GRUPPO PD
Italia democratica e progressista
Camera dei deputati

Ufficio Documentazione e Studi

Dossier n. 104

15 maggio 2024

CYBERSICUREZZA NAZIONALE E REATI INFORMATICI

*Il disegno di legge in esame reca disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché norme relative ai contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici. Si tratta di d**isposizioni finalizzate a conseguire una più elevata capacità di protezione e risposta a fronte di emergenze cibernetiche**, in forte incremento anche a seguito dei gravi conflitti internazionali in atto. L'obiettivo è quello del raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché di rispondere alla necessità di far emergere in modo più puntuale la minaccia informatica diretta ai soggetti della pubblica amministrazione non compresi nel Perimetro di sicurezza nazionale cibernetica. Le disposizioni contenute nel capo I, del provvedimento, modificato durante l'esame parlamentare, individuano, dunque, come si legge nella relazione del Governo, le norme "necessarie per sviluppare capacità nazionali **di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici***

*Il Capo II reca, invece, **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**.*

***L'istruttoria in commissione**, a parere del **Gruppo PD-IDP**, si è rivelata **sommaria e frettolosa**, risultando **ristretta agli scarni tempi residuati** dall'esame del disegno di legge sull'autonomia. Durante l'esame nelle commissioni I e II sono stati presentati all'incirca una cinquantina di emendamenti, alcuni dei quali sono stati recepiti dal Governo nel testo arrivato all'esame dell'Aula.*

***Tra le questioni più rilevanti** rimaste aperte vi è senz'altro **quella delle risorse economiche**: il provvedimento in esame, ancora una volta, **viene approvato ad invarianza finanziaria,** e formalmente il Governo ha giustificato questa scelta sulla base della considerazione che i soldi di cui necessiterebbe il provvedimento per essere realmente attuato sarebbero stati stanziati nel PNRR, dove sarebbero previsti 50 milioni di euro. Tuttavia, non tutti i soggetti contemplati dal provvedimento in esame avranno titolo accedere ai soldi stanziati nel PNRR. E molte delle disposizioni previste, alla cui inosservanza sono collegate sanzioni, potrebbero rivelarsi molto onerose.*

*Come ha ricordato **Andrea Casu (PD-IDP)**, durante la discussione generale in Aula, ci sono "una serie di **nuovi impegni e di nuovi oneri** non solo **per le amministrazioni centrali** ma anche **per le regioni, per le città metropolitane, per le province, per i comuni**", per le **società di trasporto pubblico, le aziende sanitarie locali** e **le altre società in house** che, ad esempio, forniscono servizi informatici o di gestione dei rifiuti.*

*“**Non si può dire**, nello stesso momento, – ha sottolienato **Andrea Casu (PD-IDP)** – che **la cybersicurezza è un’emergenza nazionale**, che la cybersicurezza richiede più interventi, più oneri, più impegni da parte di tutti i livelli istituzionali **e poi prevedere che tutto questo aumento di oneri, di impegni, valga zero.** Perché significa che **si dà alla cybersicurezza valore zero euro**”.*

*Da segnalare, l’avvenuta approvazione, in commissione, col parere favorevole del Governo, di un emendamento del deputato Costa (**ora articolo 22 del provvedimento in esame**) il quale prevede che - in occasione delle ispezioni presso gli uffici giudiziari - gli ispettori del Ministero della Giustizia vengano utilizzati “per verificare” il rispetto delle prescrizioni di sicurezza negli accessi alle banche dati in uso.*

*“Si consente, dunque, – ha sottolineato criticamente **Federico Gianassi (PD-IDP)** – a **un organo amministrativo alle dipendenze dell'organo politico** di esercitare un potere estremamente delicato” su **materie che riguardano la segretezza delle indagini delle procure**.*

*Il **Partito Democratico** ha presentato diversi emendamenti mirati soprattutto ad **assicurare le necessarie risorse finanziarie**, tra questi si segnala anche una proposta di **Andrea Casu (PD-IDP)** che prevede l’utilizzo di alcuni sistemi di **difesa dagli cyber attacchi** “anche attraverso la **possibilità di fermare il soggetto offendente**”. Emendamenti purtroppo respinti.*

*Il **giudizio del Partito Democratico** – come ha affermato **Matteo Mauri (PD-IDP)** nella dichiarazione di voto - **“è molto negativo** rispetto a come si sono evoluti i lavori e la discussione in questo iter prima di Commissione e poi parlamentare”.*

*“È sempre **la stessa vecchia storia, la propaganda**, perché ci sono elezioni, ma di più, perché c’è il G7 in Italia, e di conseguenza uno degli argomenti sulla bocca di tutti sarà quello della cybersicurezza, per cui **bisogna alzare l’allarme**, anche pubblicamente … cioè poter dire che l’Italia ha fatto una grande cosa, **il Governo Meloni**, per la prima volta, **ha messo mano al tema della cybersicurezza**. Ma **non è vero niente**”.*

*“Non è che, **in questi ultimi 10 anni**, siamo stati tutti qui a fare altro – ha ricordato **Matteo Mauri (PD-IDP)** - perché dal 2013 in poi si sono susseguiti, tra l’altro per iniziativa di Governi di cui non so se facesse parte l'attuale Presidente del Consiglio, cioè il Governo Monti, nel 2013, Strategia nazionale di cybersicurezza, il Governo Gentiloni, DL cybersecurity 2017, nel 2018 il recepimento della normativa europea, della direttiva NIS 1, nel 2019, Governo “Conte 2”, Perimetro di sicurezza nazionale cibernetica, Governo Draghi, nel 2021, istituzione dell'Agenzia nazionale di cybersicurezza. **Sono tutte cose che abbiamo fatto**”.*

*“Non accettiamo e **non siamo disponibili ad accettare la logica per cui il MEF non può**, i soldi non ci sono, la Ragioneria aveva un’influenza e **non potevano darci i soldi**”.*

*Il **Partito Democratico**, alla fine, per senso di responsabilità, considerata la rilevanza del tema ha deciso comunque di **astenersi sul voto finale.***

Per maggiori approfondimenti si rinvia ai lavori parlamentari del disegno di legge del Governo "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" *AC 1717 e ai relativi dossier dei Servizi Studi della Camera e del Senato.*

Assegnato alle Commissioni riunite I Affari Costituzionali e II Giustizia.

Articolo 1 - Obblighi di notifica di incidenti

L'**articolo 1,** modificato in sede referente, **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 (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).

Articolo 2 - Mancato o ritardato adeguamento a segnalazioni dell'ACN

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** (ACN) circa **specifiche vulnerabilità** cui essi risultano **potenzialmente esposti**, debbano provvedere tempestivamente, e comunque non oltre 15 giorni dalla comunicazione, all'adozione degli **interventi risolutivi** indicati dalla stessa Agenzia.

Articolo 3 - Norme di raccordo con il 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 del 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.

Articolo 4 - Disposizioni in materia dati relativi a incidenti informativi

L'**articolo 4**, introdotto **in sede referente**, 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, i compiti dell'Agenzia** per la Cybersicurezza nazionale descritti dall'articolo 7, comma 1, del decreto-legge n. 82 del 2021.

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** (art. 8 del decreto-legge 14 giugno 2021, n. 82) 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.

Articolo 6 - Disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'ACN

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** (ACN) nei casi in cui questo sia considerato strettamente necessario dai servizi di sicurezza della Repubblica.

Articolo 7 - Composizione del CISR

L'**articolo 7,** introdotto nel corso dell'esame in sede referente, **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

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

L'**articolo 8,** modificato in Aula, **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.

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

L'**articolo 9,** introdotto in sede referente**,** 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**.

Art. 10 - Funzioni ACN in materia di crittografia

L'**articolo 10,** interamente sostituito nel corso dell'esame in sede referente e ulteriormente modificato in Aula**,** valorizza l'utilizzo della **crittografia,** anche attraverso la **tecnologia *blockchain,*** quale strumento di difesa cibernetica e istituisce il **Centro nazionale di crittografia** presso l'Agenzia per la cybersicurezza nazionale (ACN), nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e **senza nuovi o maggiori oneri a carico della finanza pubblica.**

Articolo 11 - Procedimento sanzionatorio per le violazioni in materia di cybersicurezza

L'**articolo 11,** modificato in sede referente, 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** (ACN). 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).

Articolo 12 - Disposizioni in materia di personale dell'ACN

L'**articolo 12**, modificato in Aula, 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.

Fino al 31 dicembre 2026, per il personale dell'Agenzia per la cybersicurezza nazionale il **requisito di permanenza minima nell'Area operativa** ai fini del passaggio all'Area manageriale e alte professionalità **è fissato in tre anni**.

Art.12-*bis*. - Disposizioni in materia di personale degli Organismi di informazione per la sicurezza

Con questa norma, aggiunta **durante l'esame in Aula**, coloro che hanno ricoperto la carica di **Direttore generale e di Vice Direttore generale del DIS e di Direttore e di Vice Direttore di AISE o di AISI**, ovvero abbiano svolto **incarichi dirigenziali di prima fascia** di preposizione a strutture organizzative di livello dirigenziale generale **non possono**, salvo autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità Delegata ove istituita, **nei tre anni successivi** alla cessazione dell'incarico **svolgere attività lavorativa, professionale, o consulenziale, ovvero ricoprire cariche presso soggetti esteri, pubblici o privati**, ovvero presso soggetti privati italiani a cui si applica il decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56. L'autorizzazione è concessa avuto riguardo alle esigenze di protezione e di tutela del patrimonio informativo acquisito durante l'espletamento dell'incarico, e alla **necessità di evitare comunque pregiudizi per la sicurezza nazionale**.

Il personale di cui al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, **non può**, **nei tre anni successivi alla cessazione dal servizio** presso il DIS, l'AISE e

l'AISI, svolgere attività lavorativa, professionale o consulenziale, ovvero ricoprire cariche, presso enti o privati titolari di licenza ai sensi dell'articolo 134 del TULPS, o comunque **presso soggetti che a qualunque titolo svolgano attività di investigazione, ricerca o raccolta informativa.**

Il personale di cui al ruolo unico previsto dall'articolo 21 della legge 3 agosto 2007, n. 124, che **abbia partecipato**, nell'interesse e a spese del DIS, dell'AISE o dell'AISI, **a specifici percorsi formativi di specializzazione**, **non può essere assunto**, né assumere incarichi presso soggetti privati per svolgere le medesime mansioni per le quali ha beneficiato delle suddette attività formative**, per la durata di tre anni** a decorrere dalla data di completamento dell'ultimo dei predetti percorsi formativi.

I contratti conclusi e gli incarichi conferiti in violazione dei divieti di cui al presente articolo **sono nulli.**

Con un regolamento adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono definiti le procedure di autorizzazione o i casi in cui non si applicano i divieti sopra richiamati.

Articolo 13 - Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici

L'**articolo 13,** modificato in Aula**,** 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.

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 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.

Articolo 14 - Resilienza operativa digitale per il settore finanziario

L'**articolo 14** 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**.

Articolo 15 - Modifiche al codice penale

L'**articolo 15,** modificato nel corso dell'esame in Aula, reca modifiche al codice penale in materia di **prevenzione e contrasto dei reati informatici**.

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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. 15, 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 previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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. 15, 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 previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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. 15, 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. 15, 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 previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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. 15, 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. 15, 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, primo periodo.
	[Art. 15, 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	***Abrogato***

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
punito con la reclusione fino a due anni 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. 15, 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. 15, 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*

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	[Art. 15, co. 1, lett. f), n.1]
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, primo periodo;** 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. 15, 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. 15, co. 1, lett. g), n.2]

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	Quando ricorre taluna delle circostanze di cui all'articolo 617- *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. 15, 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. 15, co. 1, lett. i)]
Capo III-*bis* *(Disposizioni comuni **sulla procedibilità**)*	Capo III-*bis* ***(Disposizioni comuni)***
	[Art. 15, co. 1, lett. l)]
	Art. 623-*quater* ***(Circostanze attenuanti)***
	Le pene comminate per i delitti di cui

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	agli articoli 615-*ter*, 615-*quater*, 617-*quater*, 617-*quinquies* e 617-*sexies* sono diminuite quando, per la natura, la specie, i mezzi, le modalità o circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità. **Le pene previste per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel 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)*
Comma 1 *Omissis*	Comma 1 *Omissis*
	[Art. 15, co. 1, lett. m)]
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, nonché nel caso in cui il fatto sia commesso nei confronti di incapaci per età o per infermità.** **Chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies*, ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628**.

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
Art. 635-*bis* *(Danneggiamento di informazioni, dati e programmi informatici)*	Art. 635-*bis* *(idem)*
	[Art. 15, 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 è palesemente armato.**
	[Art. 15, 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. 15, 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	Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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.**	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. 15, 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, 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)*

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	[Art. 15, 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. 15, 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 è palesemente armato.**
	[Art. 15, 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

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	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. 15, co. 1, lett. r)]
Se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.	**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, 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.**

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
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. 15, co. 1, lett. s)]
	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

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	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. 15, 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 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)**.**	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 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**

Codice penale	
Testo previgente	**Modificazioni apportate dall'art. 15 A.C. 1717-A**
	attraverso strumenti informatici o telematici idonei ad ostacolare la propria o altrui identificazione.
	[Art. 15, 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. 15, 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 16 - Modifiche al codice di procedura penale

L'**articolo 16** 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**.

Codice di procedura penale	
Testo previgente	**Modificazioni apportate dall'A.C. 1717**
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 previgente	**Modificazioni apportate dall'A.C. 1717**
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 previgente	**Modificazioni apportate dall'A.C. 1717**
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 previgente	**Modificazioni apportate dall'A.C. 1717**
nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110;	
6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni; 7) delitto di cui all'articolo 416 del codice penale nei casi in cui è obbligatorio l'arresto in flagranza; 7-*bis*) dei delitti previsto dagli articoli 600, 600-*bis*, primo comma, 600-*ter*, primo e secondo comma, 601, 602, 609- *bis* nelle ipotesi aggravate previste dall'articolo 609-*ter*, 609-*quater*, 609- *octies* del codice penale, nonché dei delitti previsti dagli articoli 12, comma 3, e 12-*bis* del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni;	*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 previgente	**Modificazioni apportate dall'A.C. 1717**
	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 17 - Modifiche alle norme sui collaboratori di giustizia

L'**articolo 17** 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.

Decreto-legge 15 gennaio 1991, n. 8	
Testo previgente	**Modificazioni apportate dall'A.C. 1717**
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 previgente	**Modificazioni apportate dall'A.C. 1717**
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 previgente	**Modificazioni apportate dall'A.C. 1717**
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 18 – Disciplina delle intercettazioni

L'articolo 18 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 - nella prospettiva del potenziamento degli strumenti investigativi – si introduce nell'articolo 13 del decreto-legge 13 maggio 1991, n. 152 (conv. legge n. 203 del 1991) un nuovo comma.

Articolo 19 - Modifiche al decreto legislativo 8 giugno 2001, n. 231

L'articolo 19 interviene sul catalogo dei **reati presupposto** della **responsabilità amministrativa degli enti**, contemplato dall'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

Articolo 20 - Modifica alla legge 11 gennaio 2018, n. 6

L'articolo 20 interviene sul procedimento di applicazione delle speciali misure di protezione per i **testimoni di giustizia** e per gli altri protetti (modificando il comma 2 dell'articolo 11 della legge 11 gennaio 2018, n. 6), in modo tale 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.

Articolo 21 - Modifiche al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)

L'**articolo 21** 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 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.

Articolo 22 - Verifica della sicurezza negli accessi alle banche dati presso gli uffici giudiziari

L'**articolo 22**, inserito in sede referente, 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**.

Legge n. 1311 del 1962	
Testo vigente	**Modificazioni apportate 22 dell'A.C. 1717-A**
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 ordinare che esse siano ripetute entro un termine minore negli uffici ove siano state riscontrate o per i quali vengono segnalate deficienze o irregolarità.	*Identico.*
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 23 - Disposizioni finanziarie

L'**articolo 23, 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**.

Iter

Prima lettura Camera 1717

Prima lettura Senato 1143

Legge n. 90 del 28 giugno 2024

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

Riepilogo del voto finale ripartito per Gruppo parlamentare			
Gruppo Parlamentare	Favorevoli	Contrari	Astenuti
APERRE	0 (0%)	0 (0%)	8 (100%)
AVS	0 (0%)	0 (0%)	7 (100%)
FDI	87 (100%)	0 (0%)	0 (0%)
FI-PPE	26 (100%)	0 (0%)	0 (0%)
IVICRE	0 (0%)	0 (0%)	7 (100%)
LEGA	30 (100%)	0 (0%)	0 (0%)
M5S	0 (0%)	0 (0%)	39 (100%)
MISTO	0 (0%)	1 (16,7%)	5 (83,3%)
NM-M	6(100%)	0 (0%)	0 (0%)
PD-IDP	0 (0%)	0 (0%)	50 (100%)