CAMERA DEI DEPUTATI

Mercoledì 27 settembre 2017

XVII LEGISLATURA
BOLLETTINO

DELLE GIUNTE E DELLE COMMISSIONI PARLAMENTARI
Politiche dell'Unione europea (XIV)
COMUNICATO

SEDE REFERENTE

Mercoledì 27 settembre 2017. — Presidenza del presidente Michele BORDO.

La seduta comincia alle 9.05.

Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017.
C. 4620 Governo, approvato dal Senato.
(Seguito esame e rinvio).

La Commissione prosegue l'esame del provvedimento in titolo, rinviato nella seduta del 20 settembre 2017.

Michele BORDO, *presidente*, avverte innanzitutto che la Conferenza dei presidenti di Gruppo svoltasi ieri pomeriggio ha fissato l'esame del provvedimento in Assemblea a partire da lunedì 9 ottobre.

Segnala quindi che sul disegno di legge di delegazione europea si sono sinora espresse con relazioni favorevoli tutte le Commissioni di merito, ad eccezione della Commissione Finanze, della Commissione Trasporti e della Commissione parlamentare per le Questioni regionali, che dovrebbero rendere il previsto parere entro la settimana corrente.

Avverte inoltre che sul provvedimento sono state presentate presso la XIV Commissione 20 proposte emendative, che sono poste in distribuzione e che saranno allegate al resoconto della seduta odierna (*vedi allegato*).

Le proposte emendative debbono ritenersi tutte ammissibili, ad eccezione dell'articolo Pag. 139aggiuntivo 10.01 Taricco, non rientrante nell'oggetto proprio della Legge di delegazione europea, come definito dall'articolo 30, comma 2, della Legge n. 234 del 2012. L'articolo aggiuntivo non reca infatti alcuna norma di delega finalizzata ad adeguare l'ordinamento nazionale a quello dell'Unione europea, ma interviene sulla disciplina della reintroduzione e del ripopolamento di specie animali e vegetali di cui al decreto del Presidente della Repubblica n. 357 del 1997.

Avverte che il termine per la presentazione di ricorsi avverso la pronuncia di inammissibilità è fissato alle ore 15 della giornata odierna.

Informa infine la Commissione che provvederà a trasmettere le proposte emendative alle Commissioni di merito per l'espressione del prescritto parere.

Nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 9.10.

ALLEGATO

Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017 (C. 4620 Governo, approvato dal Senato).

EMENDAMENTI ED ARTICOLI AGGIUNTIVI PRESENTATI

ART. 3.

Al comma 3, dopo la lettera d), *inserire la seguente:*

d-bis) prevedere, conformemente agli articoli 11 e 10, comma 4, della direttiva (UE) 2015/2436, il diritto del titolare del marchio d'impresa di vietare ai terzi di introdurre prodotti, in ambito commerciale, nello Stato membro di registrazione del marchio, senza la loro immissione in libera pratica in tale Stato, quando tali prodotti, compreso il loro imballaggio, provengono da Paesi terzi e recano senza autorizzazione un marchio che è identico al marchio registrato in relazione a tali prodotti o che non può essere distinto nei suoi aspetti essenziali da detto marchio, nonché il diritto del medesimo titolare di vietare atti preparatori in relazione all'uso di imballaggi o altri mezzi;

3. 1. Matarrelli.

Al comma 3, lettera e), *dopo le parole:* la provenienza geografica, *inserire le seguenti:* e l'origine.

Conseguentemente, al medesimo comma 3, lettera e), *dopo le parole:* o dei servizi, *inserire le seguenti:* e la tracciabilità.

3. 2. Gianluca Pini, Bossi.

Al comma 3, lettera f), *numero 1), dopo le parole:* la provenienza geografica, *inserire le seguenti:* e l'origine.

Conseguentemente, al medesimo comma 3, lettera f), *dopo le parole:* o dei servizi, *inserire le seguenti:* e la tracciabilità.

3. 4. Gianluca Pini, Bossi.

ART. 4.

Al comma 3, dopo la lettera e), *aggiungere la seguente:*

e-bis) prevedere nel caso di controversie riguardanti brevetti europei con effetto unitario, che il titolare del brevetto fornisca, su richiesta del tribunale competente, la traduzione integrale del brevetto europeo nella lingua utilizzata nel procedimento giudiziario, senza oneri a suo carico.

***4. 1.** Matarrelli.

Al comma 3, dopo la lettera e), *aggiungere la seguente:*

e-bis) prevedere nel caso di controversie riguardanti brevetti europei con effetto unitario, che il titolare del brevetto fornisca, su richiesta del tribunale competente, la traduzione integrale del brevetto europeo nella lingua utilizzata nel procedimento giudiziario, senza oneri a suo carico.

***4. 2.** Gianluca Pini, Bossi.

ART. 5.

Al comma 1, lettera a) *aggiungere, in fine, le seguenti parole:* , prevedendo che i Pag. 148relativi decreti legislativi siano adottati dal Ministro dello sviluppo economico di concerto con il Ministro dell'economia e delle finanze, sentite la Commissione Nazionale per le Società e la Borsa (CONSOB) e l'istituto per la vigilanza sulle assicurazioni IVASS).
5. 6. Elvira Savino.

Al comma 1, lettera l), *dopo la parola:* disciplinare *aggiungere le seguenti:* e rendere obbligatoria.
5. 1. Battelli.

Al comma 1, sopprimere le lettere m) *e* p).
5. 5. Elvira Savino.

Al comma 1, lettera o), *numero 3.2), sostituire le parole:* arco temporale costituiscono *con le seguenti:* arco temporale, che non può essere superiore a un anno, costituiscono.
5. 3. Battelli.

Al comma 3, lettera o), *punto 3.2), dopo la parola:* indole *inserire le seguenti:* compiute all'interno di un determinato arco temporale.
5. 4. Battelli.

Al comma 1, lettera o), *dopo il numero 6), aggiungere il seguente:* 6-*bis)* nell'ambito delle competenze ad essa attribuite, prevedere in capo all'autorità di vigilanza designata l'obbligo di riferire in Parlamento con cadenza semestrale, con particolare riguardo ai controlli effettuati e alle sanzioni amministrative comminate.
5. 2. Battelli.

Dopo l'articolo 5, inserire il seguente:

ART. 5-*bis.*
(Princìpi e criteri direttivi per 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).

1. Nell'esercizio della delega per 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, il Governo è tenuto a seguire, oltre ai princìpi e ai criteri direttivi generali di cui all'articolo 1, comma 1, anche i seguenti princìpi e criteri specifici:

a) prevedere una disciplina dei seguenti aspetti:

1) l'istituzione e l'organizzazione del sistema nazionale di sicurezza cibernetica;

2) l'attuazione delle contromisure cibernetiche;

3) i princìpi per il raggiungimento della piena sovranità nazionale nel settore scientifico e industriale relativo alla sicurezza cibernetica, al fine di garantire il completo controllo sulle infrastrutture strategiche cibernetiche del Paese;

4) l'istituzione e le funzioni dell'Alta scuola di formazione cibernetica, al fine di garantire l'uniformità della formazione in materia cibernetica nell'ambito della pubblica amministrazione;

5) il controllo parlamentare sul sistema nazionale di sicurezza cibernetica,

b) inserire le seguenti definizioni:

1) «spazio cibernetico»: l'insieme delle infrastrutture informatiche interconnesse, comprendente *hardware*, *software*, dati e utenti, nonché delle relazioni logiche, comunque stabilite, tra essi;

2) «sicurezza cibernetica»: la condizione per la quale lo spazio cibernetico risulta protetto mediante l'adozione di Pag. 149idonee misure di sicurezza fisica, logica e procedurale rispetto a eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro illegittima modifica o distruzione ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

3) «minaccia cibernetica»: il complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia, in particolare, nelle azioni di singoli individui od organizzazioni, statali e no, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro illegittima modifica o distruzione ovvero a danneggiare, distruggere od ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

4) «sovranità cibernetica»: la capacità dello Stato di essere autosufficiente nella costruzione, nel controllo e nella certificazione in ambito sia di *software*, sia di *hardware*;

5) «evento cibernetico»: l'avvenimento significativo, di natura volontaria o accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro illegittima modifica o distruzione ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

6) «allarme cibernetico»: la comunicazione di avviso di un evento cibernetico da valutare ai fini dell'attivazione di misure di risposta pianificate;

7) «situazione di crisi cibernetica»: la situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, bensì con l'assunzione di decisioni coordinate in sede interministeriale;

8) «contromisure cibernetiche»: le azioni mirate alla risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale, effettuate al fine di eliminare la situazione di crisi;

9) *InfoSharing*: il sistema costituito da una piattaforma informatica per la condivisione delle informazioni sugli allarmi e sugli eventi cibernetici, contenente altresì le soluzioni relative agli allarmi e agli eventi cibernetici;

10) «LGC»: le linee guida comuni;

11) «IS»: le infrastrutture strategiche;

12) «operatori di servizi essenziali»: gli operatori di cui all'allegato II 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 (c.d. direttiva NIS);

13) «fornitori di servizi digitali»: i fornitori di cui all'allegato III della direttiva NIS;

14) «CERT»: il *computer emergency response team*;

15) «SOC»: il *Security operations center*;

16) «NSC»: il Nucleo per la sicurezza cibernetica, di cui all'articolo 8 del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013;

17) «CISR»: il Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124;

18) «DIS»: il Dipartimento delle informazioni per la sicurezza, di cui all'articolo 4 della legge 3 agosto 2007, n. 124;

19) «AISE»: l'Agenzia informazioni e sicurezza esterna, di cui all'articolo 6 della legge 3 agosto 2007, n. 124;Pag. 150

20) «AISI»: l'Agenzia informazioni e sicurezza interna, di cui all'articolo 7 della legge 3 agosto 2007, n. 124;

21) «ISCOM»: l'istituto superiore delle comunicazioni e delle tecnologie dell'informazione, istituito dalla legge 24 marzo 1907, n. 111;

22) «CNAIPIC»: il Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche, istituito dal decreto del Capo della Polizia – Direttore generale della pubblica sicurezza 7 agosto 2008;

23) «CERT-IT»: il CERT di cui all'articolo 10 nel quale confluiscono le competenze di CERT-Nazionale e CERT-PA;

24) «CERT-Nazionale»: il CERT di cui all'articolo 16-*bis* del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; abrogato in base all'articolo 10, comma 2, della presente legge;

25) «CERT-PA»; il CERT della pubblica amministrazione, istituito presso l'Agenzia per l'Italia digitale ai sensi del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013; abrogato in base all'articolo 10, comma 2, della presente legge;

26) «CERT-Difesa»: il CERT istituito presso lo stato maggiore della Difesa, ai sensi della direttiva del Ministro per l'innovazione e le tecnologie 16 gennaio 2002, pubblicata nella *Gazzetta Ufficiale* n. 69 del 22 marzo 2002;

27) «DACI»; il Direttore per l'analisi cibernetica internazionale;

28) «RIS»; il reparto informazioni e sicurezza dello stato maggiore della Difesa;

29) «CIOC»; il Comando Interforze per le Operazioni Cibernetiche, di cui all'articolo 15, comma 2;

30) «ANSC»; l'Agenzia Nazionale per lo Spazio Cibernetico, di cui all'articolo 7;

c) riformare l'istituzione e l'organizzazione del sistema nazionale di sicurezza cibernetica prevedendo che sia composto dai seguenti organi dotati di determinate funzioni:

1) l'Autorità Delegata coordina politicamente gli uffici ministeriali preposti alla sicurezza cibernetica;

2) il Presidente del Consiglio dei ministri provvede al coordinamento delle politiche dell'informazione per la sicurezza, impartisce le direttive e, sentito il CISR, emana ogni disposizione necessaria per l'organizzazione e per il funzionamento del sistema nazionale di sicurezza cibernetica, nonché per lo sviluppo e la sostenibilità delle capacità nazionali nello spazio cibernetico;

3) al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) l'alta direzione e la responsabilità generale della politica di sicurezza cibernetica nazionale, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento;

b) l'adozione e l'aggiornamento almeno annuale, su proposta dell'ANSC, del Quadro strategico nazionale per la sicurezza dello spazio cibernetico, contenente l'indicazione dei profili e delle tendenze evolutive delle minacce cibernetiche e dei fattori di vulnerabilità dei sistemi e delle reti di interesse nazionale, l'indicazione dei criteri per lo sviluppo degli strumenti e delle procedure con cui si provvede all'incremento delle capacità di prevenzione e di risposta rispetto ad eventi occorrenti nello spazio cibernetico, al fine di diffondere la cultura della sicurezza;

c) l'adozione, previa deliberazione dell'ANSC, sentito il CISR, del Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, contenente gli obiettivi da conseguire e le linee Pag. 151di azione da porre in essere per realizzare il Quadro strategico nazionale di cui alla lettera *b)*;

d) l'emanazione delle direttive e degli atti d'indirizzo necessari per l'attuazione del Piano di cui alla lettera *c)*;

e) la nomina e la revoca, sentito il CISR, del direttore dell'ANSC;

f) la determinazione, di concerto con i Ministri dell'economia e delle finanze, dell'interno e della difesa, dell'ammontare annuo delle risorse finanziarie destinate all'attività del sistema nazionale di sicurezza cibernetica a valere sul fondo di cui alla lettera *t)*;

4) il Presidente del Consiglio dei ministri, delega le funzioni che non sono ad esso attribuite in via esclusiva all'Autorità delegata. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate e sui risultati conseguiti. Fermo restando il potere di direttiva, egli può comunque avocare a sé in qualsiasi momento l'esercizio di tutte le funzioni delegate o di alcune di esse. In deroga a quanto previsto dal comma 1 dell'articolo 9 della legge 23 agosto 1988, n. 400, e successive modificazioni, non è richiesto il parere del Consiglio dei ministri per il conferimento delle deleghe di cui al presente articolo al Ministro senza portafoglio;

5) l'Autorità delegata esercita l'alta sorveglianza sull'attuazione del Piano nazionale;

6) l'Agenzia Nazionale per la Sicurezza Cibernetica svolge attività a carattere tecnico-operativo di interesse nazionale. Essa opera al servizio delle amministrazioni pubbliche, comprese anche quelle regionali e locali. L'ANSC ha piena autonomia nei limiti stabiliti dalla legge ed è sottoposta al controllo della Corte dei conti, ai sensi dell'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20. Essa è sottoposta ai poteri di indirizzo e di vigilanza dell'Autorità Delegata. All'ANSC sono attribuiti, nell'ambito del sistema nazionale di sicurezza cibernetica, i seguenti compiti:

a) proporre al Presidente del Consiglio dei ministri l'adozione del Quadro strategico nazionale;

b) deliberare, sentito il CISR, il Piano nazionale, ai fini della sua adozione da parte del Presidente del Consiglio dei ministri;

c) esprimere parere, ai sensi dell'articolo 5, comma 2, lettera *h)*, della legge 23 agosto, 1988, n. 400, sulle direttive e sugli atti d'indirizzo del Presidente del Consiglio dei ministri;

d) esprimere parere, ai sensi dell'articolo 1, comma 3-*bis*, della legge 3 agosto 2007, n. 124, ai fini dell'adozione delle direttive del Presidente del Consiglio dei ministri destinate al DIS e ai servizi di informazione per la sicurezza in materia di sicurezza cibernetica;

e) approvare le LGC per favorire l'efficace e strutturata collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di buone pratiche e di misure rivolte all'obiettivo della sicurezza cibernetica;

f) elaborare, ai sensi dell'articolo 5 della legge 3 agosto 2007, n. 124, gli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali, da perseguire nel quadro della politica dell'informazione per la sicurezza da parte degli organismi di informazione per la sicurezza, ciascuno per i profili di rispettiva competenza;

g) promuovere, tramite il CERT-IT e il CERT-Difesa, l'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale, sia in ambito bilaterale o multilaterale, sia negli ambiti dell'Unione europea e dell'Alleanza atlantica, al fine Pag. 152della definizione e dell'adozione di politiche e strategie comuni di prevenzione e di risposta alla minaccia cibernetica;

h) formulare le proposte di intervento normativo e organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle situazioni di crisi;

i) partecipare, con funzioni di consulenza e di proposta, alle decisioni del Presidente del Consiglio dei ministri in caso di situazioni di crisi. Alle riunioni del CISR aventi ad oggetto la materia della sicurezza cibernetica partecipa, con funzioni di consulenza, il direttore dell'ANSC. Si applicano le disposizioni dell'articolo 5, comma 5, della legge 3 agosto 2007, n. 124;

7) il DIS, l'AISE e l'AISI svolgono la propria attività nel campo della sicurezza cibernetica avvalendosi degli strumenti e secondo le modalità e le procedure previsti dalla legge 3 agosto 2007, n. 124, avvalendosi, quando opportuno, del supporto e del coordinamento dell'ANSC. Il direttore generale del DIS, sulla base delle direttive adottate dal Presidente del Consiglio dei ministri ai sensi dell'articolo 1, comma 3-*bis*, della legge 3 agosto 2007, n. 124, nonché degli indirizzi generali e degli obiettivi fondamentali individuati dall'ANSC, cura, ai sensi dell'articolo 4, comma 3, lettera *d-*

bis), della citata legge n. 124 del 2007, il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Il DIS, sulla base delle informazioni raccolte e delle acquisizioni provenienti dallo scambio informativo di cui all'articolo 4, comma 3, lettere *c)* ed *e)*, della legge 3 agosto 2007, n. 124, nonché degli elementi acquisiti ai sensi dell'articolo 13, commi 1 e 2, della medesima legge n. 124 del 2007, trasmette al CERT-IT informazioni e analisi su eventi cibernetici. Il DIS e il CERT-IT provvedono a trattare tempestivamente le informazioni e a pubblicarle, con le garanzie necessarie in base alla loro classificazione di segretezza, nella piattaforma *InfoSharing*. Per lo svolgimento delle attività di coordinamento, il direttore generale del DIS si avvale delle strutture del medesimo DIS nonché, ove necessario, della collaborazione del CERT-IT. Il DIS, sulla base delle informazioni raccolte e delle acquisizioni provenienti dallo scambio informativo di cui all'articolo 4, comma 3, lettere *c)* ed *e)*, della legge 3 agosto 2007, n. 124, nonché degli elementi acquisiti ai sensi dell'articolo 13, commi 1 e 2, della medesima legge n. 124 del 2007, cura altresì la formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica. Provvede inoltre, secondo le disposizioni della presente legge, alla trasmissione delle informazioni rilevanti ai fini della sicurezza cibernetica all'ANSC, alle pubbliche amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni medesime, ai sensi dell'articolo 4, comma 3, lettera *f)*, della citata legge n. 124 del 2007;

8) L'AISE e l'AISI, nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive del Presidente del Consiglio dei ministri e le linee di coordinamento delle attività di ricerca informativa stabilite dal direttore generale del DIS, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali. Per lo svolgimento delle attività previste dal presente articolo, il DIS, l'AISE e l'AISI corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilità, le università e gli enti di ricerca; per il medesimo fine possono stipulare convenzioni con tali soggetti ai sensi dell'articolo 13, comma 1, della legge 3 agosto 2007, n. 124, previa comunicazione all'ANSC. Per le stesse finalità, le pubbliche amministrazioni e i soggetti erogatori di servizi di pubblica utilità consentono l'accesso del DIS, dell'AISE e dell'AISI ai propri archivi informatici, per il tramite degli uffici per la sicurezza cibernetica e la digitalizzazione ai sensi dell'articolo 28, secondo le modalità e con le procedure previste dal regolamento di cui al decreto del Presidente Pag. 153del Consiglio dei ministri 12 giugno 2009, n. 2.

Il Ministro degli affari esteri e della cooperazione internazionale nomina, sentita l'AISE, il Direttore per l'analisi cibernetica internazionale (DACI), con il compito di fornire ai competenti organi politici una visione geopolitica complessiva rispetto agli eventi cibernetici. L'AISE collabora con il DACI per l'analisi degli eventi cibernetici pertinenti agli interessi italiani all'estero e ne comunica i risultati al direttore dell'ANSC;

9) presso l'ANSC è costituito, in via permanente, il Nucleo per la sicurezza cibernetica, a supporto del Direttore dell'ANSC, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il NSC è presieduto da un direttore dell'ANSC ed è composto da un rappresentante, rispettivamente, del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri e dell'Agenzia per l'Italia digitale nonché dal direttore del CERT-IT.

I rappresentanti degli organi ed enti di cui al primo periodo sono designati secondo quanto previsto dalle LGC approvate.

Per gli aspetti relativi alla trattazione di informazioni classificate, il NSC è integrato da un rappresentante dell'ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124.

L'incarico di Direttore dell'ANSC ha durata triennale, rinnovabile una sola volta, ed è conferito con decreto del Presidente del Consiglio dei ministri, sentito il CISR, a un soggetto dotato di

adeguata qualificazione e affidato ad un dirigente di prima fascia o equiparato, appartenente al DIS, al Ministero della difesa, al Ministero dell'interno o al Ministero dello sviluppo economico.

I rappresentanti degli organi ed enti competenti, nelle riunioni del NSC, sono coadiuvati da esperti appartenenti alle strutture operative del rispettivo organo o ente. Il Direttore del NSC può autorizzare la partecipazione di rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della sicurezza cibernetica. Il NSC si riunisce su iniziativa del direttore dell'ANSC o su richiesta di almeno uno dei suoi componenti;

10) presso l'ANSC è istituito il CERT-IT, il CERT-PA e il CERT Nazionale sono abrogati e le loro competenze e strutture sono trasferite al CERT-IT cui sono attribuiti i seguenti compiti:

a) valutare e promuovere, in raccordo con le amministrazioni competenti per specifici profili della sicurezza cibernetica, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi cibernetiche;

b) acquisire e coordinare, tramite il Ministero dello sviluppo economico, gli organismi di informazione per la sicurezza, le Forze di polizia e le strutture del Ministero della difesa, le comunicazioni circa i casi di violazione o i tentativi di violazione della sicurezza cibernetica e i casi di perdita dell'integrità di dati significativi ai fini del corretto funzionamento delle reti e dei servizi;

c) esercitare le funzioni di punto di riferimento nazionale per i rapporti con le organizzazioni internazionali e con gli altri Stati, nell'ambito della sicurezza cibernetica, ferme restando le specifiche competenze del Ministero dello sviluppo economico, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa e delle altre amministrazioni competenti, assicurando il necessario coordinamento;

d) mantenere un costante scambio di informazioni e coordinare le proprie attività Pag. 154con il CNAIPIC e con il CERT-Difesa, al fine di conseguire la massima efficacia delle rispettive azioni;

e) attivare un unico sito internet istituzionale per gli organi competenti, nel quale sono pubblicate le informazioni sullo stato della sicurezza cibernetica;

f) promuovere e coordinare, d'intesa con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni che coinvolgono amministrazioni diverse nonché la partecipazione nazionale a esercitazioni internazionali con la simulazione di eventi cibernetici;

g) definire la base di dati, il sistema di accesso e il mantenimento del sistema di *InfoSharing* unico; la definizione delle caratteristiche tecniche relative alla conservazione e all'accesso alle informazioni classificate è effettuata d'intesa con il CNAIPIC, il CERT-Difesa e il DIS;

Il CERT-IT inoltre:

aa) individua una sede unica per gli operatori del CERT-IT, del CERT-Difesa e del CNAIPIC;

bb) redige un protocollo per l'integrazione delle funzioni degli organi interessati, al fine di rendere più efficace e temporalmente completo il controllo delle IS;

cc) attiva un sistema di *InfoSharing* unico, che consenta di memorizzare dati, con distinte autorizzazioni all'accesso in relazione al livello di segretezza del dato inserito, nel rispetto delle disposizioni della legge 3 agosto 2007, n. 124. L'accesso al sistema di *InfoSharing* unico nonché l'inserimento dei dati da parte di enti diversi dal CERT-IT sono gratuiti. Il sistema di *InfoSharing* unico è certificato dall'ISCOM;

dd) definisce le LGC per la gestione delle simulazioni di eventi cibernetici;

ee) redige protocolli per la comunicazione e lo scambio di dati con i CERT interni delle pubbliche amministrazioni e degli enti privati tenuti a tale adempimento secondo le disposizioni della presente legge;

ff) stabilisce i criteri in base ai quali gli organi della pubblica amministrazione sono tenuti a dotarsi di un CERT interno;

gg) stabilisce i criteri in base ai quali un'amministrazione può usufruire dei CERT di altre amministrazioni;

hh) adotta le regole per la gestione, l'inserimento dei dati e la consultazione del sistema di *InfoSharing* unico;

11) nell'ambito del sistema nazionale di sicurezza cibernetica, il CNAIPIC esercita le funzioni di autorità di pubblica sicurezza, in coordinamento con il CERT-IT.

Al CNAIPIC sono attribuiti i seguenti compiti:

a) disporre l'interruzione dei pubblici servizi, su richiesta del Presidente del Consiglio dei ministri o dell'Autorità delegata, qualora sia necessario per contrastare un evento cibernetico di gravità tale da poter evolvere in una crisi cibernetica nazionale;

b) ricevere o produrre le informazioni classificate relative a eventi cibernetici e trattarle, provvedendo nel più breve tempo possibile alla rimozione dei dati e degli elementi classificati allo scopo di condividere con gli altri soggetti del sistema nazionale di sicurezza cibernetica le notizie necessarie alla risoluzione della crisi cibernetica o dell'evento cibernetico;

c) raccogliere e trasmettere ai soggetti interessati, in collaborazione con il DIS e nel rispetto delle disposizioni della legge 3 agosto 2007, n. 124, le informazioni classificate o riservate o la cui divulgazione potrebbe comunque costituire un pericolo per la sicurezza nazionale;

d) garantire al CERT-IT l'integrazione del personale necessario ad assicurare la piena e ininterrotta operatività dei servizi di difesa cibernetica.

Il CNAIPIC inoltre:

aa) compila l'elenco delle IS;

bb) definisce le LGC per l'integrazione dell'elenco di cui alla lettera *a)*;

12) All'ISCOM sono attribuiti i seguenti compiti:

a) elaborare, convalidare, controllare e certificare le caratteristiche dei sistemi *software* e *hardware* distribuiti nel territorio nazionale;

b) elaborare e proporre al Presidente del Consiglio dei ministri le soluzioni per raggiungimento della completa sovranità cibernetica.

L'ISCOM, entro sei mesi dalla data di entrata in vigore della presente legge:

aa) definisce le LGC per la certificazione delle procedure operative dei CERT, adottando le regole comuni e i criteri da applicare;

bb) definisce le LGC per la certificazione dei sistemi hardware e software per garantire la sovranità cibernetica;

cc) coadiuva tecnicamente l'attività del CERT-IT nella realizzazione del sistema di *InfoSharing* unico;

13) nell'ambito del sistema nazionale di sicurezza cibernetica, il CERT-Difesa opera nel campo della sicurezza militare, alle dipendenze del Ministro della difesa, in coordinamento con il DIS e con il RIS. Nell'ambito dello Stato maggiore della difesa è istituito il Comando Interforze per le Operazioni Cibernetiche (CIOC), al quale spettano l'organizzazione e la direzione operativa delle attività relative alla difesa cibernetica. Le attribuzioni, la struttura e l'organizzazione del CIOC sono stabilite con decreto del Ministro della difesa, da adottare entro quattro mesi dalla data di entrata in vigore della presente legge. Al CIOC spetta la direzione delle operazioni relative alle contromisure cibernetiche di cui all'articolo 19. Al CERT-Difesa sono attribuiti i seguenti compiti:

a) organizzare il sistema di protezione dei sistemi cibernetici delle Forze armate;

b) esercitare le funzioni di punto di riferimento nazionale per i rapporti con le organizzazioni internazionali e con altri Stati, nell'ambito della sicurezza cibernetica nel settore militare.

Il CERT-Difesa opera alle dipendenze del CIOC con la finalità di fornire informazioni sugli eventi cibernetici nel settore cibernetico militare.

Con decreto del Ministro della difesa è definita l'organizzazione del CERT-Difesa nell'ambito del CIOC;

14) presso l'Alta scuola di formazione cibernetica di cui all'articolo 21 è istituito un comitato scientifico composto da esperti nelle discipline inerenti alla sicurezza cibernetica provenienti dalle università, dagli enti di ricerca, dalle pubbliche amministrazioni e dal settore privato. Il comitato predispone programmi di intervento volti a migliorare i parametri e i livelli di sicurezza dei sistemi e delle reti, al fine di coadiuvare il sistema nazionale di sicurezza cibernetica;

d) definire le disposizioni in materia di personale garantendo la riservatezza delle informazioni raccolte dagli organi di cui fanno parte, il personale civile impiegato per le funzioni svolte dai medesimi organi può essere assunto soltanto con contratto di lavoro a tempo indeterminato.

Il personale civile da destinare agli organi suddetti è scelto in via prioritaria tra coloro che hanno conseguito l'attestato di qualificazione presso l'Alta scuola di formazione cibernetica. Ci si può avvalere di consulenti esterni scelti tra cittadini italiani che possiedono comprovate capacità nelle attività cibernetiche;

e) disciplinare e programmare l'assunzione di personale definendo per ogni triennio le modalità di assunzione del personale civile da assegnare e programmare annualmente il fabbisogno del personale civile necessario indicando i requisiti necessari per ciascun ruolo individuato Pag. 156e definire gli ambiti della difesa cibernetica per i quali si possono stipulare contratti di consulenza di durata non superiore a un anno con soggetti esterni alla pubblica amministrazione;

f) disciplinare la classificazione dei dati attribuendo al DIS l'esercizio, la gestione e il trattamento dei dati classificati nel settore della sicurezza cibernetica con gli strumenti e secondo le modalità e le procedure stabiliti dalla legge 3 agosto 2007, n. 124.

Il CERT-Difesa e il CNAIPIC collaborano con il DIS per il trattamento dei dati classificati nel campo della sicurezza cibernetica;

g) definire la gestione di eventi cibernetici classificati secondo i seguenti principi:

1) Il CNAIPIC d'intesa con il DIS e con gli organi competenti definisce le LGC per la presa in carico e la gestione degli eventi cibernetici classificati e per la pubblicazione, mediante la piattaforma *InfoSharing*, delle informazioni utili a ridurre l'eventuale crisi cibernetica o la sua propagazione;

2) Nelle LGC predisposte ai sensi del comma 1 sono stabiliti:

a) il termine, non superiore a tre ore, per la presa in carico delle informazioni da parte del CNAIPIC e per la valutazione della necessità di pubblicazione delle stesse, previa rimozione dei dati e degli elementi classificati ai sensi dell'articolo 11, comma 2, lettera *b)*;

b) il termine decorso il quale, senza che il CNAIPIC abbia proceduto alla pubblicazione delle informazioni, gli organi di cui agli articoli 9, 10, 11, 12 e 11 possono reiterare la richiesta ai fini della presa in *h)* stabilire gli organi e le funzioni degli operatori di contromisure cibernetiche prevedendo che:

1) le Forze armate sono autorizzate all'uso e alla gestione delle contromisure cibernetiche;

2) le Forze armate possono sviluppare programmi di contromisure cibernetiche finalizzati alla verifica della funzionalità dei sistemi di difesa cibernetica previsti ai sensi della presente legge;

3) per le finalità di cui al numero 2, le Forze armate possono avvalersi delle imprese iscritte presso la Presidenza del Consiglio dei ministri nell'elenco delle imprese certificate per lo sviluppo negli ambiti cibernetici;

4) le attività di cui ai numeri 1 e 2 sono finanziate a valere sul Fondo di cui alla lettera *u)*;

h) stabilire la competenza a deliberare le contromisure cibernetiche secondo i seguenti princìpi:

1) fuori dei casi previsti dagli articoli 78 e 87, nono comma, della Costituzione, l'uso delle contromisure cibernetiche è consentito, in conformità a quanto disposto dalla presente legge, a condizione che avvenga nel rispetto dei princìpi di cui all'articolo 11 della Costituzione, del diritto

internazionale generale, del diritto internazionale dei diritti umani, del diritto internazionale umanitario e del diritto internazionale penale;

2) l'uso delle contromisure cibernetiche è deliberato dal Consiglio dei ministri, previa comunicazione al Presidente della Repubblica. Ove il Presidente della Repubblica o il Governo ne ravvisi la necessità, può essere convocato il Consiglio supremo di difesa, ai sensi dell'articolo 8, comma 2, del codice dell'ordinamento militare, di cui al decreto legislativo 13 marzo 2010, n. 66;

3) il Governo comunica al Comitato parlamentare per la sicurezza della Repubblica, ai sensi dell'articolo 44, le misure deliberate ai sensi del numero 2;

4) agli operatori che attuano le deliberazioni di cui ai numeri 2 e 6, sono riconosciute le garanzie funzionali di cui all'articolo 15 della legge 3 agosto 2007, n. 124, alle condizioni ivi previste. La deliberazione di cui al numero 2 del Pag. 157presente articolo tiene luogo dell'autorizzazione di cui all'articolo 16 della citata legge n. 124 del 2007;

5) le garanzie di cui al numero 4 non si applicano in nessun caso ai crimini previsti dagli articoli da 5 a 8 dello Statuto della Corte penale internazionale, adottato a Roma il 15 luglio 1998, ratificato ai sensi della legge 12 luglio 1999, n. 232;

6) le disposizioni di cui ai numeri 1 e 2, non si applicano per le contromisure cibernetiche impiegate nell'ambito della protezione delle forze impegnate nelle missioni internazionali autorizzate ai sensi della legge n. 147 del 2016;

i) prevedere un alta scuola di formazione cibernetica disciplinata secondo i seguenti princìpi:

1) è istituita presso l'ANSC l'Alta scuola di formazione cibernetica, di seguito denominata «Alta scuola», con il compito di curare la formazione:

a) del personale della pubblica amministrazione da inquadrare presso gli organi di cui alle lettere precedenti;

b) del personale della pubblica amministrazione competente per l'ambito cibernetico;

2) il funzionamento dell'Alta scuola è assicurato a valere sulle risorse del Fondo di cui alla lettera *t)*;

3) l'Alta scuola può istituire corsi destinati a personale della pubblica amministrazione, diverso dai soggetti indicati al numero 1, nonché a personale delle università, degli enti di ricerca e di enti e imprese privati, al fine di diffondere e incrementare la cultura e la formazione nel settore della sicurezza cibernetica;

4) al termine dei corsi di formazione, l'Alta scuola rilascia il corrispondente attestato di qualificazione ai partecipanti che hanno superato l'esame finale;

5) l'Alta scuola si avvale oltre che del personale competente anche di docenti e ricercatori delle università, sulla base di contratti di consulenza;

6) con decreto del Ministro dell'istruzione, dell'università e della ricerca, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, di concerto con il Ministro della difesa e con il Ministro dello sviluppo economico e sentito l'ISCOM, sono definite la struttura, l'organizzazione e la disciplina dei corsi dell'Alta scuola, nonché gli ambiti della formazione da essa impartita;

7) i percorsi di studio dell'Alta scuola, uniformi per il personale di tutte le pubbliche amministrazioni, sono distinti in base alle funzioni dirigenziali od operative esercitate e al livello di qualificazione richiesto. Per il personale che esercita funzioni operative sono previste esercitazioni e verifiche pratiche secondo la specificità della materia cibernetica;

l) prevedere una Scuola di formazione per la gestione dei dati classificati in materia cibernetica disciplinata secondo i seguenti principi:

1) alla formazione cibernetica del personale degli organi di cui agli articoli 11 e 13, nell'ambito riguardante dati classificati, provvede la Scuola di formazione del DIS, istituita ai sensi dell'articolo della legge 3 agosto 2007, n. 124;

2) la Scuola di formazione del DIS provvede alla formazione del personale necessario a svolgere le funzioni relative alla gestione e all'uso delle contromisure cibernetiche in collaborazione con il RIS;

3) l'Alta scuola assicura il coordinamento e il collegamento con le università ai fini di:

a) selezionare i docenti e i ricercatori universitari da impiegare per lo svolgimento dei corsi di formazione;

b) attivare corsi di formazione nell'ambito cibernetico per gli studenti universitari meritevoli;

c) attivare corsi di aggiornamento permanente per il personale docente e i ricercatori universitari nel settore della sicurezza cibernetica;Pag. 158

m) prevedere un ente di definizione degli standard cibernetici disciplinato secondo i seguenti principi:

1) è istituito presso l'ISCOM l'Ente per la definizione degli standard in ambito cibernetico (EDSC), con il compito di:

a) definire gli standard relativi a *hardware*, *software* e *firmware* per garantire il corretto funzionamento dei sistemi nell'ambito della sicurezza cibernetica;

b) definire annualmente, in collaborazione con l'Alta scuola, le LGC per la formazione nel settore della difesa cibernetica;

2) in caso di definizione di nuovi *standard* ai sensi del numero 1 che comportino oneri di adeguamento per i soggetti privati, gli oneri conseguenti a carico di questi ultimi sono ristorati, anche parzialmente, a valere sul Fondo di cui alla lettera *t)*;

n) predisporre dei programmi di diffusione della cultura cibernetica seguendo i seguenti princìpi:

1) entro un anno dalla data di entrata in vigore della presente legge, con decreto del Ministro dell'istruzione, dell'università e della ricerca, di concerto con i Ministri dell'interno, della difesa e dello sviluppo economico, sono disciplinati:

a) un programma di diffusione della cultura della sicurezza cibernetica, anche tramite appositi corsi da attivare nelle università e nelle scuole primarie e secondarie di primo e di secondo grado;

b) una campagna di informazione, tramite i mezzi di comunicazione di massa e la rete *internet*, finalizzata alla diffusione della cultura della sicurezza cibernetica;

2) il programma e la campagna di cui al numero 1 sono aggiornati con cadenza almeno annuale;

o) prevedere le disposizioni per gli enti pubblici e privati in particolare:

1) per i ministeri e le Agenzie:

a) presso tutti i ministeri e le agenzie dello Stato è istituito un ufficio per la sicurezza cibernetica e la digitalizzazione, alle dirette dipendenze dell'ANSC;

b) nell'ambito delle attività del ministero in cui sono istituiti, gli uffici per la sicurezza cibernetica e la digitalizzazione provvedono a:

1) predisporre il piano di digitalizzazione del rispettivo ministero;

2) vigilare sull'applicazione delle norme di sicurezza cibernetica;

3) predisporre l'istituzione di un SOC e garantire il pieno e costante funzionamento, anche in collaborazione con il CERT-IT.

2) per le Regioni ed Enti locali:

a) entro sei mesi dall'entrata in vigore della presente legge, regioni ed enti locali istituiscono un proprio SOC e ne garantiscono il pieno e costante funzionamento. A tale scopo gli enti locali possono avvalersi anche di forme di gestione associata;

b) i SOC di cui al comma 1 collaborano direttamente con il CERT-IT e provvedono a popolarne la piattaforma di *InfoSharing*, secondo le modalità definite dall'ANSC;

3) per gli enti privati di interesse strategico:

a) Ai fini della presente legge, sono considerati enti privati di interesse strategico gli enti privati gestori o responsabili delle IS definite dal CNAIPIC;

b) Per il supporto e l'aggiornamento dei sistemi di difesa cibernetica è consentito agli enti privati di interesse strategico l'accesso alle risorse del Fondo di cui alla lettera *u)*;

c) Con decreto del Presidente del Consiglio dei ministri, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, sono definite le modalità per l'accesso alle risorse del

Fondo di cui alla lettera *u)*;Pag. 159

4) per gli enti privati di rilevanza cibernetica:

a) sono considerati enti privati di rilevanza cibernetica per la pubblica amministrazione i soggetti privati che hanno rapporti con essa;

b) con decreti dei Ministri competenti, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, sono approvati gli elenchi degli enti di cui al comma 1, previa valutazione della rilevanza cibernetica, della natura e della frequenza dei rapporti tra gli enti privati interessati e la pubblica amministrazione. Gli elenchi sono aggiornati con le stesse modalità ogni volta che il Ministro lo ritenga necessario e, comunque, annualmente;

c) il CERT-IT definisce le LGC per la fissazione dei livelli di sicurezza da applicare agli enti privati che hanno rapporti con la pubblica amministrazione. Le LGC sono rese pubbliche nel sito internet istituzionale del CERT-IT;

d) ai soggetti di cui al numero 2 che hanno rapporti con la pubblica amministrazione non si applicano le disposizioni di cui alla lettera *c)*. Ad essi si applicano le disposizioni del numero 10;

5) per gli altri enti privati:

a) l'Alta scuola organizza corsi di formazione finalizzati a rafforzare la cultura della sicurezza cibernetica, ai quali può partecipare il personale degli enti privati diversi da quelli di cui ai numeri 3 e 4, selezionato in base ad appositi bandi pubblici. I corsi di formazione sono gratuiti. Restano a carico degli enti privati di appartenenza tutte le spese relative alla frequenza dei partecipanti, compreso il costo dell'eventuale materiale didattico necessario per il corso ceduto in proprietà al partecipante;

6) stabilire un obbligo di comunicazione e accesso alla piattaforma *InfoSharing*:

a) agli enti privati di cui ai numeri 3 e 4 è consentito l'accesso gratuito alla piattaforma *InfoSharing*, in modalità di lettura e scrittura e con il supporto degli organi competenti, limitatamente alle informazioni non classificate;

b) agli enti privati di cui al numero 4 è consentito l'accesso gratuito alla piattaforma *InfoSharing*, in modalità di lettura e scrittura, limitatamente alle informazioni non classificate;

c) gli enti privati di cui ai numeri 3, 4 e 5 che accedono alla piattaforma *InfoSharing* devono comunicare, con le necessarie garanzie di tutela della riservatezza, tramite la medesima piattaforma *InfoSharing*, gli eventuali attacchi ai propri sistemi informatici entro ventiquattro ore dal momento in cui sono stati rilevati;

7) definire il livello di sicurezza di base per gli enti privati:

a) gli enti privati di cui all'articolo 5 devono adottare le misure minime definite dall'articolo 34 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196;

8) stabilire il livello di sicurezza medio per gli enti privati:

a) gli enti privati individuati ai sensi del numero 4 devono adottare le seguenti misure per la sicurezza cibernetica:

1) definire un responsabile della sicurezza cibernetica, dipendente dell'ente privato stesso o di un ente fornitore;

2) qualora abbiano più di 100 dipendenti, computati indipendentemente dalla forma del rapporto di lavoro instaurato, dotarsi di un SOC, i cui componenti devono essere formati annualmente mediante appositi corsi organizzati dall'Alta scuola;

3) garantire ai dipendenti adibiti a mansioni che prevedono l'impiego di sistemi cibernetici un aggiornamento, almeno annuale, sulla sicurezza cibernetica.

Gli oneri di adeguamento a carico degli enti privati sono ristorati, anche parzialmente, Pag. 160a valere sul Fondo di cui alla lettera *t)*;

9) stabilire il livello di sicurezza alto per enti privati:

a) agli enti privati individuati ai sensi del numero 4, che hanno più di mille *host IP* nell'azienda e i cui proventi derivano almeno per il 5 per cento da soggetti aventi sede in uno Stato

estero si applicano le disposizioni del medesimo numero. Tali enti devono adottare le seguenti misure per la sicurezza cibernetica:

aa) istituire un CERT interno all'ente, che opera secondo i protocolli definiti dal CERT-IT;

bb) realizzare un sistema di scambio dei dati prioritario e garantito dal CERT-IT tramite la piattaforma *InfoSharing;*

cc) assicurare la formazione dei componenti del CERT interno di cui alla lettera *a)* mediante la partecipazione ad appositi corsi organizzati presso l'Alta scuola.

Gli oneri di adeguamento a carico degli enti privati sono ristorati, anche parzialmente, a valere sul Fondo di cui alla lettera *t);*.

10) definire il livello di sicurezza per gli enti privati di interesse strategico:

a) gli enti privati di cui al numero 3, devono:

1) individuare un responsabile per i rapporti con gli organi competenti;

2) organizzare una squadra di tecnici, con il compito di garantire ininterrottamente l'operatività del CERT;

11) predisporre criteri di formazione del personale degli enti privati:

a) con regolamento emanato con decreto del Presidente della Repubblica, su proposta dei Ministri delle attività produttive e dell'istruzione, dell'università e della ricerca, entro un anno dalla data di entrata in vigore della presente legge, sono disciplinati:

1) l'organizzazione di corsi di formazione di base sulla sicurezza cibernetica presso le Camere di commercio, industria, artigianato e agricoltura sotto la supervisione formativa dell'Alta scuola;

2) la pubblicazione di materiali informativi e la predisposizione di corsi di formazione sulla sicurezza cibernetica fruibili tramite la rete internet;

p) definire le regole di sovranità cibernetica prevedendo:

1) una certificazione delle aziende cibernetiche secondo i seguenti princìpi:

a) presso la Presidenza del Consiglio dei ministri è istituito l'elenco delle imprese certificate per lo sviluppo negli ambiti cibernetici ai fini del mantenimento della sovranità cibernetica. A tali imprese spetta, in via prioritaria, l'accesso alle risorse del Fondo di cui alla lettera *u)*. La certificazione delle aziende è effettuata dal CERT-Nazionale;

2) una definizione di sistemi operativi e *software antivirus* per le infrastrutture strategiche secondo i seguenti principi:

a) entro cinque anni dalla data di entrata in vigore della presente legge, L'ANSC, in collaborazione con il Ministero dello sviluppo economico, provvede, anche mediante accordi con le imprese certificate, alla realizzazione di un sistema operativo sovrano, basato su codice libero e aperto, da utilizzare nelle IS informatiche. Il sistema operativo è mantenuto e aggiornato costantemente;

b) entro tre anni dalla data di entrata in vigore della presente legge, il Ministero dello sviluppo economico provvede, anche mediante accordi con le imprese certificate, alla realizzazione di un *software antivirus* di protezione sovrano, da utilizzare nelle IS informatiche, distribuito in forma gratuita. Il software è mantenuto e aggiornato costantemente.Pag. 161

c) la certificazione della sicurezza cibernetica dei software prodotti in Italia è rilasciata dall'ISCOM, su richiesta del produttore. Il rilascio della certificazione è soggetto al pagamento di un contributo nella misura determinata e aggiornata con decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dello sviluppo economico;

3) una definizione di *hardware* e *firmware* secondo i seguenti principi:

a) entro dieci anni dalla data di entrata in vigore della presente legge, il Ministero dello sviluppo economico provvede, anche mediante accordi con le imprese certificate, allo sviluppo di un sistema sovrano di comunicazione e re-indirizzamento dei dati internet (IP), costituito da componenti progettati e prodotti in Italia, da utilizzare nelle IS informatiche. Il sistema è mantenuto e aggiornato costantemente utilizzando componenti prodotti esclusivamente da imprese certificate;

b) la certificazione relativa alla sicurezza cibernetica degli *hardware* e dei *firmware* prodotti in Italia è rilasciata dall'ISCOM, su richiesta del produttore. Il rilascio della certificazione è soggetto a un contributo nella misura determinata e aggiornata con decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dello sviluppo economico;

4) una disciplina della Ricerca e sviluppo nel settore cibernetico:

a) il Governo predispone un piano per la ricerca e lo sviluppo nel settore cibernetico, la cui attuazione inizia entro un anno dalla data di entrata in vigore della presente legge, in collaborazione con l'ISCOM e con le università. All'attuazione del piano partecipano, ove possibile, le imprese certificate;

b) il Ministro della difesa, anche in collaborazione con le imprese certificate, redige un piano per la ricerca e lo sviluppo di contromisure cibernetiche in ambito militare;

c) l'attuazione del piano di cui al comma 1 è finanziata a valere sul Fondo di cui alla lettera *t)*;

5) disciplinare le *Start-up* e la proprietà intellettuale:

a) al fine di incrementare la capacità di sviluppo industriale del settore cibernetico nazionale, le imprese start-up innovative, come definite dall'articolo 25 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, possono accedere alle risorse del Fondo di cui all'articolo 48, secondo le modalità stabilite dal decreto del Presidente del Consiglio dei ministri adottato ai sensi del medesimo articolo;

b) le imprese di cui alla lettera *a)* sono esonerate dal pagamento dei diritti e di ogni altro onere dovuto per la registrazione dei brevetti relativi ai progetti cibernetici da esse realizzati;

q) disciplinare il controllo parlamentare secondo i seguenti principi:

1) prevedere il parere delle Commissioni parlamentari conformemente ai seguenti princìpi:

a) gli schemi dei decreti previsti dalla presente legge trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti per materia, con le modalità e nelle forme stabilite dai Regolamenti delle Camere. Il termine per l'espressione del parere è di trenta giorni dalla richiesta. Ove tale termine decorra senza che le Commissioni si siano pronunciate i decreti sono comunque emanati;

b) gli schemi delle LGC previste dalla presente legge sono trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti per materia. Il termine per l'espressione del parere è di trenta giorni dalla trasmissione. Decorso tale termine, le LGC possono essere comunque adottate;Pag. 162

2) prevedere una riforma del Comitato parlamentare per la sicurezza della Repubblica secondo i seguenti principi:

a) il Comitato parlamentare per la sicurezza della Repubblica, di cui all'articolo 30 della legge 3 agosto 2007, n. 124, esercita il controllo parlamentare sull'attività del sistema nazionale di sicurezza cibernetica, verificando che essa si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni;

b) Oltre alle audizioni previste dall'articolo 31 della legge 3 agosto 2007, n. 124, il Comitato parlamentare per la sicurezza della Repubblica ascolta periodicamente il direttore del ANSC e il vicedirettore dell'ANSC, il direttore del CERT-IT e il comandante del CERT-Difesa;

r) aggiornare la disciplina della tutela della riservatezza prevedendo che:

1) il Garante per la protezione dei dati personali può disporre, ai sensi dell'articolo 157 del codice di cui al decreto legislativo 30 giugno 2003, n. 196, accessi a banche di dati e archivi nonché ispezioni e verifiche nei luoghi ove si svolge il trattamento di dati inerenti alla sicurezza cibernetica;

s) disciplinare la divulgazione e la pubblicità secondo i seguenti princìpi:

1) entro il 31 dicembre di ogni anno il Presidente del Consiglio dei ministri presenta alle Camere una relazione sulla sicurezza cibernetica. La relazione è predisposta dal Presidente del Consiglio dei ministri, di concerto con il Direttore dell'ANSC e il Ministro della Difesa, ed è integrata con i pertinenti elementi di valutazione trasmessi dagli organi competenti;

2) il CERT-IT pubblica nel proprio sito internet istituzionale, in formato aperto e con aggiornamento almeno giornaliero, i dati relativi agli eventi cibernetici non classificati. Agli oneri derivanti si provvede a carico del Fondo di cui alla lettera *t)*;

t) predisporre un Fondo per la sicurezza cibernetica istituito secondo i seguenti principi:

1) è istituito nello stato di previsione del Ministero dell'economia e delle finanze, per il successivo trasferimento al bilancio autonomo della Presidenza del Consiglio dei ministri, il Fondo per la sicurezza cibernetica;

2) con decreto del Presidente del Consiglio dei ministri, da emanare entro sessanta giorni dalla data di entrata in vigore della presente legge, di concerto con il Ministro della difesa, con il Ministro dello sviluppo economico, con il Ministro dell'interno, con il Ministro dell'istruzione, dell'università e della ricerca e con il Ministro dell'economia e delle finanze, sono definite le modalità di impiego del fondo di cui al comma 1;

u) disciplinare l'approvvigionamento di servizi, lavori, materiali e strumenti del sistema nazionale di sicurezza cibernetica secondo i seguenti principi:

1) al fine di assicurare il funzionamento ottimale e ininterrotto del sistema nazionale di sicurezza cibernetica, gli organi che lo compongono procedono a un'attenta e puntuale programmazione a medio e a lungo termine degli approvvigionamenti di servizi, lavori, materiali e strumenti necessari a tale fine;

2) in caso di situazioni di crisi che richiedano il rapido approvvigionamento di servizi, lavori, materiali e strumenti per evitare il rischio di interruzione del servizio o per provvedere all'integrazione della capacità operativa, gli organi che compongono il sistema nazionale di sicurezza cibernetica possono impiegare le procedure disciplinate dal decreto legislativo 15 novembre 2011, n. 208;

3) per l'approvvigionamento dei servizi, lavori, materiali e strumenti, nei casi di cui al numero 2, gli organi che Pag. 163compongono il sistema nazionale di sicurezza cibernetica, possono accedere alle risorse del Fondo di cui alla lettera *u)* per un importo complessivo, riferito a ciascun esercizio finanziario, non eccedente il 10 per cento dell'importo che l'organo stesso ha destinato all'approvvigionamento di servizi, lavori, materiali e strumenti nell'esercizio finanziario precedente e, comunque, non superiore a un milione di euro;

4) l'organo che utilizza risorse del Fondo di cui alla lettera *u)* ai sensi del numero 3 della presente lettera deve reintegrare l'importo ricevuto mediante versamento al Fondo, da effettuare entro il secondo esercizio finanziario successivo a quello in corso alla data del prelevamento:

v) prevedere un regime sanzionatorio secondo i seguenti principi:

1) introdurre il seguente articolo 280-*ter* del codice penale, in materia di terrorismo cibernetico:

«ART. 280-*ter*. – *(Terrorismo cibernetico)*. – Salvo che il fatto costituisca più grave reato, chiunque, per finalità di terrorismo, anche internazionale, di cui all'articolo 270-*sexies*, provoca un evento cibernetico rilevante, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi, è punito con la reclusione da cinque a dieci anni»;

2) relativamente alle sanzioni amministrative prevedere quanto segue:

a) agli enti privati di cui al numero 4, in caso di mancato adeguamento alle disposizioni del numero 8, si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 100 mila euro e non superiore a un milione di euro;

b) agli enti privati individuati ai sensi dell'articolo 5, commi 1 e 2, in caso di mancato adeguamento alle disposizioni del numero 8 e, ricorrendone le condizioni, del numero 11 si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 10 mila euro e non superiore a 100.000 euro;

3) agli enti di cui al numero 6, in caso di mancato adeguamento alle disposizioni del numero 9, si applicano le sanzioni previste dal codice in materia di protezione dei dati personali, di

cui al decreto legislativo 30 giugno 2003, n. 196;

4) in caso di violazione della disposizione del numero 8, si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 10 mila euro e non superiore a 100 mila euro per ciascuna segnalazione omessa o non inviata nel termine ivi previsto;

5) l'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui numeri 1,2 e 4 è il prefetto competente per territorio. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al numero 3 è il Garante per la protezione dei dati personali. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689. I proventi delle sanzioni irrogate ai sensi dei numeri 1, 2 e 4 sono versati all'entrata del bilancio dello Stato per essere riassegnati al Fondo di cui alla lettera *t)*;

z) prevedere che agli oneri derivanti dall'attuazione delle disposizioni della presente legge si provvede mediante corrispondente riduzione del fondo di cui all'articolo 1, comma 965, della legge 28 dicembre 2015, n. 208;

zz) predisporre l'abrogazione del decreto del Presidente del Consiglio dei Ministri del 17 gennaio 2017, pubblicato nella *Gazzetta Ufficiale* n. 87 del 13 aprile 2017 e che l'ANSC subentra nella titolarità delle convenzioni stipulate da enti pubblici, ad eccezione degli enti istituiti dalla Pag. 164legge 124/2007, con enti privati e Università, in materia di sicurezza cibernetica.

5. 01. Artini, Baldassarre, Bechis, Segoni, Turco.

ART. 8.

Al comma 3, dopo la lettera h), *inserire la seguente:*

«h-bis) nell'ambito delle competenze ad essa attribuite, prevedere in capo all'autorità di vigilanza designata l'obbligo di riferire in Parlamento annualmente, con particolare riguardo ai controlli effettuati e alle sanzioni amministrative comminate».

8. 1. Galgano, Mazziotti di Celso.

Al comma 3, dopo la lettera l) *aggiungere la seguente: «m)* nell'ambito delle competenze ad essa attribuite, prevedere in capo all'autorità di vigilanza designata l'obbligo di riferire in Parlamento con cadenza semestrale, con particolare riguardo ai controlli effettuati e alle sanzioni amministrative comminate».

8. 2. Battelli.

ART. 9.

Al comma 3, dopo la lettera g), aggiungere la seguente:

«g-bis) nell'ambito delle competenze ad essa attribuite, prevedere in capo all'autorità di vigilanza designata l'obbligo di riferire in Parlamento annualmente, con particolare riguardo ai controlli effettuati e alle sanzioni amministrative comminate».

9. 1. Galgano, Mazziotti di Celso.

Al comma 3, dopo la lettera g) *aggiungere la seguente: g-bis*. nell'ambito delle competenze ad essa attribuite, prevedere in capo all'autorità di vigilanza designata l'obbligo di riferire in Parlamento con cadenza semestrale, con particolare riguardo ai controlli effettuati e alle sanzioni amministrative comminate.

9. 2. Battelli.

ART. 10.

Dopo l'articolo 10, inserire il seguente:

ART. 10-*bis.*
(Introduzione e reintroduzione di specie animali e vegetali).

1. Il Ministero dell'ambiente e della tutela del territorio e del mare, sentiti il Ministero delle politiche agricole alimentari e forestali e il Ministero della salute, per quanto di competenza, e la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, previo parere dell'istituto superiore per la protezione e la ricerca ambientale, stabilisce, con proprio decreto, le linee guida per la reintroduzione e il ripopolamento delle specie autoctone di cui all'allegato D annesso al regolamento di cui al decreto del Presidente della Repubblica 8 settembre 1997, n. 357, e successive modificazioni, e delle specie di cui all'allegato 1 della direttiva 2009/ 147/CE del Parlamento europeo e del Consiglio, del 30 novembre 2009, nonché per l'introduzione in deroga a quanto disposto dal comma 3 del presente articolo, nel rispetto delle finalità del citato regolamento di cui al decreto del Presidente della Repubblica 8 settembre 1997, n. 357, e della salute e del benessere delle specie, tenendo conto di quanto disposto dal regolamento (CE) n. 708/2007 del Consiglio, dell'11 giugno 2007.

2. Le regioni e le province autonome di Trento e di Bolzano, nonché gli enti di gestione delle aree protette nazionali, sentiti gli enti locali interessati e dopo un'adeguata consultazione del pubblico interessato dall'adozione del provvedimento di reintroduzione o di ripopolamento sulla Pag. 165base delle linee guida di cui al comma 1, autorizzano la reintroduzione o il ripopolamento delle specie di cui al citato comma 1, dandone comunicazione al Ministero dell'ambiente e della tutela del territorio e del mare, al Ministero delle politiche agricole alimentari e forestali e al Ministero della salute, nonché presentando agli stessi Ministeri un apposito studio che evidenzi che tale reintroduzione o ripopolamento contribuisce in modo soddisfacente al conseguimento delle finalità di cui all'articolo 1, comma 2, del regolamento di cui al decreto del Presidente della Repubblica 8 settembre 1997, n. 357.

3. È vietata l'introduzione in natura di specie e di popolazioni non autoctone. Tale divieto si applica anche nei confronti di specie e di popolazioni autoctone quando la loro introduzione interessa porzioni di territorio esterne all'area della loro presenza naturale.

4. Su istanza delle regioni e delle province autonome di Trento e di Bolzano, nonché degli enti di gestione delle aree protette nazionali.

L'introduzione delle specie e delle popolazioni di cui al comma 3 può essere autorizzata in deroga dal Ministero dell'ambiente e della tutela del territorio e del mare, di concerto con il Ministero delle politiche agricole alimentari e forestali e con il Ministero della salute, per quanto di competenza, previo parere dell'istituto superiore per la protezione e la ricerca ambientale, per motivate ragioni di rilevante interesse pubblico, connesse ad esigenze ambientali, economiche, sociali e culturali, nel rispetto della salute e del benessere delle specie autoctone.

5. Per l'introduzione e la traslocazione di specie e di popolazioni faunistiche alloctone per l'impiego ai fini di acquacoltura si applica il regolamento (CE) n. 708/2007 del Consiglio, dell'11 giugno 2007.

6. L'autorizzazione di cui al comma 4 è subordinata alla valutazione di uno specifico studio, comprendente un'analisi dei rischi ambientali, predisposto dai soggetti privati ovvero dagli enti territoriali richiedenti, i quali vi provvedono con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che evidenzi l'assenza di pregiudizi per le specie e gli habitat naturali. Qualora lo studio evidenzi l'inadeguatezza delle informazioni scientifiche disponibili, devono essere applicati principi di prevenzione e di precauzione, compreso il divieto dell'introduzione.

I risultati degli studi di valutazione effettuati sono comunicati al Comitato previsto dall'articolo

20 della direttiva 92/43/CEE del Consiglio, del 21 maggio 1992, e successive modificazioni.

7. Nel decreto di cui al comma 1 è specificata la procedura per l'autorizzazione in deroga al divieto di cui al comma 3.

8. Il Governo provvede ad apportare le modifiche necessarie all'articolo 12 del regolamento di cui al decreto del Presidente della Repubblica 8 settembre 1997, n. 357, e successive modificazioni.

10. 01. Taricco.

(Inammissibile)

ART. 14.

Al comma 1, lettera a) *sopprimere le parole da:* prendendo come riferimento *fino alla fine della lettera.*

14. 2. Coppola.

Al comma 1, lettera b), *dopo le parole:* linee guida nazionali *aggiungere le seguenti:* avvalendosi dell'Agenzia per l'Italia Digitale (AglD).

14. 1. Coppola.

Al comma 1, lettera b) *sopprimere gli ultimi due periodi.*

14. 3. Coppola.