impiegati nelle reti e nei 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, **modificato in sede referente** (il testo originario faceva riferimento alle 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).

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, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica (articolo 1, comma 7, lettera c), del decreto-legge n. 105 del 2019).

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

In materia di certificazione per la cybersicurezza a livello europeo, rileva il Regolamento (UE) 2019/881 (Regolamento sulla Cybersicurezza) del 17 aprile 2019 relativo all'ENISA, l'Agenzia

dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione. Il regolamento, allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, stabilisce, da un lato, gli obiettivi, i compiti e l'organizzazione dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), e, dall'altro, un quadro comune per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, anche al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione. Al tempo stesso, il quadro comune contempla l'esistenza di autorità nazionali di certificazione (articolo 58 del Regolamento); inoltre, l'articolo 1, comma 2, del Regolamento fa salve le competenze degli Stati membri per quanto riguarda le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

Articolo 15
(Resilienza operativa digitale per il settore finanziario)

L'**articolo 15** introduce nel testo dell'articolo 16 della legge di delegazione europea 2022-2023 **nuovi principi e criteri direttivi specifici** a cui il Governo dovrà attenersi nel recepimento della normativa europea in materia di **resilienza operativa digitale per il settore finanziario**.

L'**articolo 15, introdotto dalla Camera dei deputati**, reca delle modifiche all'articolo 16**,** comma 2 della legge 21 febbraio 2024. n. 15 (legge di delegazione europea 2022-2023), in materia di delega al Governo per l'adeguamento della normativa nazionale ad alcune disposizioni normative dell'Unione europea (regolamento (UE) 2022/2554 e direttiva (UE) 2022/2556) relative alla **resilienza operativa digitale per il settore finanziario**.

In particolare, il sopra citato comma 2 all'articolo 16, stabilisce che, nell'esercizio della delega (adeguamento della normativa nazionale al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022) per quanto riguarda la resilienza operativa digitale per il settore finanziario, il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici:

a) apportare alla normativa vigente le occorrenti modifiche e integrazioni, anche al sistema sanzionatorio, necessarie all'adeguamento dell'ordinamento giuridico nazionale al regolamento (UE) 2022/2554 e al recepimento della direttiva (UE) 2022/2556, incluso l'eventuale esercizio delle opzioni, anche mediante la normativa secondaria di cui alla lettera d), previste dal regolamento (UE) 2022/2554. Nell'adozione di tali modifiche e integrazioni il Governo tiene conto degli orientamenti delle Autorità di vigilanza europee, degli atti delegati adottati dalla Commissione europea e delle disposizioni legislative nazionali di recepimento delle seguenti direttive strettamente correlate al regolamento (UE) 2022/2554:
    1) la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva

(UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

2) la direttiva (UE) 2022/2557 del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

b) assicurare che alle autorità competenti, individuate ai sensi dell'articolo 19, comma 1, paragrafo 2, e dell'articolo 46 del regolamento (UE) 2022/2554, siano attribuiti tutti i poteri di vigilanza, di indagine e sanzionatori per l'attuazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2556, coerentemente con il riparto di competenze nel settore finanziario nazionale;

c) attribuire alle autorità di cui alla lettera b) il potere di imporre le sanzioni e le altre misure amministrative previste dagli articoli 42, paragrafo 6, e 50 del regolamento (UE) 2022/2554, nel rispetto dei limiti edittali e delle procedure previsti dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure amministrative da parte delle autorità anzidette, avuto riguardo al riparto di competenze nel settore finanziario nazionale;

d) prevedere, ove opportuno, il ricorso alla disciplina secondaria adottata dalle autorità indicate alla lettera b) secondo le rispettive competenze.

La norma in esame, attraverso l'inserimento **della nuova lettera c-*bis* al comma 2 del richiamato articolo 16**, introduce nuovi principi e criteri direttivi specifici a cui il Governo dovrà attenersi nel recepimento della normativa europea quanto riguarda la resilienza operativa digitale per il settore finanziario.

Si ricorda che per resilienza operativa digitale si intende, secondo la definizione indicata dal Regolamento (UE) 2022/2554, la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi delle tecnologie dell'informazione e della comunicazione (TIC), l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni.

In particolare, la disposizione prevede che il Governo sarà tenuto ad apportare alla disciplina degli **intermediari finanziari** iscritti nell'albo previsto dall'articolo 106 del decreto legislativo 1° settembre 1993, n. 385 e di **Poste Italiane SpA per l'attività del patrimonio Bancoposta** (di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144), le occorrenti modifiche e integrazioni, **anche mediante la**

normativa secondaria di cui alla lettera *d*) del medesimo articolo 16, per conseguire **un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario** nel suo complesso, in particolare:

i) **definendo presidi** in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554;

ii) **tenendo conto,** nella definizione dei presidi di cui al punto i), del **principio di proporzionalità e delle attività** svolte dagli intermediari finanziari e da Bancoposta;

iii) attribuendo alla **Banca d'Italia** l'esercizio nei confronti di questi soggetti dei poteri di **vigilanza, di indagine e sanzionatori** richiamati alla lettera *b*) del medesimo articolo 16.

Il **regolamento (UE) 2022/2554 (**c.d. DORA, *Digital Operational Resilience Act*) - riconducibile al c.d. "Pacchetto finanza digitale" - è volto a definire un quadro dettagliato sulla resilienza operativa digitale per le entità finanziarie dell'UE al fine di:

-approfondire la dimensione della gestione dei rischi digitali e in particolare migliorare e razionalizzare la gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technologies – ICT) da parte delle entità finanziarie;

-istituire test accurati dei sistemi di ICT e accrescere la consapevolezza da parte delle autorità di vigilanza dei rischi informatici e degli incidenti cui sono esposte le entità finanziarie;

-conferire alle autorità di vigilanza finanziaria poteri di sorveglianza sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi;

- istituire un meccanismo coerente di segnalazione degli incidenti.

Il Regolamento in esame si applica ad un novero ampio di entità finanziarie regolamentate, tra cui enti creditizi, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, gestori di fondi di investimento alternativi e società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, agenzie di rating del credito, revisori legali e società di revisione, fornitori di servizi di *crowdfunding* (art. 2).

Il Capo II del regolamento si compone degli articoli da 5 a 16 ed è dedicato alla gestione dei rischi informatici. L'art. 5 stabilisce che le entità finanziarie devono predisporre un quadro per la gestione dei rischi relativi alle ICT efficace e prudente. Le entità finanziarie devono predisporre un quadro per la gestione dei rischi informatici (art. 6) "solido, esaustivo ed adeguatamente documentato", che consenta di affrontare i rischi in maniera "rapida, efficiente ed esaustiva", assicurando un elevato livello di resilienza operativa digitale corrispondente alle esigenze, alle dimensioni e alla complessità delle loro attività commerciali. Esso deve comprendere anche una strategia di resilienza digitale, che definisca le modalità di attuazione del quadro medesimo.

In particolare, le entità finanziarie devono:

-utilizzare strumenti e sistemi di ICT idonei, affidabili, di sufficiente capacità e resilienti, tali da fare fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse (art. 7);

-identificare costantemente tutte le fonti di rischi relativi alle ICT (art. 8);

-introdurre misure di protezione e prevenzione (art. 9);

-individuare tempestivamente le attività anomale, compresi i problemi di prestazione della rete delle ICT e gli incidenti a esse connessi, nonché per individuare i potenziali singoli punti di vulnerabilità rilevanti, c.d. points of failure (art. 10);

-mettere in atto politiche di continuità operativa e sistemi e piani di risposta e ripristino in caso di disastro relativo alle ICT (artt. 11 e 12).

Ulteriori disposizioni del Capo II dispongono in ordine agli strumenti di riesame delle situazioni critiche, alle capacità evolutive di resilienza dei sistemi e alla comunicazione tra le entità finanziarie. L'art. 16 chiude il Capo II in parola e reca una disciplina concernente talune entità che non sono destinatarie delle disposizioni sopra ricordate.

Il Capo III (artt. da 17 a 23) disciplina le misure per la gestione, classificazione e segnalazione degli incidenti informatici. Le entità finanziarie devono approntare un processo di gestione per individuare, gestire e notificare gli incidenti (art. 17), per classificarli e determinarne l'impatto, sulla base dei criteri ivi specificati (art. 18) e segnalarli alle autorità competenti secondo determinate modalità (art. 19). Ulteriori disposizioni riguardano l'armonizzazione dei modelli e dei contenuti per le segnalazioni e la centralizzazione delle segnalazioni. Si prevede, infatti, la possibilità di istituire un polo unico dell'UE per la segnalazione degli incidenti gravi connessi alle ICT da parte delle entità finanziarie (art. 21).

Il Capo IV (composto dagli articoli da 24 a 27) dispone in ordine ai test di resilienza, ordinari ed avanzati, al fine di identificare punti deboli, carenze o lacune, nonché verificare la capacità di attuare tempestivamente misure correttive. Si prevede un'applicazione proporzionata di tali prescrizioni: solo talune entità hanno l'obbligo di svolgere prove avanzate mediante test di penetrazione guidati dalla minaccia (TLPT). Tali test sono eseguiti da soggetti che rispettano specifici requisiti.

Il Capo V (articoli da 28 a 44) reca disposizioni concernenti i rischi informatici derivanti da terzi, in considerazione del fatto che le società finanziarie dipendono sempre più da società tecnologiche non finanziarie per i loro servizi ICT. A tale riguardo, l'art. 30 precisa le principali disposizioni contrattuali inerenti a diritti e obblighi dell'entità finanziaria e del fornitore terzo di servizi ITC. Tali diritti e obblighi dovranno essere attribuiti chiaramente e definiti per iscritto. In particolare, i contratti che disciplinano il rapporto dovranno contenere una descrizione chiara e completa dei servizi, l'indicazione delle località in cui i dati devono essere trattati, descrizioni complete del livello dei servizi accompagnate da obiettivi di prestazione quantitativi e qualitativi, disposizioni pertinenti in materia di accessibilità,

disponibilità, integrità, sicurezza e protezione dei dati personali, nonché garanzie per l'accesso, il ripristino e la restituzione in caso di inadempienze dei fornitori terzi di servizi di ICT, termini di preavviso e obblighi di segnalazione dei fornitori terzi di servizi di ICT, diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tale scopo, strategie di uscita dedicate. Inoltre, il medesimo Capo V reca disposizioni finalizzate a sottoporre i fornitori terzi di servizi di ICT critici a un quadro di sorveglianza dell'Unione per garantire la convergenza in materia di vigilanza.

Il Capo VI si compone del solo art. 45, il quale mira a consentire alle entità finanziarie di istituire accordi per lo scambio di informazioni e dati sulle minacce informatiche.

Il regolamento, inoltre, individua le autorità competenti ad assicurare il rispetto degli obblighi disposti dalla nuova disciplina in relazione alle varie categorie di entità finanziarie (Capo VII, artt. 46-56). Il Capo VIII dispone in ordine agli atti delegati mentre il Capo IX reca le disposizioni transitorie e finali e le modifiche ai regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e regolamento (UE) 2016/1011.

Il regolamento si applica a decorrere dal 17 gennaio 2025 (art. 64).

La **direttiva (UE) 2022/2556** introduce un'esenzione temporanea per i sistemi multilaterali di negoziazione e modifica o chiarisce talune disposizioni delle vigenti direttive UE relative ai servizi finanziari onde conseguire gli obiettivi previsti dalla proposta sulla resilienza operativa digitale. La direttiva dovrà essere recepita dagli Stati membri entro il 17 gennaio 2025.

Articolo 16
(Modifiche al codice penale)

L'**articolo 16,** modificato nel corso dell'esame presso la Camera dei deputati, reca modifiche al codice penale in materia di **prevenzione e contrasto dei reati informatici**.

Nel segnalare che le disposizioni recate dal comma 1, lettera *a)*, risultano conseguenti alle modifiche introdotte dalla lettera *t)* del medesimo comma 1 (su cui vedi *infra*), si fa presente che il **comma 1**, **lett. *b)***, 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**);
- nella fattispecie pluriaggravata in cui ricorrano 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**);

Il **comma 1, lett. *c)***, 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[5]) (**n. 3**).

Il **comma 1**, **lett. *e)***, 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 ann**i 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

[5] 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".

con violazione dei doveri o da un **investigatore privato** anche abusivo (secondo comma).

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.** ***f)***, 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 **intercett**a 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 **circostanze 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**);
- 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[6]) (**n. 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) (**nn. 3 e 4**).

Il **comma** 1, **lett.** ***g)***, 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 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).

[6] 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".

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

In particolare, si dispone:

- la previsione – mediante rinvio all'art. 617-*quater*, quarto comma, n. 2, come modificato dalla lett. *f)* - 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. *f)*[7]) (**n. 2**).

Il **comma 1**, **lett. *h)***, 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

[7] 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".

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).

Il **comma 1**, **lett. *i)***, reca una **disposizione di coordinamento** volta a modificare la rubrica del capo III-*bi*s del titolo XII del libro secondo del codice penale, ora denominata "*Disposizioni comuni",* conseguentemente all'introduzione dell'art. 623-*quate*r (vedi *infra*).

Il **comma 1**, **lett. *l),*** 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. *m)***, 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 ann**i e con la **multa da euro 5.000 a euro 10.000**.

Si prevede, inoltre, la **reclusione da 8 a 22 anni** e la **multa da euro 6.000 a euro 18.000** se ricorre taluna delle circostanze aggravanti indicate dal terzo comma dell'articolo 628 c.p. relativo al 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.

Il **comma** 1, **lett.** ***n)***, 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.** ***o)***, 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.

È 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[8] **(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);

[8] 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.

- 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 **comma 1**, **lett. *p)***, 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. *q),*** 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.[9] (che viene contestualmente abrogato dalla **lett. *d***): è punito con la **reclusione fino a 2 anni** e con la **multa fino a euro 10.329** 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. *r)***, 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.

[9] 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.

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 **comma 1**, **lett. *s)***, 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).

Attraverso una modifica approvata nel corso dell'esame presso la **Camera**, sono state **aggiunte tre ulteriori lettere** al comma 1.

L'intervento principale è quello contenuto nella **lettera t)**, che inserisce nell'art. 640 c.p., secondo comma, una **nuova circostanza aggravante del reato di truffa** (numero 2-*ter*), nel caso in cui il **fatto sia commesso a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui individuazione**.

> L'art. 640 c.p. (*Truffa*) punisce con la reclusione da sei mesi a tre anni e con la multa da 51 a 1.032 euro chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno (primo comma).
>
> Il secondo comma individua tre aggravanti speciali del reato, che comportano un aumento di pena (reclusione da uno a cinque anni e multa da 309 a 1.549 euro):
>
> 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;
>
> 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità;
>
> 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5), c.p. (il riferimento è alla cd. minorata difesa cioè l'avere profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa).

La medesima **lettera t)**, inoltre, prevede l'applicazione alla **nuova circostanza aggravante del reato di truffa** del **regime di procedibilità a querela della persona offesa**, diversamente da quanto disposto per le altre fattispecie aggravate del reato di truffa che sono invece procedibili d'ufficio.

Consequenziali al suddetto intervento sono le modifiche apportate dalle **lettere a) e u)**, che intervengono, rispettivamente, sugli articoli 240 c.p. e 640-*quater* c.p. per disporre, in relazione al reato di truffa aggravata introdotto dalla lettera t):

- la misura di sicurezza prevista dall'art. 240, comma 2, c.p. che disciplina la **confisca obbligatoria dei beni e degli strumenti informatici o telematici** utilizzati in tutto o in parte per la commissione del reato, nonché dei beni che costituiscono il profitto o il prodotto del reato medesimo ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore

corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca diretta del profitto o del prodotto;

- ai sensi dell'art. 640-*quater* c.p., l'osservanza, in quanto applicabili, delle disposizioni contenute nell'art. **322-*ter* c.p.**, che stabilisce, in caso di **condanna** o di applicazione della pena su richiesta delle parti, **la confisca dei beni che costituiscono il profitto o il prezzo del reato**, salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto.

Nel corso dell'esame presso la **Camera dei deputati** sono state altresì approvate alcune proposte emendative volte a **sopprimere il divieto di equivalenza o prevalenza delle circostanze attenuanti sulle circostanze aggravanti** che, nel testo originario, era previsto in relazione alle fattispecie di cui agli artt. 615-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*ter* c.p., oggetto di modifica ad opera del presente disegno di legge (vedi *supra*).

In riferimento al **divieto di prevalenza delle circostanze attenuanti sulle circostanze 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».

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
Art. 240 *(Confisca)*	Art. 240 *(Idem)*
Nel caso di condanna, il giudice può ordinare la confisca delle cose che servirono o furono destinate a commettere il reato, e delle cose, che ne sono il prodotto o il profitto.	*Identico*
	[Art. 16, comma 1, lett. a)]
È sempre ordinata la confisca: 1. delle cose che costituiscono il prezzo del reato; 1-*bis*. dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-bis, 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*ter* e 640-*quinquies* nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca del profitto o del prodotto diretti; 2. delle cose, la fabbricazione, l'uso, il porto, la detenzione o l'alienazione delle quali costituisce reato, anche se non è stata pronunciata condanna.	È sempre ordinata la confisca: 1. delle cose che costituiscono il prezzo del reato; 1-*bis*. dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-bis, 635-*ter*, 635-*quater*, 635-*quinquies*, **640, secondo comma, numero 2-*ter*,** 640-*ter* e 640-*quinquies* nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca del profitto o del prodotto diretti; 2. delle cose, la fabbricazione, l'uso, il porto, la detenzione o l'alienazione delle quali costituisce reato, anche se non è stata pronunciata condanna.
Le disposizioni della prima parte e dei numeri 1 e 1-*bis* del capoverso precedente non si applicano se la cosa o il bene o lo strumento informatico o telematico	*Identico*

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
appartiene a persona estranea al reato. La disposizione del numero 1-*bis* del capoverso precedente si applica anche nel caso di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale.	
La disposizione del n. 2 non si applica se la cosa appartiene a persona estranea al reato e la fabbricazione, l'uso, il porto, la detenzione o l'alienazione possono essere consentiti mediante autorizzazione amministrativa.	*Identico*
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.	*Identico*
	[Art. 16, co. 1, lett. b), n. 1]
La pena è della reclusione da **uno a cinque** anni:	La pena è della reclusione da **due a dieci** 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;	*Identico*
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;	2) se il colpevole per commettere il fatto usa **minaccia o** violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o	3) se dal fatto deriva la distruzione o il danneggiamento del sistema o

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.	l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento **ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare** dei dati, delle informazioni o dei programmi in esso contenuti.
	[Art. 16, co. 1, lett. b), n. 2]
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 pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione **da uno a cinque anni e da tre a otto anni**.	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 pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione **da tre a dieci anni e da quattro a dodici anni.**
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.	*Identico*
Art. 615-*quater* *(Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)*	Art. 615-*quater* *(idem)*
	[Art. 16, co. 1, lett. c), n. 1]
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	Chiunque, al fine di procurare a sé o ad altri un **vantaggio** 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

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
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.	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.
	[Art. 16, co. 1, lett. c), n. 2]
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-*quater*.	**La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-*ter*, secondo comma, numero 1).**
	[Art. 16, co. 1, lett. c), n. 3]
	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.
	[Art. 16, co. 1, lett. d)]
Art. 615-*quinquies* *(Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*	Art. 615-*quinquies* *(idem)*
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	***Abrogato***

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
e con la multa sino a euro 10.329.	
Art. 617-*bis* *(Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche)*	Art. 617-*bis* *(idem)*
Comma 1 *Omissis*.	Comma 1 *Omissis*.
	[Art. 16, co. 1, lett. e), n.1]
	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).
	[Art. 16, co. 1, lett. e), n.2]
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 **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.**	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.
Art. 617-*quater* *(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)*	Art. 617-*quater* *(idem)*
Commi da 1 a 3 *Omissis*	Commi da 1 a 3 *Omissis*
	[Art. 16, co. 1, lett. f), n.1]

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
Tuttavia si procede d'ufficio e la pena è della reclusione da **tre a otto** anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) 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, ovvero con abuso della qualità di operatore del sistema; **3) da chi esercita anche abusivamente la professione di investigatore privato.**	Tuttavia si procede d'ufficio e la pena è della reclusione da **quattro a dieci** anni se il fatto è commesso: **1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-*ter*, terzo comma;** 2) **in danno di un pubblico ufficiale, nell'esercizio o a causa delle sue funzioni o 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; ***Abrogato***
Art. 617-*quinquies* *(Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)*	Art. 617-*quinquies* *(idem)*
Comma 1 *Omissis*	Comma 1 *Omissis*
	[Art. 16, co. 1, lett. g), n.1]
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater*.	**Quando ricorre taluna delle circostanze di cui all'articolo 617-*quater*, quarto comma, numero 2), la pena è della reclusione da due a sei anni.**
	[Art. 16, co. 1, lett. g), n.2]
	Quando ricorre taluna delle circostanze di cui all'articolo 617-

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	***quater*, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.**
Art. 617-*sexies* *(Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)*	Art. 617-*sexies* *(idem)*
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.	*Identico*
	[Art. 16, co. 1, lett. h)]
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater*.	La pena è della reclusione da **tre a otto** anni nei casi previsti dal quarto comma dell'articolo 617-*quater*.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.	*Identico*
	[Art. 16, co. 1, lett. i)]
Capo III-*bis* *(Disposizioni comuni **sulla procedibilità**)*	Capo III-*bis* *(Disposizioni comuni)*
	[Art. 16, co. 1, lett. l)]
	Art. 623-*quater* ***(Circostanze attenuanti)***
	Le pene comminate per i delitti di cui agli articoli 615-*ter*, 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* sono

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	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 recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.** **Non si applica il divieto di cui all'articolo 69, quarto comma.**
Art. 629 *(Estorsione)*	Art. 629 *(idem)*
	[Art. 16, co. 1, lett. m)]
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, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.	*Identico.*
La pena è della reclusione da sette a venti anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente.	La pena è della reclusione da sette a venti anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate **nel terzo comma dell'articolo 628**.
	Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	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 nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.
Art. 635-*bis* *(Danneggiamento di informazioni, dati e programmi informatici)*	Art. 635-*bis* *(idem)*
	[Art. 16, co. 1, lett. n)]
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 sei mesi a tre anni.	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 **due a sei anni.**
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.	**La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se**

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	è palesemente armato.
	[Art. 16, co. 1, lett. o), n.3]
Art. 635-*ter* *(Danneggiamento di informazioni, dati e programmi informatici* ***utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità****)*	Art. 635-*ter* *(Danneggiamento di informazioni, dati e programmi informatici* ***pubblici o di interesse pubblico****)*
	[Art. 16, co. 1, lett. o), n.1]
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, 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 **di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.**
	[Art. 16, co. 1, lett. o), n.2]
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.	**La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;** **3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione,**

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.
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.	**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).**
Art. 635-*quater* *(Danneggiamento di sistemi informatici o telematici)*	Art. 635-*quater* *(Danneggiamento di sistemi informatici o telematici)*
	[Art. 16, co. 1, lett. p), n. 1]
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 funzionamento è punito con la reclusione da uno a cinque anni**.**	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 funzionamento è punito con la reclusione da **due a sei** anni**.**
	[Art. 16, co. 1, lett. p), n. 2]
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.	**La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se**

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	è palesemente armato.
	[Art. 16, co. 1, lett. q)]
	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)***
	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. **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).** **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.**
Art. 635-*quinquies* *(Danneggiamento di sistemi informatici o telematici di **pubblica utilità**)*	Art. 635-*quinquies* *(Danneggiamento di sistemi informatici o telematici di **pubblico interesse**)*
	[Art. 16, co. 1, lett. r)]
Se il fatto di cui all'articolo 635-*quater* è	**Salvo che il fatto costituisca più grave**

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
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.	**reato, chiunque, mediante le condotte di cui all'articolo 635-*bis* 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.**
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.	**La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;** **3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.**
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.	**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).**
	[Art. 16, co. 1, lett. s)]

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
	Art. 639-*ter* *(Circostanze attenuanti)*
	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.
	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 recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi.
	Non si applica il divieto di cui all'articolo 69, quarto comma.
Art. 640 *(Truffa)*	Art. 640 *(Idem)*
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.	*Identico*
	[Art. 16, co. 1, lett. t), n. 1]
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o	La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o

Codice penale	
Testo vigente	**Modificazioni apportate dall'art. 16 A.S. 1143**
dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità; 2-*bis*. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5)**.**	dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità; 2-*bis*. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5)**;** **2-*ter*. Se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui identificazione.**
	[Art. 16, co. 1, lett. t), n. 2]
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal **capoverso precedente.**	Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal **secondo comma, a eccezione di quella di cui al numero 2-*ter*).**
Art. 640-*quater* *(Applicabilità dell'articolo 322*-ter)	Art. 640-*quater* *(Idem)*
	[Art. 16, co. 1, lett. t)]
Nei casi di cui agli articoli 640, secondo comma, **numero 1**, 640-*bis* e 640-*ter*, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'articolo 322-*ter*.	Nei casi di cui agli articoli 640, secondo comma, **numeri 1 e 2-*ter),*** 640-*bis* e 640-*ter*, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'articolo 322-*ter*.

Articolo 17
(Modifiche al codice di procedura penale)

L'**articolo 17** 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 15**.
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 17**, composto di un unico comma, ripartito in 3 lettere, introduce **modifiche** di natura procedurale **consequenziali a quelle introdotte nel codice penale** dal precedente articolo 15.

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**[10], 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[11]. Nello specifico i reati indicati al numero 7-*ter)* sono:

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

[10] 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.

[11] 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.

Codice di procedura penale	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
Art. 51 *(Uffici del pubblico ministero. Attribuzioni del procuratore della Repubblica distrettuale)*	Art. 51 *(idem)*
Commi da 1 a 3-*quater Omissis*	Commi da 1 a 3-*quater Omissis*
	[Art. 16, co. 1, lett. a)]
3-*quinquies*. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-*bis*, 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 609-*undecies*, 615-*ter*, 615-*quater*, **615-*quinquies,*** 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter* e 640-*quinquies* 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-*quinquies*. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-*bis*, 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 609-*undecies*, 615-*ter*, 615-*quater*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, **635-*quater*.1, 635-*quinquies,*** 640-*ter* e 640-*quinquies* del codice penale, **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,** 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 *(Proroga dei termini)*	Art. 406 *(idem)*
Commi 1 e 2 *Omissis*	Commi 1 e 2 *Omissis*
Commi 2-*bis* e 2-*ter* *Abrogati*	Commi 2-*bis* e 2-*ter* *Abrogati*
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	*Identico*

Codice di procedura penale	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
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.	*Identico*
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.	*Identico*
	[Art. 16, co. 1, lett. b)]
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 **4 e 7-*bis***. 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 **4), 7-*bis)* e 7-*ter)***. 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 *Omissis*	Commi da 6 a 8 *Omissis*
Art. 407 *(Termine di durata massima delle indagini preliminari)*	Art. 407 *(idem)*
1. Salvo quanto previsto all'articolo 393 comma 4, la durata delle indagini	*Identico*

Codice di procedura penale	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
preliminari non può comunque superare diciotto mesi o, se si procede per una contravvenzione, un anno.	
2. La durata massima è tuttavia di due anni se le indagini preliminari riguardano: a) i delitti appresso indicati: 1) delitti di cui agli articoli 285, 286, 416-*bis* e 422 del codice penale, 291-*ter*, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-quater, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43; 2) delitti consumati o tentati di cui agli articoli 575, 628, terzo comma, 629, secondo comma, e 630 dello stesso codice penale; 3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-*bis* del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; 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; 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	

Codice di procedura penale	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
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;	*Identico*
	[Art. 16, co. 1, lett. c)]
	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

Codice di procedura penale	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
	alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.
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; c) indagini che richiedono il compimento di atti all'estero; d) procedimenti in cui è indispensabile mantenere il collegamento tra più uffici del pubblico ministero a norma dell'articolo 371.	*Identiche*
3. Salvo quanto previsto dall'articolo 415-*bis*, 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.	*Identico*
3-*bis* *Abrogato*	

Articolo 18
(Modifiche alle norme sui collaboratori di giustizia di cui al decreto-legge n. 8 del 1991)

L'**articolo 18** 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 18** 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.[12] 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

[12] 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.

Decreto-legge 15 gennaio 1991, n. 8	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
Art. 9 *(Condizioni di applicabilità delle speciali misure di protezione)*	Art. 9 *(idem)*
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.	*Identico*
	[Art. 17, co. 1, lett. a)]
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*, **o all'articolo 371-*bis*, comma 4-*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.
Commi da 3 a 6 *Omissis*	Commi da 3 a 6 *Omissis*

Decreto-legge 15 gennaio 1991, n. 8	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
Art. 11 *(Proposta di ammissione)*	Art. 11 *(idem)*
Comma 1 *Omissis*	Comma 1 *Omissis*
	[Art. 17, co. 1, lett. b)]
2. Quando le dichiarazioni indicate nel comma 1 attengono a procedimenti per taluno dei delitti previsti dall'articolo 51, commi 3-*bis* e 3-*quater*, 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-*bis* e 3-*quater*, **o all'articolo 371-*bis*, comma 4-*bis*,** 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 *Omissis*	Commi da 3 a 8 *Omissis*
Art. 16-*nonies* *(Benefici penitenziari)*	Art. 16-*nonies* *(idem)*
	[Art. 17, co. 1, lett. c)]
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-*bis*, 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	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-*bis*, **o all'articolo 371-*bis*, comma 4-*bis*,** 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

Decreto-legge 15 gennaio 1991, n. 8	
Testo vigente	**Modificazioni apportate dall'A.S. 1143**
premio e l'ammissione alla misura della detenzione domiciliare prevista dall'articolo 47-*ter* della legge 26 luglio 1975, n. 354, e successive modificazioni, sono disposte su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo.	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, e successive modificazioni, sono disposte su proposta ovvero sentito il procuratore nazionale antimafia e antiterrorismo.
Commi da 2 a 8-*bis Omissis*	Commi da 2 a 8-*bis Omissis*

Articolo 19
(*Modifica al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203*)

L'articolo 19 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 19** - 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. 15 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 20
(*Modifiche al decreto legislativo 8 giugno 2001, n. 231*)

L'articolo 20 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 20** 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 in esame:

- **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. 15 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 15, 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 21
(*Modifica alla legge 11 gennaio 2018, n. 6*)

L'articolo 21 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 21** 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 17, 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 22
(*Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109*)

L'**articolo 22** 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 22** 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 del decreto legge n. 82 del 2021, 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**. È 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 in esame 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'articolo1, 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 del 2021 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 subìto 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. 15 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 23
(Verifica della sicurezza negli accessi alle banche dati presso gli uffici giudiziari)

L'**articolo 23**, inserito dalla **Camera dei deputati**, stabilisce che in occasione delle **ispezioni presso gli uffici giudiziari** sia verificato il **rispetto delle prescrizioni di sicurezza negli accessi alle banche dati in uso**.

L'**articolo 23** reca alcune modifiche all'articolo 7 della legge 12 agosto 1962, n. 1311, recante organizzazione e funzionamento dell'**ispettorato generale presso il Ministero della giustizia**.

Il primo intervento recato dall'articolo in commento (**lettera *a***) riguarda le **ispezioni ordinarie** di cui al primo comma del citato art. 7, che sono **disposte dal capo dell'ispettorato generale** in tutti gli uffici giudiziari, conformemente alle direttive impartite dal Ministro della giustizia, allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti. Nell'ambito di tali ispezioni, attraverso la modifica introdotta, si prevede che sia effettuata anche la **verifica delle prescrizioni di sicurezza negli accessi alle banche dati**.

Si ricorda che ai sensi del secondo comma dell'art. 7 le suddette ispezioni hanno di norma una frequenza triennale, ma possono essere ripetute entro un termine minore negli uffici ove siano state riscontrate o per i quali vengono segnalate deficienze o irregolarità.

Il secondo intervento recato dall'articolo in commento (**lettera *b***) riguarda le **ispezioni parziali** di cui al terzo comma dell'art. 7, che sono **disposte dal Ministro della giustizia** negli uffici giudiziari quando egli lo ritenga opportuno, allo scopo di verificare la produttività degli stessi nonché l'entità e la tempestività del lavoro di singoli magistrati. In base alla modifica apportata dalla lettera in esame, simili ispezioni possono essere volte altresì all'accertamento del **rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati** in uso presso i medesimi uffici giudiziari.

In conseguenza delle modifiche apportate dall'articolo in commento, viene infine **modificata la rubrica del Capo II** che quindi reca "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a

sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari".

- ***La funzione ispettiva del Ministro della giustizia***

La funzione ispettiva del Ministro della giustizia trova il suo fondamento nell'art. 110 Cost., che, a fronte delle competenze assegnate al Consiglio superiore della magistratura dall'art. 105 Cost. in materia di assunzioni, assegnazioni, trasferimenti, promozioni e provvedimenti disciplinari riguardanti i magistrati, a salvaguardia dell'indipendenza della funzione giurisdizionale, delimita le competenze del Ministro della giustizia circoscrivendole all'organizzazione e al funzionamento dei servizi relativi alla giustizia.

Tra tali compiti rientra l'attività ispettiva svolta dal Ministero, regolamentata principalmente dalla legge 12 agosto 1962, n. 1311, recante organizzazione e funzionamento dell'ispettorato generale presso il Ministero di grazia e giustizia.

Nell'ambito del Ministero, la predetta attività ispettiva è demandata all'**Ispettorato generale**, costituito da un magistrato di Corte di cassazione con ufficio direttivo, con le funzioni di capo dell'ispettorato generale; da un magistrato di Corte di cassazione con ufficio direttivo ovvero da un magistrato di Corte di cassazione, con le funzioni di vice capo dell'ispettorato generale; da sette magistrati di Corte di cassazione, con le funzioni di ispettori generali capi; da dodici magistrati di corte d'appello, con le funzioni di ispettori generali (art. 1).

I magistrati addetti all'Ispettorato generale sono destinati al Ministero della giustizia con funzioni amministrative e sono collocati fuori ruolo (art. 2). All'Ispettorato generale sono destinati altresì funzionari del ruolo dirigenziale e trentasei direttori aggiunti di cancelleria con funzioni di collaborazione nel servizio ispettivo (art. 4).

Le verifiche svolte dall'Ispettorato sono riconducibili a tre tipologie (art. 7):

- **ispezione ordinaria**, disposta dal Capo dell'Ispettorato allo scopo di accertare se i servizi procedano secondo le leggi, i regolamenti e le istruzioni vigenti, con frequenza di norma triennale;
- **ispezione straordinaria**, disposta dal Capo dell'Ispettorato prima dello scadere del termine triennale negli uffici in cui sono state riscontrate o vengono segnalate deficienze o irregolarità;
- **ispezione mirata**, disposta dal Ministro che ne ha facoltà in ogni tempo, ogniqualvolta lo ritenga opportuno, al fine di accertare la produttività degli stessi nonché l'entità e la tempestività del lavoro svolto dai singoli magistrati.

Al termine della verifica, l'ispettore redige una relazione nella quale menziona succintamente le irregolarità e le lacune riscontrate nei servizi e formula le proposte atte ad eliminarle.

Se nel corso delle ispezioni vengono **accertati abusi o irregolarità gravi**, l'ispettore ne informa immediatamente il capo dell'ispettorato generale, formulando le proposte circa i provvedimenti da adottare; quando dal ritardo possa derivare pregiudizio, dà egli stesso le disposizioni atte ad eliminare gli inconvenienti.

Nei casi in cui sia stata disposta un'ispezione straordinaria nella quale sia confermato il **permanere delle deficienze o irregolarità precedentemente riscontrate**, il capo dell'ispettorato generale ne informa con rapporto il Ministro per gli eventuali **provvedimenti anche di carattere disciplinare**.

All'Ispettorato sono inoltre demandate le **inchieste amministrative** (art. 12), che possono riguardare sia il personale appartenente all'ordine giudiziario sia qualsiasi altra categoria di personale dipendente dal Ministero della giustizia (ad esclusione del personale dipendente dagli istituti di prevenzione e di pena cui provvede normalmente provvede la relativa direzione generale).

Al termine dell'indagine, il magistrato ispettore incaricato di un'inchiesta nei riguardi di un magistrato deve chiedere informazioni al capo dell'ufficio e chiarimenti all'inquisito, e poi riferire in merito al servizio prestato da quest'ultimo, alle attitudini ed alla capacità da lui dimostrate nell'esercizio delle funzioni giudiziarie, nonché su ogni altro fatto o elemento suscettibile di valutazione in sede disciplinare. Criteri analoghi vengono adottati per le inchieste da eseguire nei confronti di funzionari. Al termine dell'inchiesta il magistrato ispettore redige una dettagliata relazione alla quale allega gli atti e i documenti acquisiti per l'accertamento della responsabilità disciplinare dell'inquisito. Il capo dell'ispettorato generale trasmette al Ministro la relazione d'inchiesta, formulando, se del caso, proposte circa i provvedimenti da adottare.

Legge n. 1311 del 1962	
Testo vigente	**Modificazioni apportate dall'art. 23 dell'A.S. 1143**
Art. 7 *(Verifiche ispettive)*	Art. 7 *(Verifiche ispettive)*
Il capo dell'Ispettorato generale dispone, in conformità delle direttive impartite dal Ministro, le ispezioni in tutti gli uffici giudiziari allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti.	Il capo dell'Ispettorato generale dispone, in conformità delle direttive impartite dal Ministro, le ispezioni in tutti gli uffici giudiziari allo scopo di accertare se i servizi procedono secondo le leggi, i regolamenti e le istruzioni vigenti. **Nelle ispezioni è verificato altresì il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari.**
Le ispezioni di cui al comma precedente hanno luogo, di norma, ogni triennio; il capo dell'ispettorato generale può	*Identico.*

Legge n. 1311 del 1962	
Testo vigente	**Modificazioni apportate dall'art. 23 dell'A.S. 1143**
ordinare che esse siano ripetute entro un termine minore negli uffici ove siano state riscontrate o per i quali vengono segnalate deficienze o irregolarità.	
Il Ministro può in ogni tempo, quando lo ritenga opportuno, disporre ispezioni negli uffici giudiziari. Il Ministro può altresì disporre ispezioni parziali negli uffici giudiziari, al fine di accertare la produttività degli stessi **nonché** l'entità e la tempestività del lavoro di singoli magistrati.	Il Ministro può in ogni tempo, quando lo ritenga opportuno, disporre ispezioni negli uffici giudiziari. Il Ministro può altresì disporre ispezioni parziali negli uffici giudiziari, al fine di accertare la produttività degli stessi, l'entità e la tempestività del lavoro di singoli magistrati **nonché il rispetto delle prescrizioni di sicurezza negli accessi alle banche di dati in uso presso gli uffici giudiziari.**

Articolo 24
(Disposizioni finanziarie)

L'**articolo 24, 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** 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.