D.P.C.M. 06/11/2015, n. 5/2015
Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva. (Decreto n. 5/2015).
Pubblicato nella Gazz. Uff. 5 dicembre 2015, n. 284, S.O.

Art. 14. Compiti del legale rappresentante o del Funzionario alla sicurezza della sede principale od unica dell'operatore economico

1. Il legale rappresentante, o, se delegato, il Funzionario alla sicurezza della sede principale o unica dell'operatore economico:

a) ha l'obbligo di conoscere le disposizioni in materia di protezione e tutela delle informazioni classificate o coperte da segreto di Stato, e di farle puntualmente applicare;

b) segnala tempestivamente all'UCSe e all'ente appaltante o al committente ogni elemento suscettibile di valutazione ai fini di cui all'art. 37, 47 e 48, nonché eventuali casi di sospetta o accertata compromissione delle informazioni classificate;

c) dirige, coordina e controlla tutte le attività che riguardano la protezione e la tutela delle informazioni, dei documenti e dei materiali classificati o coperti da segreto di Stato, trattati nell'ambito dell'operatore economico, sia a livello centrale che periferico;

d) assicura il controllo delle lavorazioni classificate o coperte da segreto di Stato e la salvaguardia delle stesse dall'accesso di personale non in possesso di abilitazione di sicurezza di livello adeguato e, comunque, non autorizzato;

e) comunica semestralmente all'UCSe le lavorazioni classificate in corso di esecuzione secondo le modalità previste dalle direttive di attuazione;

f) comunica all'UCSe i contratti classificati di cui l'impresa è affidataria;

g) coordina i servizi di sorveglianza e controllo delle infrastrutture COMSEC e dei CIS;

h) cura gli adempimenti relativi al rilascio dei NOS al personale dell'operatore economico che ha necessità di trattare informazioni classificate a livello RISERVATISSIMO o superiore;

i) comunica all'UCSe ogni variazione riguardante la legale rappresentanza, i componenti del Consiglio di amministrazione, il direttore tecnico, l'Organizzazione di sicurezza e le relative preposizioni, il possesso di quote di partecipazione qualificate in rapporto al capitale sociale;

l) istruisce il personale abilitato alla trattazione di informazioni classificate sulle disposizioni che regolano la materia;

m) comunica all'UCSe ogni evento che possa costituire minaccia alla sicurezza e alla tutela delle informazioni classificate;

n) assicura la corretta osservanza delle procedure relative alle visite da parte di persone estranee all'operatore economico nei siti dove sono trattate informazioni classificate;

o) chiede l'autorizzazione prevista dalle norme vigenti e cura i relativi aspetti di sicurezza inerenti le trattative contrattuali che prevedono la cessione di informazioni classificate.

2. Per lo svolgimento dei compiti di cui al comma 1 la Scuola di formazione del Dipartimento delle informazioni per la sicurezza, d'intesa con l'Ufficio centrale per la segretezza, organizza appositi corsi in materia di protezione e tutela delle informazioni classificate, a diffusione esclusiva, o coperte da segreto di Stato. A tali corsi possono essere ammessi anche altri dirigenti o dipendenti dell'operatore economico.

D.P.C.M. 24/01/2013
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica

nazionale.
Pubblicato nella Gazz. Uff. 19 marzo 2013, n. 66.

IL PRESIDENTE DEL CONSIGLIO DEI Ministri

Vista la *legge 3 agosto 2007, n. 124* , recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla *legge 7 agosto 2012, n. 133* , e, in particolare, l' *art. 1* , comma 3-bis, che dispone che il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, adotti apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, e l' *art. 38* , comma 1-bis, ai sensi del quale il Governo allega alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, che presenta annualmente al Parlamento, un documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica;

Visto l' *art. 4, comma 3, lett. d-bis) della citata legge 3 agosto 2007, n. 124* , ai sensi del quale il Dipartimento delle informazioni per la sicurezza coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

Visto l' *articolo 1 della legge 1° aprile 1981, n. 121* ;

Visti il *decreto-legge 27 luglio 2005, n. 144* , convertito, con modificazioni, dalla *legge 31 luglio 2005, n. 155* , recante misure urgenti per il contrasto del terrorismo internazionale che, all' *articolo 7-bis* , dispone che, ferme restando le competenze dei Servizi di informazione per la sicurezza, i competenti organi del Ministero dell'interno assicurano i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale ed il *decreto del Ministro dell'interno 9 gennaio 2008* , con il quale sono state individuate le predette infrastrutture ed è stata prevista l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche;

Visti l' *art. 14 del decreto legislativo 30 luglio 1999, n. 300* , recante "Riforma dell'organizzazione del Governo, a norma dell' *articolo 11 della legge 15 marzo 1997, n. 59* ", che attribuisce, tra l'altro, al Ministero dell'interno competenze in materia di difesa civile ed il decreto del Ministro dell'interno 28 settembre 2001 che istituisce la Commissione interministeriale tecnica di difesa civile;

Visti il *decreto legislativo 15 marzo 2010, n. 66* , recante "Codice dell'ordinamento militare" e, in particolare, l' *art. 89* che individua le attribuzioni delle Forze armate e le disposizioni e direttive conseguenti che disciplinano i compiti attinenti alla difesa cibernetica;

Visto il *decreto legislativo 1° agosto 2003, n. 259* , recante "Codice delle comunicazioni elettroniche" e, in particolare, le disposizioni che affidano al Ministero dello sviluppo economico competenze in materia di sicurezza ed integrità delle reti pubbliche di comunicazione e dei servizi di comunicazione elettronica accessibili al pubblico;

Visto il *decreto-legge 22 giugno 2012, n. 83* , convertito, con modificazioni, dalla *legge 7 agosto 2012, n. 134* , che ha istituito l'Agenzia per l'Italia digitale, cui sono affidate, tra l'altro, le funzioni attribuite all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione in materia di sicurezza delle reti, nonché quelle di coordinamento, indirizzo e regolazione già affidate a DigitPA;

Visto il *decreto legislativo 7 marzo 2005, n. 82* , recante il Codice dell'amministrazione digitale e, in particolare, le disposizioni in materia di sicurezza informatica;

Visto il decreto interministeriale 14 gennaio 2003, così come modificato dal decreto 5 settembre 2011, che ha istituito l'Osservatorio per la sicurezza delle reti e la tutela delle comunicazioni;

Vista la *legge 24 febbraio 1992, n. 225* , recante "Istituzione del Servizio nazionale della protezione civile";

Visto il *decreto legislativo 11 aprile 2011, n. 61* , attuativo della *direttiva 2008/114/CE* recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione;

Visto l' *art. 5, comma 2, lett. h), della legge 23 agosto 1988, n. 400* ;

Visto il *decreto legislativo 30 luglio 1999, n. 303* , recante "Ordinamento della Presidenza del Consiglio dei Ministri a norma dell' *articolo 11 della legge 15 marzo 1997, n. 59* ";

Visto il *decreto del Presidente del Consiglio dei Ministri 1° ottobre 2012* , recante "Ordinamento delle strutture generali della Presidenza del Consiglio dei Ministri";

Visto il *decreto del Presidente del Consiglio dei Ministri 5 maggio 2010* , recante l'Organizzazione nazionale per la gestione di crisi;

Vista la mozione approvata in data 23 maggio 2012, con la quale il Parlamento ha impegnato il Governo a porre in essere ogni idonea iniziativa per giungere alla costituzione presso la Presidenza del Consiglio dei Ministri di un Comitato interministeriale con il compito di elaborare una strategia nazionale per la sicurezza dello spazio cibernetico, di definire gli indirizzi generali e le direttive da perseguire nel quadro della politica nazionale ed internazionale in tale settore e di individuare, infine, gli interventi normativi ritenuti necessari;

Ritenuto che, in ragione delle caratteristiche della minaccia cibernetica quale rischio per la sicurezza nazionale, sia necessario definire un quadro strategico nazionale, con la specificazione dei ruoli che le diverse componenti istituzionali devono esercitare per assicurare la sicurezza cibernetica del Paese e la predisposizione di meccanismi e procedure di azione secondo un approccio interdisciplinare e coordinato, su più livelli, che coinvolga tutti gli attori pubblici, ferme restando le attribuzioni previste dalla normativa vigente per ciascuno di essi, nonché gli operatori privati interessati;

Ritenuto altresì necessario creare le condizioni, attraverso la definizione e precisazione di compiti ed attività delle diverse componenti istituzionali ed anche con l'individuazione di organi nazionali di riferimento per la sicurezza cibernetica in grado di interagire con le corrispondenti autorità estere, affinché l'Italia possa partecipare pienamente ai diversi consessi di cooperazione internazionale, sia in ambito bilaterale e multilaterale, sia dell'UE e della NATO;

Considerato l'attuale quadro legislativo, improntato alla distribuzione di funzioni e compiti aventi rilievo per la sicurezza cibernetica tra molteplici soggetti istituzionali competenti nelle diverse fasi della prevenzione degli eventi dannosi nello spazio cibernetico; dell'elaborazione di linee guida e standard tecnici di sicurezza; della difesa dello Stato da attacchi nello spazio cibernetico; della prevenzione e repressione dei crimini informatici;

della preparazione e della risposta nei confronti di eventi cibernetici;

Ritenuto che, sulla base del citato dato normativo, la definizione di un quadro strategico nazionale in materia di sicurezza cibernetica debba procedere secondo un percorso di graduale e progressiva razionalizzazione di ruoli, strumenti e procedure con l'obiettivo di accrescere la capacità del Paese di assicurare la sicurezza dello spazio cibernetico, ove necessario anche con interventi di carattere normativo;

Ritenuto che, nell'immediato, debbano essere create le condizioni perché, a legislazione vigente, possa essere sviluppata un'azione integrata che metta a fattor comune le diverse attribuzioni istituzionali delineate dal quadro normativo, ed inoltre assicuri, in una logica di partenariato, il pieno apporto, nel rispetto di quanto previsto dalla normativa vigente, anche delle competenze proprie degli operatori privati, interessati alla gestione di sistemi e reti di interesse strategico;

Ravvisata a tali fini la necessità di impartire indirizzi affinché venga a delinearsi un'architettura istituzionale basata sulla chiara individuazione dei soggetti chiamati ad intervenire e dei compiti ad essi affidati, nel rispetto delle competenze già attribuite dalla legge alle diverse componenti e dei meccanismi di interazione tra di esse;

Ritenuto che tale architettura debba svilupparsi su tre distinti livelli d'intervento, di cui il primo di indirizzo politico e coordinamento strategico, cui affidare l'individuazione degli obiettivi funzionali a garantire la protezione cibernetica e la sicurezza informatica nazionali, anche attraverso l'elaborazione di un Piano nazionale per la sicurezza dello spazio cibernetico, e che tale livello debba anche sovraintendere allo studio e alla predisposizione di proposte di intervento normativo che agevolino il raggiungimento dei citati obiettivi; il secondo di supporto, a carattere permanente, con funzioni di raccordo nei confronti di tutte le Amministrazioni ed enti competenti, ai fini dell'attuazione degli obiettivi e delle linee di azione indicate dalla pianificazione nazionale e che provveda, al contempo, a programmare l'attività operativa a livello interministeriale e ad attivare le procedure di allertamento in caso di crisi; il terzo livello, di gestione delle crisi, con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate;

Ritenuto che, nel quadro del livello di supporto all'attuazione della pianificazione nazionale, debbano essere disciplinate in maniera peculiare, tenuto conto della loro specificità, le attività di informazione per la sicurezza con l'obiettivo di potenziare le attività di ricerca informativa e di analisi finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica, facendo ricorso agli strumenti ed alle procedure di cui alla *legge n. 124/2007* e, in particolare, alle direttive del Presidente del Consiglio ai sensi dell' *art. 1* , comma 3-bis;

Ritenuto che il modello organizzativo-funzionale così delineato debba assicurare il pieno raccordo, in particolare, con le funzioni del Ministero dello sviluppo economico e dell'Agenzia per l'Italia digitale, nonché con l'attività e le strutture di difesa dello spazio cibernetico del Ministero della difesa, con quelle del Ministero dell'interno, dedicate alla prevenzione e al contrasto del crimine informatico e alla difesa civile, e con quelle della protezione civile;

Considerato che la legge attribuisce al Comitato interministeriale per la sicurezza della Repubblica (CISR) di cui all' *articolo 5 della legge n. 124/2007* compiti di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza, nonché di elaborazione degli indirizzi generali e degli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza e che, in particolare, ai sensi dell' *art. 1* , comma 3-bis, della predetta legge, introdotto dalla *legge n. 133/2012* , il CISR è sentito ai fini dell'adozione da parte del Presidente del Consiglio dei Ministri delle direttive in materia di sicurezza cibernetica;

Ravvisata l'esigenza di dover assicurare, nella materia della sicurezza cibernetica, un solido e affidabile meccanismo di raccordo tra la politica dell'informazione per la sicurezza e gli altri ambiti di azione che vengono in rilievo nella specifica materia, e di dovere per questo concentrare in un unico organismo interministeriale l'organo di indirizzo politico e di coordinamento strategico nel campo della sicurezza cibernetica;

Ritenuto in considerazione dei compiti attribuiti dalla legge al CISR e della composizione del Comitato, di individuare tale organismo interministeriale nello stesso CISR, attribuendogli, ai sensi dell' *art. 5, comma 2, lett. h) della legge 23 agosto 1988, n. 400* , i compiti suindicati;

Ritenuto che il CISR, nell'esercizio delle citate funzioni, debba essere adeguatamente e costantemente supportato da una attività istruttoria, di approfondimento e di valutazione e che a tali fini il Comitato interministeriale possa avvalersi dell'organismo collegiale di coordinamento istituito presso il DIS, ai sensi dell' *art. 4, comma 5, del D.P.C.M. 26 ottobre 2012, n. 2*, recante l'organizzazione ed il funzionamento del Dipartimento delle informazione per la sicurezza;

Ritenuto altresì che per un efficace assolvimento dei compiti attribuiti al CISR sia necessario assicurare un qualificato contributo di carattere scientifico di informazione, di valutazione e

di proposta e che, per questo, appare opportuno istituire presso la Scuola di formazione del DIS un organo dedicato, cui affidare anche compiti funzionali alla promozione e diffusione di una cultura della sicurezza cibernetica;

Ravvisata la necessità, ai fini dell'attuazione delle linee di intervento contenute nel Piano nazionale di sicurezza dello spazio cibernetico, in particolare per ciò che riguarda la preparazione e la pianificazione interministeriale per la gestione delle crisi, che parallelamente alle attività di acquisizione informativa e di analisi demandate agli organismi informativi di cui alla *legge n. 124/2007* , le attività delle diverse Amministrazioni ed enti svolte secondo le previsioni normative trovino una sede di raccordo che agevoli e favorisca lo svolgimento in forma coordinata delle attribuzioni di ciascuna componente;

Ritenuto a tale scopo, di prevedere la costituzione in via permanente di un Nucleo per la sicurezza cibernetica, da istituire presso l'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri;

Ritenuto infine, che una ulteriore e specifica esigenza di coordinamento si ponga con riguardo alla gestione operativa delle crisi e all'adozione delle misure necessarie al ripristino della funzionalità dei sistemi, richiedendo la chiara definizione di ruoli e procedure in modo da garantire un processo decisionale unitario e, al contempo, l'interazione degli organi nazionali preposti alla gestione dell'emergenza con gli omologhi organismi esistenti a livello internazionale, e che, per le suddette finalità, debba essere previsto un organo interministeriale da attivare in caso di crisi;

Ritenuto di individuare tale organo nel Nucleo interministeriale situazione e pianificazione di cui al *D.P.C.M. 5 maggio 2010* , prevedendone una configurazione, quale "Tavolo interministeriale di crisi cibernetica", funzionale all'ottimale gestione delle crisi di natura cibernetica, e di disporre che detto organo, per gli aspetti tecnici di computer emergency response, si avvalga del CERT nazionale istituito presso il Ministero dello sviluppo economico ai sensi del *decreto legislativo n. 259/2003* ;

Sentito il Comitato interministeriale per la sicurezza della Repubblica;

Dispone:
