ANALISI TECNICO-NORMATIVA (ATN)

(All. "A" alla direttiva P.C.M. del 10 settembre 2008 – G.U. n. 219 del 2008)

Provvedimento: schema di disegno di legge, recante "Disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale".

Amministrazioni proponenti: Presidenza del Consiglio dei Ministri e Ministero della Giustizia.

Referenti ATN: PCM - Agenzia cybersicurezza nazionale – Ufficio legislativo giustizia.

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) *Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.*

La proposta normativa si pone l'obiettivo, in coerenza con il programma di Governo, di prevenire minacce alla sicurezza informatica attraverso modifiche sostanziali e processuali in relazione ai reati informatici attraverso anche il rafforzamento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) e il suo coordinamento con l'Autorità giudiziaria in caso di attacchi informatici, con specifiche procedure volte a rendere più immediato l'intervento dell'Agenzia a fini di prevenzione degli attacchi e delle loro conseguenze e del ripristino rapido delle funzionalità dei sistemi informatici.

Nello specifico, le disposizioni di cui al **Capo I**, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici*", sono finalizzate a conseguire una più elevata capacità di protezione e risposta alle emergenze cibernetiche. L'attuale contesto geo-politico, infatti, caratterizzato in particolare dai gravi conflitti internazionale in atto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale. La proposta normativa risponde alla necessità che si è venuta a profilare sempre di più nell'ultimo periodo di far emergere in modo più puntuale la minaccia informatica diretta ai soggetti della pubblica amministrazione non ricompresi nel Perimetro di sicurezza nazionale cibernetica (di cui al decreto-legge 21 settembre 2019, n. 105), né al momento interessati dalla direttiva NIS, considerato che potrebbero essere interessati dalla direttiva NIS 2, allo stato in fase di recepimento.

Le disposizioni di cui al **Capo II**, recante **"***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*" sono volte, in particolare, a realizzare una più intensa tutela della sicurezza cibernetica e dei beni finali, afferenti alla persona ed al patrimonio, che nell'attuale contesto tecnologico e digitale sono fortemente esposti ad allarmanti forme di criminalità informatica.
A tal fine, si interviene:

- **sul versante sanzionatorio strettamente inteso, e cioè delle comminatorie edittali** (in tale ambito, con particolare riguardo al sistema delle aggravanti, a fronte di un diffuso aggravamento delle pene, si è dato ingresso, alle attenuanti del fatto di lieve entità e delle condotte di collaborazione, funzionali a riequilibrare il sistema punitivo, anche nella prospettiva dell'individualizzazione del trattamento sanzionatorio; è stata introdotta un'autonoma fattispecie di *estorsione informatica*; è stata prevista l'estensione della disciplina prevista per i reati di criminalità organizzata in materia di proroga delle indagini, termine per le indagini preliminari, intercettazioni, collaboratori e testimoni di giustizia);

- **sulla precisazione ed ampliamento delle fattispecie** (in tale ambito, si inserisce l'intervento di ampliamento, dal «profitto» al più generico «vantaggio», del *dolo specifico* previsto per la fattispecie prodromica di detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici);

- **sul sostanziale riordino e riallineamento sistematico delle fattispecie**, soprattutto con riguardo a quelle circostanziali (in tale ambito merita menzione, in particolare, la *reductio ad unum* dei sistemi informatici o telematici di interesse pubblico, come tali meritevoli di protezione rafforzata, ora uniformemente identificabili sulla base della descrizione contenuta nella fattispecie di accesso abusivo).

Sono stati, altresì, innalzati i livelli sanzionatori previsti per gli illeciti dell'ente, dipendenti dal reato informatico, ai sensi del d.lgs. 231 del 2001.

È stato disciplinato il rapporto tra ACN, procuratore nazionale antimafia e pubblico ministero, regolando gli aspetti operativi connessi ai flussi informativi nei casi in cui le notifiche di incidente informatico includano notizie di reati informatici.

Con specifico riferimento alle disposizioni di cui al Capo II la necessità degli interventi normativi proposti deriva:

- dall'esigenza del rafforzamento della tutela preventiva e del contrasto dei reati informatici a tutela della sicurezza cibernetica e dei beni finali, afferenti alla persona

ed al patrimonio, che nell'attuale contesto tecnologico e digitale sono fortemente esposti ad allarmanti forme di criminalità informatica.
- dalla esigenza di coordinamento tra l'ACN, la PNAA, la polizia giudiziaria ed il pubblico ministero degli interventi in caso di attacchi a sistemi informatici o telematici.

2) ***Analisi del quadro normativo nazionale.***

Il quadro normativo ordinamentale nazionale relativo agli interventi posti in essere con le disposizioni contenute nel **Capo I** del disegno di legge è così composto:

- decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Il decreto-legge n. 105 del 2019 contiene disposizioni in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

- decreto legislativo 18 maggio 2018, n. 65.

Il decreto legislativo n. 65 del 2018 reca l'attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

- decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

Il decreto-legge n. 82 del 2021 ha ridefinito l'architettura nazionale in materia di cybersicurezza ed ha istituito l'Agenzia per la cybersicurezza nazionale;

- legge 3 agosto 2007, n. 124.

Con la legge n. 124 del 2007 è stato istituito il sistema di informazione per la sicurezza della Repubblica e riformato il comparto dell'*intelligence* italiana;

- decreto legislativo 1° agosto 2003, n. 259.

Il decreto legislativo n. 259 del 2003, recante il codice delle comunicazioni elettronica, raccoglie la normativa nazionale per il settore dei servizi e del mercato delle telecomunicazioni e delle radiocomunicazioni;

- legge 24 novembre 1981, n. 689.

La legge n. 689 del 1981 reca modifiche al codice penale.

- decreto legislativo 31 marzo 2023, n. 36.

Il decreto legislativo n. 36 del 2023 recante il "Codice dei contratti pubblici", disciplina la materia degli appalti pubblici di lavori, forniture, servizi e concessioni, e dei relativi contratti pubblici.

Il quadro normativo ordinamentale nazionale relativo agli interventi posti in essere con le disposizioni contenute nel **Capo II** del disegno di legge è costituito dai seguenti provvedimenti:

1. Regio Decreto 19 ottobre 1930, n. 1398 "Codice penale";
2. Decreto del Presidente della Repubblica 22 settembre 1988, n. 447 "Codice di procedura penale";
3. Decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82;
4. Decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203;
5. Decreto legislativo 8 giugno 2001, n. 231;
6. Legge 11 gennaio 2018, n. 6;
7. Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

3) ***Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.***

Le disposizioni contenute nel **Capo I** del disegno di legge incidono sulla normativa vigente.

In particolare:

- l'articolo 3 modifica l'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, per finalità di raccordo e coordinamento con le disposizioni recate dal presente disegno di legge;

- l'articolo 4 modifica l'articolo 8 del decreto-legge 14 giugno 2021, n. 82, al fine di prevede una specifica modalità di funzionamento del Nucleo per la cybersicurezza;

- l'articolo 7 modifica l'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, inserendo la lettera m-quater), finalizzata a prevedere la possibilità per l'Agenzia per la cybersicurezza nazionale di promuovere e sviluppare iniziative per la valorizzazione dell'intelligenza artificiale;

- l'articolo 8 modifica l'articolo 17 del decreto-legge 14 giugno 2021, n. 82, prevedendo la possibilità di adottare con DPCM un regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale;

- l'articolo 9 modifica l'articolo 12 del decreto-legge 14 giugno 2021, n. 82, al fine di prevedere un divieto di assunzione, anche di incarichi, per i dipendenti appartenenti al ruolo del personale dell'Agenzia che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione;

Con riferimento alle disposizioni di cui al **Capo II** le quali sono volte alla prevenzione ed al contrasto dei reati informatici, nonché al coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici, introduce significative modifiche nel trattamento sanzionatorio dei reati informatici, con particolare riguardo al sistema delle aggravanti,

inasprendo in numerosi casi le pene ma dando altresì ingresso alle attenuanti del fatto di lieve entità e delle condotte di collaborazione, funzionali a riequilibrare il sistema punitivo nella prospettiva dell'individualizzazione del trattamento sanzionatorio. Si introduce, altresì, una autonoma fattispecie di estorsione informatica, per i casi in cui essa venga realizzata «*mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, ovvero con la minaccia di compierle*». La proposta prevede anche l'estensione della disciplina prevista per i reati di criminalità organizzata in materia di proroga delle indagini, termine per le indagini preliminari, intercettazioni, collaboratori e testimoni di giustizia. Viene, infine, disciplinato il rapporto tra ACN, procuratore nazionale antimafia e pubblico ministero, regolando gli aspetti operativi connessi ai flussi informativi nei casi in cui le notifiche di incidente informatico includano notizie di reati informatici.

La proposta normativa incide sulle disposizioni indicate *sub* 2 inerenti al Capo II.

In particolare:

A) L'articolo 11 dello schema di disegno di legge contiene le modifiche che vengono apportate al codice penale.

In particolare, con le lettere da *a)* a *r)* si apportano modifiche alle seguenti disposizioni:

- ***lettera a)*: all'articolo 615-*ter*** l'intervento modifica la disciplina del reato di «*Accesso abusivo ad un sistema informatico o telematico*». **Al numero 1)** si prevedono modifiche **al comma secondo** dell'articolo: il punto 1.1 aumenta la pena edittale per le ipotesi aggravate del reato, precedentemente fissata nella reclusione da uno a cinque anni, ora fissata «*da due a dieci anni*»; **il punto 1.2 modifica il numero 2)** introducendo all'ipotesi aggravata di esecuzione del reato l'uso di minaccia oltre che con violenza sulle cose o alle persone; **il punto 1.3** qualifica come aggravata la condotta di chi sottrae, anche mediante riproduzione o trasmissione, ovvero renda inaccessibili al titolare, i dati, le informazioni o i programmi contenuti nel sistema informatico o telematico.

  Il numero 2) apporta modifiche al **comma terzo** dell'articolo 615-ter c.p., riguardante i casi in cui i fatti di cui ai precedenti 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. **Al punto 2.1** è aumentata la pena edittale per tali fattispecie aggravate, precedentemente fissata nella reclusione «da uno a cinque anni e da tre a otto anni», alla reclusione «da tre a dieci anni e da quattro a dodici anni». **Al punto 2.2** è aggiunto un periodo **al comma terzo**, nel quale si prevede che nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89 («Vizio parziale di mente»), 98 («Minore degli anni diciotto») e 623-quater (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o

prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti;

- ***lettera b):*** **all'articolo 615-quater** recante «*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*», **il numero 1)** amplia (dal «profitto» al più generico «vantaggio») il dolo specifico previsto per la configurabilità della fattispecie. **Il numero 2)** sostituisce **il secondo comma**, prevedendo l'ipotesi aggravata punita con la pena della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui al precedente articolo 615-ter, secondo comma, numero 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). **Il numero 3)** inserisce un ulteriore comma all'articolo, introducendo un'ulteriore ipotesi aggravata punita con la pena 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 (di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- ***lettera c):*** **all'articolo 615-quinquies** con intervento abrogativo. È soppresso l'articolo che disciplinava le ipotesi di «*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*», in ottica di riordino e riallineamento sistematico delle fattispecie;
- ***lettera d)*****: all'articolo 617-bis** si aggiunge un ulteriore comma recante «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche*», che introduce l'ipotesi aggravata quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 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), punita con la reclusione da due a sei anni;
- ***lettera e):*** **all'articolo 617-quater** che disciplina il reato di «*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*». Con **il numero 1)** si modifica **il quarto comma**, che disciplina le fattispecie aggravate per cui è prevista la procedibilità d'ufficio prevedendo: l'aumento della pena edittale dalla reclusione da tre a otto anni alla reclusione da quattro a dieci anni; la procedibilità d'ufficio, quando il fatto è commesso in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma, primo periodo (di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico); l'ipotesi aggravata quando il fatto è commesso 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, contestualmente sopprimendo la disposizione specifica di cui al numero 3). **Il numero 2)** aggiunge un ulteriore comma all'articolo 617-quater, relativo al bilanciamento delle circostanze, nel quale si prevede che le circostanze attenuanti diverse da quelle di cui agli articoli 89 («Vizio parziale di mente»), 98 («Minore degli anni diciotto») e 623-quater (introdotto dal presente provvedimento, di seguito esaminato) concorrenti con l'aggravante di cui al quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alla predetta aggravante.

- ***lettera f)****:* **all'articolo 617-quinquies** recante «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*» **al numero 1)** si modifica l'ipotesi aggravata, prevedendo che quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), precedentemente esaminato, la pena è della reclusione da due a sei anni. **Al numero 2)** vengono inseriti ulteriori commi all'articolo, relativi all'ipotesi aggravata quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1) precedentemente modificato, punita con la reclusione da tre a otto anni, nonché al bilanciamento delle circostanze;
- ***lettera g):*** **all'articolo 617-sexies** recante la fattispecie di reato «*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*». Si prevede, nell'ipotesi aggravata di cui al comma secondo, l'aumento della pena edittale della reclusione da uno a cinque anni alla reclusione da tre a otto anni, nonché si introducono norme relative al bilanciamento delle circostanze in sede di calcolo della pena;
- ***lettera h):*** **alla rubrica del Capo III-bis del Titolo XII**, precedentemente rubricato «Disposizioni comuni sulla procedibilità», si apportano modifiche eliminando il riferimento alla procedibilità in considerazione delle modifiche di cui alla successiva lettera i);
- ***lettera i):*** si introduce **l'articolo 623-quater** rubricato "*Circostanza attenuante*". Si prevede, in particolare, che le pene previste per i delitti di cui agli articoli 615-ter, 615-quater, 617-quater, 617-quinquies e 617-sexies 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, escludendo l'operatività del divieto di bilanciamento.
- ***lettera l):*** **all'articolo 629,** recante la fattispecie del reato di estorsione, è aggiunto un ulteriore comma che commina la pena della reclusione da sei a dodici anni e della

multa da euro 5.000 a euro 10.000 *per il fatto di chi,* «*mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno*». La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo 628;

- ***lettera m):*** **all'articolo 635-bis,** recante la disciplina del reato di «Danneggiamento di informazioni, dati e programmi informatici», sono apportate modifiche, prevedendo: l'aumento della pena edittale della reclusione da sei mesi a tre anni alla reclusione da due a sei anni. Con le modifiche al secondo comma dell'articolo si introducono disposizioni relative alle fattispecie aggravate. Si prevede che la pena è della reclusione da tre a otto anni 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 o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato;
- ***lettera n):*** si apportano modifiche **all'articolo 635-ter** relativo a «*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*», prevedendo che nella rubrica, le parole: «*utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*» siano sostituite dalle più generiche: «*pubblici o di interesse pubblico*», aumentando la pena edittale della reclusione da uno a quattro anni alla reclusione da due a sei anni e prevedendo, mediante la sostituzione integrale dei commi secondo e terzo, ulteriori ipotesi aggravate. In particolare, la pena è della reclusione da tre a otto anni 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; o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato; o ancora, se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici. La pena è della reclusione da quattro a dodici anni in ipotesi di concorrenza delle circostanze aggravanti di cui al precedente comma; in tal caso le circostanze attenuanti diverse da quelle di cui agli articoli 89 («Vizio parziale di mente»), 98 («Minore degli anni diciotto») e 639-ter (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti. Infine, viene modificata la rubrica che prende la seguente denominazione "Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico";

- ***lettera o)*: all'articolo 635-quater** recante la disciplina della fattispecie di reato «*Danneggiamento di sistemi informatici o telematici*» si interviene aumentando la pena edittale della reclusione da uno a cinque anni, alla reclusione da due a sei anni e si prevedono**,** mediante la sostituzione integrale del comma secondo, ulteriori ipotesi aggravate. In particolare, si prevede che la pena è della reclusione da tre a otto anni 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, o se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato;
- ***lettera p):* si inserisce l'articolo 635-quater.1**, recante «*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*». Si prevede che chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329. 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) (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). 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 (di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico);
- ***lettera q)*: sostituisce integralmente l'articolo 635-quinquies** e reca la seguente rubrica «*Danneggiamento di sistemi informatici o telematici di pubblico interesse*». Si prevede che salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis (Danneggiamento di informazioni, dati e programmi informatici), ovvero attraverso 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, è punito con la pena della reclusione da due a sei anni. La pena è della reclusione da tre a otto anni 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; se il colpevole per commettere il fatto usa minaccia o violenza, ovvero se è palesemente armato; 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 quattro a dodici anni in ipotesi di concorrenza delle circostanze aggravanti di cui al precedente comma; in tal caso le circostanze attenuanti diverse da quelle di cui agli articoli 89 («Vizio parziale di mente»), 98 («Minore degli anni diciotto») e 639-ter (introdotto dal presente provvedimento, di seguito esaminato) non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti;

- ***lettera r)***: **si inserisce l'articolo 635-sexies**, rubricato "*Circostanza attenuante*" che prevede che le pene per i delitti di cui agli articoli 629, terzo comma, 635-ter, 635-quater.1 e 635-quinquies 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, escludendo l'operatività del divieto di bilanciamento.

B) L'articolo 12 dello schema di disegno di legge contiene le modifiche che vengono apportate al codice di procedura penale.

In particolare, con le lettere da *a)* a *c)* si apportano modifiche alle seguenti disposizioni:

- ***lettera a):*** all'articolo 51, comma 3-*quinquies* del codice di procedura penale **si sostituisce il riferimento all'art. 615-*quinquies*** del codice penale con quello all'articolo 635-*quater.1*, fattispecie di nuovo conio che ricalca la norma sostanziale abrogata; si inserisce inoltre anche il riferimento al nuovo articolo 635-*quinquies,*. Inoltre, viene elencato, di seguito a questi, il reato 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 cui è estesa la competenza procedurale per identità di materia, trattandosi di sanzionare condotte omissive o elusive, che ostacolano l'emersione di tali reati commessi attraverso strumenti informatici.

- ***lettere b)* e *c):* sono integrati gli articoli 406 e 407 c.p.p.** Nel dettaglio, **all'articolo 406**, comma 5-*bis*, dopo le parole: «*7-bis*» sono inserite le parole: «*e 7-ter*»; **all'art. 407** comma 2, dopo il numero 7-*bis* è aggiunto il seguente: «*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 alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.*» Si estende ai reati in esame, nei casi sopra indicati, eccezione alle disposizioni che prevedono la comunicazione della richiesta del p.m. di proroga dei termini intermedi delle indagini preliminari e

l'instaurazione del contraddittorio sul punto, e si prevede che il termine massimo delle indagini sia di due anni anziché di diciotto mesi.

C) L'articolo 13 dello schema di disegno di legge contiene le modifiche che vengono apportate al decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82.

In particolare, comma 1:

- alla lettera a) modifica l'articolo 9 comma 2, del decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, consentendo l'adozione, per gli autori dei reati informatici previsti al comma 4-*bis* dell'articolo 371-*bis*, delle **speciali misure di protezione riservate ai soggetti che abbiano collaborato** nell'ambito di un procedimento penale;
- alla lettera b) modifica l'articolo 11, comma 2 dello stesso decreto-legge, prevedendo che per i reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, sia effettuata la comunicazione della **proposta di ammissione** alle speciali misure di protezione al procuratore nazionale antimafia e antiterrorismo, ampliando altresì la cognizione di quest'ultimo sui contrasti nel caso di più uffici del pubblico ministero che procedono a indagini collegate;
- alla lettera c) modifica l'articolo 16-*novies*, comma 1, del medesimo decreto-legge, estendendo alle persone condannate per i reati informatici attribuiti dall'articolo 371-*bis*, comma 4-*bis* al coordinamento del procuratore nazionale antimafia e antiterrorismo, la disciplina speciale dei **benefici penitenziari** riservati dalla legge ai soggetti che collaborano con la giustizia.

D) L'articolo 14 dello schema di disegno di legge contiene le modifiche che vengono apportate al decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203.

In particolare, con il comma 1 si apportano modifiche alle seguenti disposizioni:

Si modifica l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, inserendo il nuovo comma 3-*bis* con il quale si prevede che le disposizioni di cui ai commi 1, 2 e 3 del citato decreto relative alla disciplina delle intercettazioni di conversazioni e comunicazioni si applicano anche quando si procede con riferimento ai delitti, consumati o tentati, previsti dall'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale. La finalità è quella di estendere ai crimini informatici che mettono in serio pericolo la sicurezza dei sistemi di interesse pubblico la disciplina delle intercettazioni e comunicazioni telefoniche prevista in materia di criminalità organizzata.

E) L'articolo 15 dello schema di disegno di legge contiene le modifiche che vengono apportate al decreto legislativo 8 giugno 2001, n. 231.

In particolare, con le lettere da *c)* a *c)* si apportano modifiche alle seguenti disposizioni:

- ***lettere a), b) e c)***: si apportano **modifiche all'articolo 24-*bis*** del decreto legislativo 8 giugno 2001, n. 231 in materia di delitti informatici e trattamento illecito dati.
  Nel dettaglio la modifica **al comma 1** inasprisce la sanzione pecuniaria applicata all'ente che commette i delitti di cui agli articoli 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, sostituendo le parole "*da cento a cinquecento quote*" con le parole "*da duecento a settecento quote*".
  Sempre in tale ottica di repressione di condotte lesive dell'interesse pubblico, **si introduce il nuovo comma 1-*bis*** che prevede di applicare all'ente la sanzione pecuniaria da trecento a ottocento quote nel caso di commissione del nuovo delitto di cui all'articolo 629, terzo comma, del Codice penale.
  Con la modifica **al comma 2** del citato articolo 24-*bis*, viene sostituito il riferimento all'articolo 615-*quinquies* c.p. con quello all'articolo 635.*quater.1* c.p. e la sanzione pecuniaria viene elevata da trecento a quattrocento quote.
  Infine, con l'intervento **sul comma 4** del citato articolo, dopo il primo periodo s'inserisce un ulteriore periodo col quale si prevede che nei casi di condanna per il delitto indicato nel comma 1-*bis* si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 del D.lgs. 231/2000 per una durata non inferiore a due anni.

F) L'articolo 16 dello schema di disegno di legge contiene le modifiche che vengono apportate alla legge 11 gennaio 2018, n. 6. In particolare, si apportano modifiche alle seguenti disposizioni:

articolo 11 comma 2, relativo al procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, al fine di prevedere che la Commissione centrale richieda il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, non solo per le fattispecie delittuose di cui all'articolo 51, commi 3-*bis*, 3-*ter* e 3-*quater*, del codice di procedura penale, ma anche nel caso di delitti *di cui all'articolo 371-bis, comma 4-bis* del codice di procedura penale. Viene in tal modo estesa la disciplina dei testimoni di giustizia anche ai reati informatici di cui alla norma citata.

G) L'articolo 17 dello schema di disegno di legge contiene le modifiche che vengono apportate al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

In particolare, con le *lettere a) e b)* si apportano modifiche alle seguenti disposizioni:

- **lettera a): all'articolo 17, dopo il comma 4**, si inseriscono quattro nuovi commi **(4-bis.1; 4-bis.2; 4-bis.3 e 4-bis.4)**, al fine di meglio regolare i rapporti fra le diverse autorità coinvolte (Agenzia Cybersicurezza, procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria e il pubblico ministero).

Il comma 4 viene completamente sostituito, ribadendo che il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale e prevedendo che la trasmissione delle notifiche di incidente, ricevute dal 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 144/2005, deve essere immediata, in quanto costituisce adempimento dell'obbligo previsto dall'articolo 331 del codice di procedura penale in materia di denuncia da parte dei pubblici ufficiali e incaricati di pubblico servizio.

Con il nuovo comma 4-*bis*.1 introducono reciproci obblighi informativi tra l'ACN e l'autorità giudiziaria e si prevede che nei casi in cui l'Agenzia abbia notizia di un attacco ai danni di uno dei sistemi informatici o telematici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale e comunque in tutti quei casi in cui risulti coinvolto uno dei soggetti individuati **dall'articolo 1, comma 2-*bis*, del decreto-legge n. 105/2019** (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 o dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale), **dall'articolo 3, comma 1, lettere g) ed i) del D.lgs. 65/2018** (operatore di servizi essenziali, soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2 del citato decreto legislativo e fornitore di servizio digitale), **dall'articolo 40, comma 3 alinea, del decreto legislativo 1° agosto 2003, n. 259** (imprese reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico), *fermo restando quanto previsto dal comma 4*, procede alle attività di cui all'articolo 7, comma 1, lettere n) e n-bis) (che sono indispensabili per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, nonché il ripristino dell'operatività dei sistemi compromessi) e ne informa senza ritardo il procuratore nazionale antimafia e antiterrorismo, ai sensi del comma 4-bis.

Con il successivo **comma 4-*bis*.2** si prevede che fuori dai casi previsti dal precedente comma, il pubblico ministro sia tenuto ad informare tempestivamente l'Agenzia della cybersicurezza quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

Il comma 4-*bis*.3 prevede che il pubblico ministero, nell'impartire le disposizioni necessarie ad assicurare gli accertamenti urgenti, tenga conto delle attività di analisi e prevenzione svolte dall'Agenzia della Cybersicurezza, potendo con decreto motivato altresì differire una o più delle predette attività se ritiene che le stesse possano creare un pregiudizio al corso delle indagini. Si prevede, inoltre, che il pubblico ministero assicuri il necessario collegamento informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, al fine di assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto

del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate (articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155).

Infine, **con il comma 4-*bis*.4** viene previsto, in caso di accertamenti irripetibili, la facoltà per l'Agenzia della cybersicurezza di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio.

4) Analisi della compatibilità dell'intervento con i principi costituzionali.

Non si rilevano profili di incompatibilità con i principi costituzionali, con la giurisprudenza della Corte costituzionale, né con altre disposizioni vigenti. Le disposizioni proposte, inoltre, sono coerenti con i principi costituzionali che disciplinano l'efficienza e la legittimità dell'azione della pubblica amministrazione.

5) Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Le disposizioni proposte con il **Capo I** del presente disegno di legge rientrano tra le materie riservate in via esclusiva allo Stato e, in particolare, tra quelle indicate dall'articolo 117, secondo comma, lettera d), della Costituzione. Non si ravvisano, pertanto, profili di incompatibilità con le competenze e le funzioni delle regioni ordinarie e a statuto speciale, nonché degli enti locali. Tuttavia, in considerazione della incidenza di talune disposizioni previste dal provvedimento - in particolare, gli articoli 1, 2, 6 e 10 - sulle attività delle pubbliche amministrazioni anche locali, sarà necessario un confronto ed un raccordo operativo con i richiamati soggetti in relazione all'attuazione di tali disposizioni.

Le disposizioni di cui al **Capo II** non presentano aspetti di interferenza o di incompatibilità con le competenze costituzionali delle regioni, ordinarie e a statuto speciale nonché degli enti locali, incidendo su materia riservata alla competenza legislativa dello Stato (ai sensi dell'articolo 117, comma 2, lett. g) ed l) della Costituzione).

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Le disposizioni contenute nell'intervento esaminato sono compatibili e rispettano i principi di cui all'articolo 118 della Costituzione, in quanto non prevedono né determinano, sia pure in via indiretta, nuovi o più onerosi adempimenti a carico degli enti locali.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

L'intervento normativo attiene a materia regolata da disposizioni di rango primario e, come tale, non pone prospettive di delegificazione od ulteriori possibilità di semplificazione normativa.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Non risultano pendenti in Parlamento iniziative normative in materia analoga a quella trattata nelle proposte analizzate.

9) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Le disposizioni contenute nel provvedimento non contrastano con i principi fissati in materia dalla giurisprudenza anche costituzionale e su di esse non pendono giudizi di costituzionalità.

PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

10) Analisi della compatibilità dell'intervento con l'ordinamento comunitario.

Le disposizioni contenute nel **Capo I** del provvedimento sono compatibili con la normativa europea in materia di cybersicurezza, con particolare riferimento alla direttiva NIS 2.

A livello europeo, numerose sono le iniziative miranti a rafforzare la resilienza, non solo per far fronte dell'aumento delle minacce informatiche, ma anche in considerazione del fatto che la cybersicurezza è un fattore imprescindibile per costruire una Unione europea in grado di garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili.

Tra le varie iniziative normative, di particolare rilevanza per i fini del presente disegno di legge, vi è quella relativa all'adozione della richiamata direttiva (UE) 2022/2555, c.d. direttiva NIS2, che, superando e abrogando la precedente direttiva NIS, ha l'obiettivo di garantire un livello comune elevato di cybersicurezza nell'Unione, al fine di rispondere alle crescenti minacce poste dalla digitalizzazione e rafforzare la sicurezza dei soggetti coinvolti nel processo. In tal senso, la direttiva NIS 2 prevede un ampliamento dell'ambito di applicazione, che obbliga più entità e settori ad adottare misure di sicurezza, includendo, per quanto riguarda il settore pubblico, anche le pubbliche amministrazioni. Le disposizioni del **Capo I** del presente disegno di legge, dunque, rispondono alla necessità di aumentare la resilienza dei soggetti della pubblica amministrazione non ricompresi nell'ambito di

applicazione del decreto-legge 21 settembre 2019, n. 105, né al momento interessati dalla direttiva NIS, tenuto conto del fatto che potrebbero essere interessati dalla direttiva NIS 2.

Le disposizioni di cui al **Capo II** non presentano aspetti di interferenza o di incompatibilità con l'ordinamento europeo.

11) Verifica dell'esistenza di procedure di infrazione da parte della Commissione Europea sul medesimo o analogo oggetto.

Non risultano procedure di infrazione da parte della Commissione Europea sul medesimo o analogo oggetto.

12) Analisi della compatibilità dell'intervento con gli obblighi internazionali.

L'intervento è pienamente compatibile con gli obblighi internazionali.

13) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non risultano pendenti giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

14) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.

Non risultano pendenti giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.

15) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione Europea.

Relativamente alle disposizioni contenute nel **Capo I** del disegno di legge non sussistono indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Si richiama che, ai sensi dell'articolo 4, paragrafo 2, del Trattato sull'Unione europea, l'Unione rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale, e la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Inoltre, l'articolo 346, paragrafo 1, lettera a), del Trattato sul funzionamento dell'Unione europea stabilisce che nessuno Stato membro è tenuto a fornire informazioni la cui

divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza.

Per le disposizioni di cui al **Capo II** non vi sono indicazioni da fornire attesa la settorialità e la limitatezza dell'intervento.

PARTE III. ELEMENTI DI QUALITA' SISTEMATICA E REDAZIONALE DEL TESTO

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

Non vengono utilizzate definizioni normative che non appartengano già al linguaggio tecnico giuridico della materia regolata.

2) Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni ed integrazioni subite dai medesimi.

È stata verificata positivamente la correttezza dei riferimenti normativi contenuti negli articoli del provvedimento.

3) Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.

Il presente intervento legislativo fa ricorso alla tecnica della novella legislativa per introdurre modificazioni, integrazioni ed abrogazioni a disposizioni vigenti come sono state riportate *sub 3)* della parte I.

4) Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.

L'intervento normativo non comporta effetti abrogativi impliciti.

5) Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

Non sussistono disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica.

Quanto alla sussistenza di disposizioni derogatorie rispetto alla normativa vigente, si evidenzia che il regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale, previsto dall'articolo 8 del disegno di legge, può essere adottato anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400.

6) Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.

Non sussistono deleghe aperte sul medesimo oggetto delle disposizioni contenute nel presente disegno di legge, né di carattere integrativo né di carattere correttivo.

7) Indicazione degli eventuali atti successivi attuativi; verifica della congruenza dei termini previsti per la loro adozione.

In attuazione delle misure contenute nel **Capo I** del disegno di legge sono previsti i seguenti atti attuativi:

- determina del direttore generale dell'Agenzia per la cybersicurezza nazionale, per la disciplina delle modalità di ispezioni che l'Agenzia stessa potrà effettuare nel caso di inosservanza degli obblighi previsti dall'articolo 1 (articolo 1, comma 4);
- decreto del Presidente del Consiglio dei ministri per l'adozione del regolamento recante la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia della cybersicurezza nazionale (articolo 8);
- determina del direttore generale dell'Agenzia per la cybersicurezza nazionale per l'individuazione dei percorsi formativi di specializzazione la cui frequenza dà luogo ad un divieto per i dipendenti appartenenti al ruolo del personale dell'Agenzia medesima di assunzione, o assunzione di incarichi, presso soggetti privati al fine di svolgere mansioni in materia di cybersicurezza (articolo 9);
- decreto del Presidente del Consiglio dei ministri per l'individuazione degli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, devono tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici (articolo 10, comma 1).

Con riferimento alle disposizioni di cui al **Capo II** non sono previsti atti successivi attuativi.

8) Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.

Per la predisposizione del provvedimento in esame sono stati utilizzati i dati informativi già in possesso delle Amministrazioni proponenti e non è stato necessario commissionare l'acquisizione di ulteriori dati statistici o informativi all'Istituto nazionale di statistica.