Senato della Repubblica

Camera dei deputati

Schema di decreto legislativo recante attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

Atto del Governo n. 10

Schede di lettura

DOSSIER - XVIII LEGISLATURA

aprile 2018

Senato della Repubblica

SERVIZIO STUDI
TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi
Dossier n. 7

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-3855 - st_istituzioni@camera.it - @CD_istituzioni

Dipartimento Trasporti
Tel. 06 6760-2614 - st_trasporti@camera.it - @CD_trasporti

Ha collaborato l'Ufficio Rapporti con l'Unione europea

Atti del Governo n. 10

La redazione del presente dossier è stata curata dal Servizio Studi della Camera dei deputati

AC0087

I N D I C E

INTRODUZIONE

Lo schema di decreto legislativo contenuto nell'Atto del Governo n. 10 mira al recepimento della disciplina posta dalla direttiva (UE) 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 - *Network and Information Security*").

Tale disciplina è volta a conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".

In Italia, è stata delineata per la prima volta l'architettura strategica nazionale per la protezione cibernetica e la sicurezza informatica con il DPCM 24 gennaio 2013. Dandovi attuazione sono stati successivamente adottati il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica che contengono gli obiettivi strategici e operativi della *cyber security* italiana.

Da ultimo, nelle Gazzetta ufficiali del 17 febbraio e del 1° giugno 2017 sono stati, rispettivamente pubblicati il DPCM in materia di protezione cibernetica ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica relativo al 2017.

Lo schema di decreto legislativo in esame detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva 2016/1148.

In particolare, al **Presidente del Consiglio dei ministri** compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (**CISR**), della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

La qualifica di "**autorità competente NIS**" viene attribuita ai singoli ministeri in base ai settori di competenza (Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio) e, per taluni ambiti,

alle regioni e alle province autonome di Trento e di Bolzano. Tali autorità sono i soggetti competenti per settore (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) in materia di sicurezza delle reti e dei sistemi informativi; verificano, in particolare, l'applicazione della direttiva a livello nazionale ed individuano gli operatori di servizi essenziali nell'ambito dei criteri ivi definiti.

Presso la Presidenza del Consiglio dei ministri è istituito il **CSIRT-***Computer Emergency Response Team* italiano, con un contingente di 30 persone e lo stanziamento di specifiche risorse finanziarie, al quale sono attribuite – a decorrere dall'entrata in vigore del relativo decreto di organizzazione e funzionamento - le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

Viene designato il Dipartimento delle informazioni per la sicurezza (DIS) quale **punto di contatto unico**, organo incaricato a livello nazionale di coordinare·le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea.

L'**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione al quale è attualmente attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Gli **operatori di servizi essenziali**, ai fini dello schema di decreto legislativo, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS. Entro il 9 novembre 2018 le autorità competenti sono tenute ad identificare tali soggetti, ai fini del rispetto degli obblighi della direttiva.

Lo schema definisce inoltre gli **obblighi** in capo agli **operatori dei servizi essenziali e ai fornitori dei servizi digitali** con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III. E' posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e,

sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi.

Sono poi individuati i **poteri di controllo delle autorità NIS** sia nei confronti degli operatori di servizi essenziali, che dei fornitori di servizi digitali anche prevedendo poteri di verifica e di ispezione oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti.

Oltre alle notifiche obbligatorie lo schema, secondo quanto previsto dalla direttiva, disciplina le notifiche facoltative, effettuate cioè con riferimento a incidenti relativi a soggetti **che non sono stati identificati** come operatori di servizi essenziali e non sono fornitori di servizi digitali.

Ulteriori disposizioni concernono la giurisdizione, l'armonizzazione della normazione relativa alla sicurezza delle reti e dei sistemi informativi mediante l'adozione armonizzata di **norme e specifiche europee o accettate a livello internazionale** relative alla sicurezza della rete e dei sistemi informativi e le norme finanziarie.

La disposizione di delega e la direttiva 2016/1148

Lo schema di decreto legislativo è adottato in attuazione della disposizione di delega recata dall'articolo 1 della legge 25 ottobre 2017, n. 163 (*Legge di delegazione europea 2016-2017),* per il recepimento delle direttive elencate nell'allegato A, tra cui è ricompresa la direttiva 2016/1148.

E' previsto che gli schemi di decreto legislativo di recepimento delle ventotto direttive contenute nell'allegato A, siano essere preliminarmente sottoposti all'esame delle competenti Commissioni parlamentari per l'espressione del relativo **parere**.

Per quanto riguarda i **termini, le procedure, i princìpi e i criteri direttivi** della delega, è fatto rinvio alle disposizioni previste dagli articoli 31 e 32 della legge 24 dicembre 2012, n. 234.

L'articolo 31, comma 1, della legge n. 234 del 2012 dispone che il termine per l'esercizio delle deleghe conferite al Governo con la legge di delegazione europea sia di **quattro mesi antecedenti il termine di recepimento** indicato in ciascuna delle direttive . Per le direttive il cui termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, o scada nei tre mesi successivi, la delega deve essere esercitata entro **tre mesi dalla data di entrata in vigore della legge stessa**. Per le direttive che non prevedono un termine di recepimento, il termine per l'esercizio della delega è di dodici mesi dalla data di entrata in vigore della legge di delegazione europea.

L'articolo 31, comma 5, della legge n. 234 del 2012 prevede inoltre che il Governo possa adottare **disposizioni integrative e correttive** dei decreti legislativi emanati in base alla delega conferita con la legge di delegazione entro **24 mesi** dalla data di entrata in vigore di ciascun decreto legislativo, sempre nel rispetto dei princìpi e criteri direttivi fissati dalla legge stessa.

Il termine di recepimento della direttiva 2016/1148 è fissato – dall'art. 25 della medesima - al **9 maggio 2018**. La legge di delegazione europea è entrata in vigore il 21 novembre 2017 (quindi il termine del 9 gennaio 2018 per il relativo recepimento veniva a scadenza nei tre mesi successivi alla data del 21 novembre 2017) ed ha trovato dunque applicazione, per l'esercizio della delega legislativa, il termine di tre mesi dalla data di entrata in vigore della legge medesima fissato, quindi, al 21 febbraio 2018. Considerato che l'articolo 31, comma 3, della legge 234 del 2012 prevede che qualora il termine fissato per l'espressione del parere parlamentare scada nei trenta giorni che precedono il termine per l'esercizio della delega o **successivamente**, il termine per la delega è prorogato di tre mesi, il termine finale per l'esercizio della delega legislativa è fissato al **21 maggio 2018**.

I **princìpi e criteri direttivi generali di delega** indicati dall’articolo 32 della legge n. 234 del 2012 sono i seguenti:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture, secondo il principio della massima semplificazione dei procedimenti;

b) ai fini di un migliore coordinamento con le discipline vigenti sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione della normativa;

c) gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse (c.d. *gold plating*);

d) ove necessario, al fine di assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. In ogni caso le sanzioni penali sono previste "solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti";

e) al recepimento di direttive o di altri atti che modificano precedenti direttive o di atti già attuati con legge o con decreto legislativo si procede apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione;

f) nella redazione dei decreti legislativi si tiene conto delle eventuali modificazioni delle direttive comunque intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o comunque siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano le procedure per salvaguardare l'unitarietà dei processi decisionali, l’efficacia e la trasparenza dell’azione amministrativa, nel rispetto dei princìpi di sussidiarietà e delle competenze delle regioni e degli enti territoriali;

h) le direttive che riguardano le stesse materie o che comunque comportano modifiche degli stessi atti normativi vengono attuate con un unico decreto legislativo, compatibilmente con i diversi termini di recepimento;

i) è sempre assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.

Per quanto concerne il procedimento per il parere delle competenti Commissioni parlamentari, la disposizione segue lo schema procedurale disciplinato in via generale dall’articolo 31, comma 3, della legge 234 del 2012.

Esso prevede che gli schemi di decreto legislativo, una volta acquisiti gli altri pareri previsti dalla legge, siano trasmessi alle Camere per l'espressione del parere e che, decorsi **quaranta giorni dalla data di trasmissione**, i decreti siano emanati anche in mancanza del parere.

Come già ricordato, qualora il termine fissato per l'espressione del parere parlamentare scada nei trenta giorni che precedono il termine per l'esercizio della delega o successivamente, il termine per la delega è **prorogato di tre mesi**. Finalità di tale proroga è quella di permettere al Governo di usufruire in ogni caso di un adeguato periodo di tempo per l'eventuale recepimento nei decreti legislativi delle indicazioni emerse in sede parlamentare.

Il comma 9 del medesimo articolo 31 prevede altresì che ove il Governo **non intenda conformarsi ai pareri espressi dagli organi parlamentari** relativi a **sanzioni penali** contenute negli schemi di decreti legislativi, ritrasmette i testi alle Camere, con le sue osservazioni e con eventuali modificazioni. Decorsi venti giorni dalla data di ritrasmissione, i decreti sono emanati anche in mancanza di nuovo parere.

Alla copertura degli oneri recati dalle spese eventualmente previste nei decreti legislativi attuativi, nonché alla copertura delle minori entrate eventualmente derivanti dall'attuazione delle direttive, qualora non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, si provvede a carico del **Fondo per il recepimento della normativa europea**, di cui all'articolo 41-bis della legge n. 234/2012.

Gli oneri recati dal provvedimenti in titolo (articoli 7 e 8) – pari a 5 milioni di euro per il 2018 e a 3 milioni di euro a decorrere dal 2019 – si provvede, ai sensi dell'art. 22, nell'ambito di tale Fondo.

Lo stesso comma 3 prevede inoltre che, in caso di incapienza del Fondo per il recepimento della normativa europea, i decreti legislativi attuativi delle direttive dai quali derivano nuovi o maggiori oneri sono emanati solo successivamente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie, in conformità all'articolo 17, comma 2, della legge di contabilità e finanza pubblica (legge 31 dicembre 2009, n. 196).

È altresì previsto il parere delle **Commissioni parlamentari competenti anche per i profili finanziari** sugli schemi dei decreti legislativi in questione, come richiesto dall'articolo 31, comma 4, della legge 24 dicembre 2012, n. 234, che disciplina le procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea.

In particolare, il citato comma 4 dell'articolo 31 prevede che gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della **relazione tecnica**, ai sensi

dell’articolo 17, comma 3, della legge di contabilità pubblica (legge n. 196/2009). Su di essi è richiesto anche il parere delle Commissioni parlamentari competenti per i **profili finanziari**.

E’ previsto che il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, **ritrasmette** alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

La direttiva (UE) 2016/1148 in sintesi

La direttiva 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione (c.d. “Direttiva NIS”), rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza informatica.

Attraverso l’adozione da parte dei singoli Stati membri di una serie di misure strategiche e organizzative comuni in materia di sicurezza cibernetica, la direttiva mira a raggiungere un livello elevato di sicurezza dei sistemi, delle reti e delle informazioni in ambito europeo, nella convinzione che il rafforzamento del dominio digitale rappresenti un importante volano di crescita del sistema economico dell’Unione, incidendo, positivamente sulla propensione ad investire degli operatori economici, con particolare riferimento al commercio internazionale.

Nello specifico, la direttiva prevede l’adozione di una serie di iniziative da parte degli Stati membri volte a migliorare le capacità di sicurezza cibernetica dei singoli Paesi, aumentare il livello di collaborazione in ambito europeo nella prevenzione delle minacce cibernetiche e nelle eventuali misure di risposta ad attacchi cyber, sviluppare una cultura della sicurezza con particolare riferimento a quei settori vitali per l’economia e la società e che si basano sulle tecnologie dell’informazione e della comunicazione.

Relativamente al miglioramento delle capacità dei singoli Stati dell’Unione, la direttiva “fa obbligo a tutti gli Stati membri di adottare una **strategia nazionale** in materia di sicurezza della rete e dei sistemi informativi” (articoli 1 e 7), definendo, in particolare:

1. gli obiettivi strategici;
2. le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi;

3. gli operatori di servizi essenziali nei settori reputati essenziali dal punto di vista della sicurezza cibernetica.

Per l'individuazione degli **operatori essenziali** la direttiva fornisce alcuni criteri per la loro individuazione e fissa il termine del 9 novembre 2018.

In particolare, è qualificato come operatore di servizio essenziale il soggetto pubblico o privato che appartiene alle categorie elencate nell'allegato 2 della medesima direttiva (energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari), il quale fornisce un servizio reputato essenziale per il mantenimento di attività sociali e/o economiche fondamentali.

Si prevede, inoltre, che la fornitura di tale servizio dipenda dalla rete e dai sistemi informativi e che un eventuale incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Sempre con riferimento al miglioramento delle capacità di sicurezza cibernetica e alla cooperazione a livello europeo ed internazionale in materia di sicurezza delle reti e dei sistemi informativi la direttiva (artt.8 e 9) stabilisce l'obbligo per gli Stati membri di:

1. individuare **una o più autorità nazionali** in materia di sicurezza delle reti e dei sistemi informativi, con funzioni, tra le altre, di controllo circa l'applicazione della direttiva;
2. designare un **punto di contatto unico nazionale** in materia di sicurezza delle reti e dei sistemi informativi ("punto di contatto unico");
3. istituire **uno o più Gruppi di intervento** per la sicurezza informatica in caso di incidente (Computer Security Incident Response Team CSIRT) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti.

In particolare, il punto di contatto è tenuto a garantire la cooperazione transfrontaliera tra le autorità nazionali competenti in materia di sicurezza cibernetica e il gruppo di cooperazione, composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (*European Union for Network and Information Security Agency*). Il punto di contatto dovrà, altresì, svolgere un ruolo di coordinamento tra i richiamati organismi nazionali e la rete di *Computer Security Incident Response Team* formata da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

Spetta, invece, ai Gruppi di intervento per la sicurezza informatica (CSIRT), gestire gli incidenti e i rischi cibernetici secondo una procedura ben definita dai singoli ordinamenti.

A tal fine gli Stati membri devono garantire le necessarie risorse finanziarie.

In relazione alla tempistica, in base alla direttiva entro il mese di agosto 2017 i fornitori di servizi digitali sono stati chiamati ad adottare i requisiti minimi di sicurezza e di notifica degli incidenti.

Entro novembre 2018 ogni Stato membro dovrà identificare gli operatori di servizi essenziali.

Nel 2019 la Commissione europea valuterà la coerenza dell'identificazione degli operatori di servizi essenziali da parte degli Stati membri e nel 2021 verrà esaminato il funzionamento delle direttiva con particolare attenzione alla cooperazione strategica e operativa degli Stati e l'applicazione da parte dei gestori di servizi essenziali e dei fornitori di servizi digitali.

Evoluzione della normativa nazionale in materia di sicurezza cibernetica

Nel gennaio del 2013, anche sulla base di analoghe iniziative intraprese a livello europeo ed internazionale, il Governo ha adottato il **DPCM del 24 gennaio del 2013**, che, fino all'entrata in vigore del successivo DPCM del 17 febbraio 2017, ha definito l'architettura istituzionale "deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali".

Nel dicembre del medesimo anno, in attuazione di un'espressa disposizione contenuta nel DPCM del 2013, sono stati approvati il *Quadro Strategico nazionale per la sicurezza dello spazio cibernetico* e il *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*.

Nell'insieme questi documenti individuano, per la prima volta in maniera organica a livello nazionale, i compiti affidati a ciascuna componente istituzionale con competenze nel settore della sicurezza e della difesa cibernetica ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi.

Nello specifico, il sistema delineato dal DPCM 24 gennaio 2013 pone al vertice del potere decisionale il Presidente del Consiglio dei ministri e i Ministri facenti parte del Comitato per la sicurezza della Repubblica (CISR), a cui sono demandati i compiti di indirizzo politico-strategico. Ad essi, infatti, spetta la definizione della strategia nazionale di *cyber-security* nonché l'emanazione delle conseguenti direttive d'indirizzo. A supporto del Comitato interministeriale viene individuato un apposito organismo collegiale di coordinamento (articolo 5), presieduto dal Direttore generale del Dipartimento delle Informazioni per la Sicurezza (DIS).

A supporto del Presidente del Consiglio dei ministri, per gli aspetti relativi alla prevenzione e all'approntamento rispetto a situazioni di crisi, il DPCM del 2013 istituisce il Nucleo per la sicurezza cibernetica, costituito in via permanente presso l'Ufficio del Consigliere militare e da questi presieduto. Il Nucleo è altresì composto da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, 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 e dell'Agenzia per l'Italia digitale. Per gli aspetti relativi alla trattazione di informazioni classificate, il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

Nel **febbraio 2017** il Governo ha emanato una nuova direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale (**D.P.C.M 17 febbraio 2017**) che sostituisce integralmente la precedente direttiva del 2013.

Nel nuovo assetto strategico al **Presidente del Consiglio dei ministri viene affidata l'alta direzione** e la responsabilità generale della politica dell'informazione per la sicurezza. In tale funzione, egli provvede anche al coordinamento delle politiche dell'informazione per la sicurezza, impartisce le direttive e, sentito il CISR, emana le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema di sicurezza cibernetica.

Il DPCM, **nelle more del recepimento della direttiva NIS**, rafforza, in particolare, **il ruolo del CISR**, che emanerà direttive con l'obiettivo di innalzare il livello della sicurezza informatica del Paese e si avvarrà in questa attività del supporto del coordinamento interministeriale delle amministrazioni CISR tecnico e del DIS.

Nello specifico, con il nuovo DPCM è il direttore generale del DIS a dover adottare le iniziative idonee a definire le necessarie linee di azione per innalzare i migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati e avanzati supporti tecnologici. Per la realizzazione di tali iniziative, "è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore".

Sempre il Direttore del DIS è chiamato a predisporre gli opportuni moduli organizzativi, di coordinamento e di raccordo, prevedendo il ricorso anche a professionalità delle pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle università e di operatori economici privati.

Tra le novità c'è che il Nucleo Sicurezza Cibernetica (NSC), composto da rappresentanti dei ministeri principali, delle agenzie di *intelligence*, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale, viene ricondotto all'interno del DIS ed assicurerà la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale, in raccordo con tutte le strutture dei ministeri competenti in materia. Infatti, nel campo della prevenzione e della preparazione a eventuali situazioni di crisi cibernetica, spetta al Nucleo Sicurezza Cibernetica:

1. promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e curare l'elaborazione delle necessarie procedure di coordinamento interministeriale;
2. mantenere attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica;

3. valutare e promuovere procedure di condivisione delle informazioni, anche con gli operatori privati interessati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi;
4. acquisire le comunicazioni circa i casi di violazione o dei tentativi di violazione della sicurezza o di perdita dell'integrità dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal CNAIPIC, nonché dalle strutture del Ministero della difesa e dai CERT;
5. promuovere e coordinare, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale, per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica;
6. costituire il punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE e le altre organizzazioni internazionali e gli altri Stati, 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 interessate dalla normativa vigente, assicurando comunque in materia ogni necessario raccordo.

Nello specifico **campo dell'attivazione delle azioni di risposta e ripristino** rispetto a situazioni di crisi cibernetica, il Nucleo Sicurezza Cibernetica:

1. riceve, anche dall'estero, le segnalazioni di eventi cibernetici e dirama gli allarmi alle amministrazioni e agli operatori privati;
2. valuta se l'evento assuma dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richieda l'assunzione di decisioni coordinate in sede interministeriale;
3. informa tempestivamente il Presidente del Consiglio dei ministri, per il tramite del Direttore generale del DIS, sulla situazione in atto.

Il Nucleo riferisce direttamente al direttore generale del DIS per la successiva informazione al Presidente del Consiglio dei ministri e al Comitato interministeriale per la sicurezza della Repubblica (CISR).

A sua volta il CISR viene rafforzato anche alla luce di quanto già stabilito nella legge 11 dicembre 2015, n. 198. In particolare, al CISR viene assegnata la facoltà di emanare direttive al fine di innalzare il livello della sicurezza informatica del Paese, avvalendosi a tal fine del supporto del CISR Tecnico e del Dipartimento per le Informazioni e la Sicurezza (DIS).

Viene meno sia il Comitato Scientifico, sia il cosiddetto NISP, entrambe strutture tecniche precedentemente poste a supporto del CISR.

Lo spostamento del Nucleo per la sicurezza cibernetica dalla competenza dell'Ufficio del Consigliere militare di Palazzo Chigi a quella del Dipartimento delle informazioni per la sicurezza (DIS) sembra rispondere all'esigenza di una maggiore agilità della catena di comando e di un maggiore coordinamento con tutte le strutture istituzionali previste nel nuovo quadro strategico.

Infine è stato attribuito al Ministero dello sviluppo economico il compito di istituire un centro di valutazione e certificazione nazionale per la verifica dell'affidabilità della componentistica delle apparecchiature ICT (*Information and Communication Technology*) che vengono utilizzate da parte della pubblica amministrazione nelle strutture critiche e nelle strutture strategiche ed è stato inoltre previsto l'accesso alle banche dati dei soggetti privati e ai cosiddetti SOC *(security operation center*) dal parte del DIS, in modo tale da poter avere una visione unitaria del sistema[1].

[1] Per un approfondimento si rinvia al documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa dello spazio cibernetico condotta dalla IV Commissione della Camera dei deputati nel corso della XVII legislatura.

Articolo 1
(Oggetto e ambito di applicazione)

Finalità dello schema di decreto legislativo è quella di definire – dando attuazione alla direttiva 2016/1148 - misure "volte a conseguire un **livello elevato di sicurezza della rete e dei sistemi informativi** in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".

Nel preambolo della direttiva si evidenzia come le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano **affidabili e sicuri** per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno.

Si rileva inoltre come la portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una **grave minaccia** per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione europea.

A tal fine lo schema di decreto legislativo prevede:

a) l'inclusione nella **strategia nazionale** di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del decreto;

Si ricorda che la direttiva prevede l'obbligo, in primo luogo, per tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi. Lo schema di decreto legislativo, all'art. 6, affida al Presidente del Consiglio dei ministri l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), della **strategia nazionale di sicurezza cibernetica** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale che viene successivamente trasmessa alla Commissione europea.

b) la **designazione** delle autorità nazionali competenti e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale;

A tal fine, lo schema di decreto legislativo, all'art. 7, attribuisce ai **singoli ministeri** in base agli ambiti di competenza (Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio e, per taluni profili, alle regioni e

province autonome), la qualifica di **autorità competente NIS** - *Network and Information Security*.

Le autorità competenti NIS sono responsabili, ai sensi dell'art. 7, dell'attuazione del provvedimento, individuano gli operatori essenziali soggetti agli obblighi e vigilano sull'applicazione del decreto a livello nazionale esercitando altresì le relative potestà ispettive e sanzionatorie.

Individua inoltre il Dipartimento delle informazioni per la sicurezza (DIS) quale **punto di contatto** unico in materia di sicurezza delle reti e dei sistemi informativi.

Quale **Gruppo di intervento per la sicurezza informatica in caso di incidente** (**CSIRT**) in ambito nazionale lo schema di decreto legislativo istituisce - presso la Presidenza del Consiglio dei ministri - un nuovo organismo, il **CSIRT italiano**, al quale sono attribuite le funzioni attualmente svolte dal CERT nazionale e dal CERT-PA.

c) il rispetto di obblighi da parte degli **operatori di servizi essenziali** e dei **fornitori di servizi digitali** relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

Il Capo IV e il Capo V dello schema di decreto legislativo disciplinano gli obblighi in materia di scurezza e notifica in caso di incidenti, rispettivamente, per gli operatori di servizi essenziali e per i fornitori di servizi digitali.

d) la partecipazione nazionale al **gruppo di cooperazione europeo**, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea nonché dell'incremento della fiducia tra di essi;

L'art. 10 dello schema di decreto legislativo dispone la partecipazione del **punto di contatto** (individuato, come si è detto, dallo schema di decreto legislativo nel DIS) alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA). Tra le principali previsioni della direttiva vi è infatti quella di istituire un gruppo di cooperazione al fine di sostenere e agevolare la **cooperazione strategica** e lo **scambio di informazioni** tra Stati membri e di sviluppare la fiducia tra di essi.

All'art. 7 si specifica inoltre che il punto di contatto unico svolge una funzione di collegamento per garantire la **cooperazione transfrontaliera** delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione e la rete di CSIRT. Il punto unico di contatto è chiamato a collaborare nel gruppo di cooperazione "in modo effettivo, efficiente e sicuro" con i rappresentanti designati dagli altri Stati.

e) la partecipazione nazionale alla rete CSIRT "nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace".

A tal fine l'art. 11 dello schema di decreto legislativo disciplina l'attività del **CSIRT italiano nell'ambito della rete CISRT** composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE. Tra gli obblighi principali previsti dalla direttiva vi è infatti quello di crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace.

Si prevede che le disposizioni sulle misure di sicurezza e di notifica degli incidenti, previste dal provvedimento, **non si applicano**:

- alle imprese che forniscono **reti pubbliche di comunicazioni o servizi di comunicazione elettronica** accessibili al pubblico (soggette agli obblighi di cui agli articoli 16-*bis* e 16-*ter* del d. lgs. n. 259/2003, finalizzati a "conseguire un livello di sicurezza delle reti adeguato al rischio esistente, e di garantire la continuità della fornitura dei servizi su tali reti");
- ai fornitori di **servizi fiduciari** qualificati e non qualificati (soggetti agli obblighi di cui all'art. 19 del regolamento UE n. 910/2014), intendendo per "prestatore di servizi fiduciari qualificato", un "prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato".

E' fatto salvo quanto previsto dalla disciplina vigente, di attuazione di direttiva 2013/40/UE, riguardante l'individuazione e la designazione delle infrastrutture critiche europee e la relativa protezione.

Come stabilito dalla direttiva al medesimo art. 1 è inoltre previsto che lo **scambio di informazioni riservate** con la Commissione Europea e con le autorità competenti di altri Stati membri UE avvenga nel rispetto della **riservatezza** e della **sicurezza** nonché della **protezione degli interessi commerciali** delle imprese. Le informazioni scambiate devono essere in ogni caso "pertinenti e commisurate allo scopo".

Sono altresì impregiudicate le misure adottate per la salvaguardia delle funzioni essenziali dello Stato e, in particolare, di **tutela della sicurezza nazionale**, incluse le misure volte alla tutela delle informazioni, in particolare a fini di indagine, accertamento e perseguimento dei reati.

In presenza di uno specifico atto giuridico dell'Unione avente ad oggetto obblighi per le imprese su cui interviene lo schema di decreto legislativo, inoltre, tale atto continua ad applicarsi se gli obblighi in esso fissati sono almeno equivalenti a quelli del decreto.

Articolo 2
(Trattamento dei dati personali)

L’articolo 2 specifica che il trattamento dei dati personali in applicazione del decreto legislativo è effettuato ai sensi del **Codice per la protezione dei dati personali** di cui al decreto legislativo n. 196 del 2003.

Viene così data attuazione all’art. 2 della direttiva, che rimanda per il trattamento dei dati alla direttiva 95/46/CE, la cui disciplina è posta a fondamento del nostro Codice della privacy.

Peraltro, in merito, occorre ricordare che il 25 maggio 2018 entrerà in vigore il **regolamento UE 2016/679** - regolamento generale sulla protezione dei dati - che detta una nuova disciplina europea sul trattamento dei dati personali ed abroga proprio l’originaria direttiva del 1995.

L’entrata in vigore della riforma, che prevede un accesso più agevole ai dati, il diritto alla portabilità dei dati, un più chiaro 'diritto all'oblio'; il diritto di essere informati in caso di violazione dei dati, determinerà una sostanziale riscrittura del decreto legislativo n. 196 del 2003.

La legge di delegazione europea 2016-2017 (legge n. 163 del 2017) ha a tal fine delegato il Governo (art. 13) ad adottare uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del citato regolamento. In particolare, il Governo dovrà abrogare espressamente le disposizioni del codice della privacy incompatibili con il regolamento (UE) 2016/679 e modificare le restanti parti al fine di dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento. Il Governo dovrà, inoltre, adeguare, nell'ambito delle modifiche al codice, il sistema sanzionatorio penale e amministrativo vigente, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Il Consiglio dei Ministri del 21 marzo 2018 ha approvato uno schema di decreto legislativo, attuativo della delega, non ancora trasmesso alle Camere.

Articolo 3
(Definizioni)

L’art. 3 reca le **definizioni** ai fini del decreto legislativo, sulla base di quanto previsto dalla direttiva all’art. 4 e degli obblighi ivi stabiliti.

Tra i principali obblighi previsti dalla direttiva (art. 1) si ricordano:

- l’adozione di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;
- l’istituzione di un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;
- la creazione di una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace;
- la definizione di obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;
- la designazione di autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

Viene, in primo luogo, definita quale **autorità competente NIS**, l'autorità competente per settore in materia di sicurezza delle reti e dei sistemi informativi, che l'articolo 7, comma l attribuisce ai **singoli ministeri** in base agli ambiti di competenza (Ministero dello sviluppo economico, Ministero dell’economia e delle finanze, Ministero della salute e Ministero dell’ambiente e della tutela del territorio) e, per taluni ambiti, alle **regioni e province autonome**.

Viene definito il **CSIRT** quale gruppo di intervento per la sicurezza informatica in caso di incidente; a tal fine, ai sensi dell'articolo 8, è istituito presso la Presidenza del Consiglio dei ministri un nuovo organismo, il **CSIRT italiano**, al quale sono attribuite le funzioni del CERT nazionale e del CERT-PA.

Ai sensi dell’art. 11 dello schema di decreto legislativo, il CSIRT italiano partecipa alla rete CISRT composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

Il **punto di contatto unico** è definito quale organo incaricato a livello nazionale di coordinare· le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea ed individuato, dall’art. 7, nel Dipartimento delle informazioni per la sicurezza (DIS).

L’art. 10 dello schema di decreto legislativo dispone, tra l’altro, la partecipazione del **punto di contatto** (individuato, come si è detto, dallo schema di decreto legislativo nel DIS) alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell’Agenzia dell’UE per la sicurezza delle reti e dell’informazione (ENISA).

L’**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione al quale è attualmente attribuita – ai sensi dell'art. 7-*bis* del decreto-legge 27 luglio 2005, n. 144 – la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Sono quindi definiti la “rete e il sistema informativo” e la “sicurezza della rete e dei sistemi informativi” in corrispondenza con la direttiva.

Gli **operatori di servizi essenziali**, ai fini dello schema di decreto legislativo, sono i soggetti pubblici o privati, della tipologia prevista dall’elenco dell'allegato II (settori dell’energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS.

E’ prescritto che, **entro il 9 novembre 2018** – termine corrispondente a quello indicato dalla direttiva all’art. 5 - le autorità competenti NIS (quindi i ministeri competenti – v. *supra*) identifichino con propri provvedimenti, per ciascun settore e sotto-settore, gli operatori con sede nel territorio nazionale, secondo i seguenti criteri e tenuto conto dei documenti prodotti al riguardo dal Gruppo di cooperazione: un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o o economiche fondamentali; la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Si ricorda che la direttiva elenca i medesimi settori e sottosettori all’allegato II.

Sono quindi definiti il “**servizio digitale**” – nell’ambito delle seguenti tipologie: mercato *on line*, motore di ricerca on line e servizi di *cloud computing* - e il “**fornitore di servizio digitale**” in aderenza con la direttiva.

Per “**incidente**” si intende – in linea con la direttiva - ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi e per “**trattamento dell'incidente**”, tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e

l'intervento in caso di incidente. Per "**rischio**" ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

Sono quindi definite gli ambiti di **IXP, DNS e TLD**, richiamati nell'elenco delle **tipologie di operatori dei servizi essenziali** di cui all'allegato II.

Il punto di interscambio internet (IXP) è definito quale infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico.

Il sistema dei nomi di dominio (DNS), è un sistema distribuito e gerarchico di *naming* in una rete che inoltra le richieste dei nomi di dominio.

Si intende per registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD).

Sono infine definite le categorie ricomprese nell'allegato III tra le **tipologie di servizi digitali**.

Per **mercato *online*** si intende un servizio digitale che consente ai consumatori ovvero ai professionisti di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato on line.

Per **motore di ricerca *on line***, un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto.

Per **servizio di *cloud computing***, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

Articoli 4 e 5
(Identificazione degli operatori di servizi essenziali ed effetti negativi rilevanti)

Ai fini dello schema di decreto legislativo, gli **operatori di servizi essenziali** sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e dei trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), **individuati** dalle **autorità competenti NIS**.

Le autorità competenti NIS sono così individuate dall'art. 7 dello schema di decreto legislativo:

- il **Ministero dello sviluppo economico** per il settore energia, sotto-settori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD[2], nonché per i servizi digitali;
- il **Ministero delle infrastrutture e trasporti** per il settore trasporti, sotto-settori aereo, ferroviario, per vie d'acqua e su strada;
- il **Ministero dell'economia e delle finanze** per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, la Banca d'Italia e la·Consob, secondo modalità di collaborazione e di scambio di informazioni che saranno stabilite con decreto del Ministro dell'economia e delle finanze;
- il **Ministero della salute** per l'attività di assistenza sanitaria, intesa come "servizi prestati da professionisti sanitari a pazienti, al fine di valutare, mantenere o ristabilire il loro stato di salute, ivi compresa la prescrizione, la somministrazione e la fornitura di medicinali e dispositivi medici", prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e **le regioni e le province autonome**, direttamente o per il tramite delle autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria svolte dagli operatori

[2] Il punto di interscambio internet (IXP) è definito dall'art. 3 dello schema di decreto legislativo quale infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico.

Il sistema dei nomi di dominio (DNS), è un sistema distribuito e gerarchico di *naming* in una rete che inoltra le richieste dei nomi di dominio.

Si intende per registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD).

autorizzati e accreditati delle regioni o dalle province autonome negli ambiti territoriali di rispettiva competenza;

- il **Ministero dell'ambiente e della tutela del territorio e del mare** e le **regioni e le province autonome**, direttamente o per il tramite delle autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

Come stabilito dalla direttiva **entro il 9 novembre 2018** le autorità competenti NIS identificano, con propri provvedimenti, per ciascun settore e sotto-settore, gli operatori con sede nel territorio nazionale, sulla base di **specifici criteri** definiti in corrispondenza con le prescrizioni della direttiva:

- un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o o economiche fondamentali;

Qualora un soggetto fornisca un servizio di tale tipologia sul territorio nazionale e in altro o altri Stati membri dell'Unione europea, le autorità competenti NIS sono tenute a consultare le autorità competenti degli altri Stati membri prima dell'adozione dei provvedimenti di individuazione.

- la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
- un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Ai fini della determinazione della rilevanza degli effetti negativi è previsto che le autorità competenti NIS considerino i seguenti fattori intersettoriali: a) il **numero di utenti** che dipendono dal servizio fornito dal soggetto interessato; b) la **dipendenza di altri settori** di cui all'allegato Il dal servizio fornito da tale soggetto; c) **l'impatto** che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza; d) la **quota di mercato** di detto soggetto; e) **la diffusione geografica** relativamente all'area che potrebbe essere interessata da un incidente; f) l'importanza del soggetto per il mantenimento di un **livello sufficiente del servizio**, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio. Per la determinazione degli effetti negativi rilevanti di un incidente sono altresì considerati, ove opportuno, fattori settoriali.

Tenuto conto del riparto di competenze costituzionalmente definite tra lo Stato e le regioni è prevista **l’intesa della Conferenza Stato-regioni** per l’individuazione degli operatori che rispettivamente prestano attività di assistenza sanitaria o forniscono e distribuiscono acque destinate al consumo umano.

Ai fini dell’individuazione degli operatori si tiene conto altresì dei documenti prodotti dal **Gruppo di cooperazione** (composto dai

rappresentanti degli Stati membri, della Commissione europea e dell’ENISA).

E’ quindi disposta l’istituzione - presso il Ministero dello sviluppo economico – di un **elenco nazionale degli operatori di servizi essenziali**.

L'elenco degli operatori di servizi essenziali così identificati è riesaminato con le medesime modalità e, occorre, aggiornato su base regolare, ed almeno **con cadenza biennale** dopo il 9 maggio 2018, a cura delle autorità competenti NIS ed è comunicato al Ministero dello sviluppo economico.

Entro il 9 novembre 2018, ed in seguito ogni due anni, il punto di contatto unico (il DIS in base a quanto stabilito dall’art. 7 dello schema di decreto legislativo) **trasmette alla Commissione europea** le informazioni necessarie per la valutazione dell'attuazione del decreto, in particolare della coerenza dell'approccio in merito all'identificazione degli operatori di servizi essenziali.

Tali informazioni comprendono almeno:

a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;

b) l'elenco dei servizi essenziali;

c) il numero degli operatori di servizi essenziali identificati per ciascun settore ed un'indicazione della loro importanza in relazione a tale settore;

d) le soglie, ove esistano, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio o all'importanza di tale particolare operatore di servizi essenziali.

Articolo 6
(Strategia nazionale di sicurezza cibernetica)

La direttiva 2016/1148 si fonda sull'obbligo, per tutti gli Stati membri, di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi.

Lo schema di decreto legislativo affida dunque al Presidente del Consiglio dei ministri l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR[3]), della **strategia nazionale di sicurezza cibernetica** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Tale atto è trasmesso alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.

Con la medesima procedura sono adottate **linee di indirizzo per l'attuazione** della strategia nazionale di sicurezza cibernetica.

Nell'ambito della strategia nazionale di sicurezza cibernetica, devono essere in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del decreto (cfr. allegato II):

a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi infornativi;

b) il quadro di *governance* per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;

c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;

d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

e) i piani di ricerca e sviluppo;

f) un piano di valutazione dci rischi;

g) l'elenco dei vari attori coinvolti nell'attuazione.

[3] Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza. In particolare il Comitato: delibera sulla ripartizione delle risorse finanziarie e sui bilanci preventivi e consuntivi di DIS, AISE e AISI; indica il fabbisogno informativo necessario ai ministri per svolgere l'attività di governo.
Sono membri del CISR: il Presidente del Consiglio dei ministri; l'Autorità delegata; il Ministro degli affari esteri; il Ministro dell'interno; il Ministro della difesa; il Ministro della giustizia; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico. Al Direttore generale del DIS sono assegnate le funzioni di segretario del Comitato.

Con riferimento all'obbligo posto dalla direttiva di definire una strategia nazionale in materia di sicurezza cibernetica si ricorda che il Italia, con il D.P.C.M. 24 gennaio 2013, il Governo ha delineato per la prima volta in Italia l'architettura strategica nazionale per la protezione cibernetica e la sicurezza informatica.

In attuazione di quanto previsto dal richiamato DPCM sono stati successivamente adottati il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica che contengono gli obiettivi strategici e operativi della *cyber security* italiana.

Da ultimo, nelle Gazzetta ufficiali del 17 febbraio e del 1° giugno 2017 sono stati, rispettivamente pubblicati il nuovo DPCM in materia protezione cibernetica ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica relativo al 2017.

Attualmente, in linea con quanto previsto dal D.P.C.M. 17 febbraio 2017, il documento operativo di breve periodo nel quale vengono individuate le priorità, gli obiettivi specifici e le linee d'azione per dare concreta attuazione a quanto descritto nel Quadro strategico nazionale è costituito dal Piano nazionale per la protezione cibernetica e la sicurezza informatica adottato nel marzo 2017 dal Governo.

Nel Piano sono, in particolare, indicati i seguenti indirizzi operativi:

- potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare;
- potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;
- promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento;
- cooperazione internazionale ed esercitazioni;
- operatività delle strutture nazionali di *incident prevention, response e remediation;*
- interventi legislativi e *compliance* con obblighi internazionali;
- *compliance* a standard e protocolli di sicurezza;
- supporto allo sviluppo industriale e tecnologico;
- comunicazione strategica;
- risorse;
- implementazione di un sistema di *cyber risk management* nazionale.

Articolo 7
(Autorità nazionali competenti e punto di contatto unico)

Le autorità competenti NIS-*Network and Information Security* sono i soggetti cui spetta il **controllo dell'applicazione** della direttiva a livello nazionale e sono designate da ogni Stato membro che può affidare questo ruolo a una o più autorità esistenti (art. 8 direttiva 2016/1148)

Tali autorità sono individuate, a livello nazionale, nei **dicasteri competenti** in base al settore di riferimento unitamente, per alcuni profili dei settori della sanità e delle acque per il consumo umano, alle **regioni e alle province autonome**.

Tale ruolo è di nuova previsione, dal momento che attualmente sono svolte unicamente dal MISE e dall'Agenzia per l'Italia digitale, rispettivamente, le funzioni di CERT nazionale e di CERT-PA (v. oltre art. 8).

A tal fine l'articolo 7 specifica i seguenti ambiti di competenza:

- il **Ministero dello sviluppo economico** per il settore energia, sotto-settori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD[4], nonché per i servizi digitali;
- il **Ministero delle infrastrutture e trasporti** per il settore trasporti, sotto-settori aereo, ferroviario, per vie d'acqua e su strada;
- il **Ministero dell'economia e delle finanze** per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, la Banca d'Italia e la·Consob, secondo modalità di collaborazione e di scambio di informazioni che saranno stabilite con decreto del Ministro dell'economia e delle finanze;
- il **Ministero della salute** per l'attività di assistenza sanitaria, intesa come "servizi prestati da professionisti sanitari a pazienti, al fine di valutare, mantenere o ristabilire il loro stato di salute, ivi compresa la

[4] Il punto di interscambio internet (IXP) è definito dall'art. 3 dello schema di decreto legislativo quale infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico.

Il sistema dei nomi di dominio (DNS), è un sistema distribuito e gerarchico di *naming* in una rete che inoltra le richieste dei nomi di dominio.

Si intende per registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD).

prescrizione, la somministrazione e la fornitura di medicinali e dispositivi medici", prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e **le regioni e le province autonome**, direttamente o per il tramite delle autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria svolte dagli operatori autorizzati e accreditati delle regioni o dalle province autonome negli ambiti territoriali di rispettiva competenza;

- il **Ministero dell'ambiente e della tutela del territorio e del mare** e le **regioni e le province autonome**, direttamente o per il tramite delle autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.
  Pertanto, mentre per la sanità il testo definisce espressamente il riparto di competenze tra lo Stato e le regioni, per quello dell'acqua potabile il ruolo di autorità-NIS è attribuito contestualmente ad entrambi i soggetti (Ministero e regioni, eventualmente per il tramite delle autorità territorialmente competenti). Si ricorda, in ogni caso, che l'individuazione degli operatori essenziali in tali settori è effettuata dal Dicastero competente d'intesa con la Conferenza Stato-regioni (art. 5).

A tali autorità è attribuito dallo schema di decreto legislativo l'esercizio delle relative potestà ispettive e sanzionatorie, definite dai successivi articoli 19 e 20 (v. oltre).

E' quindi individuato il Dipartimento delle informazioni per la sicurezza (**DIS**) quale **punto di contatto unico**, organo incaricato a livello nazionale di coordinare·le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea.

Il punto di contatto unico svolge una funzione di collegamento per garantire la **cooperazione transfrontaliera** delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il Gruppo di cooperazione[5] (finalizzato allo scambio di informazioni tra Stati membri ed all'agevolazione della cooperazione strategica) e la rete di CSIRT (composta dai CSIRT degli Stati membri e dal CERT-UE e volta ad una cooperazione operativa rapida ed efficace). E' chiamato a collaborare nel gruppo di cooperazione "in modo effettivo, efficiente e sicuro" con i rappresentanti designati dagli altri Stati.

[5] L'art. 10 dello schema di decreto legislativo dispone la partecipazione del punto di contatto alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA).

Si ricorda che attualmente - in base al D.P.C.M, 17 febbraio 2017 - al **direttore generale del DIS** compete l'adozione delle iniziative idonee a definire le necessarie **linee di azione** per innalzare i migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati e avanzati supporti tecnologici. Per la realizzazione di tali iniziative, "è previsto il coinvolgimento del mondo accademico e della ricerca, con la possibilità di avvalersi di risorse di eccellenza, così come una diffusa collaborazione con le imprese di settore".

Sempre il Direttore del DIS è chiamato a predisporre gli opportuni moduli organizzativi, di coordinamento e di raccordo, prevedendo il ricorso anche a professionalità delle pubbliche amministrazioni, degli enti di ricerca pubblici e privati, delle università e di operatori economici privati.

Il D.P.C.M. 17 febbraio 2017 ha altresì previsto la collocazione istituzionale presso il DIS del Nucleo per la sicurezza cibernetica (NSC).

Le autorità competenti NIS e il punto di contatto unico sono tenute a consultare l'autorità di contrasto (operante presso il Ministero dell'interno) ed il Garante per la protezione dei dati personali ed a collaborare con essi.

Gli oneri derivanti dall'articolo in esame sono pari a 1.000.000 euro e sono riportati in dettaglio dalla relazione tecnica. In gran parte attengono agli oneri per l'acquisto di beni e servizi, per attività di ispezione e analisi *in loco* delle infrastrutture informatiche e per la formazione del personale addetto al settore. Alla copertura di tali oneri si provvede attraverso la contestuale riduzione del Fondo per il recepimento della normativa europea.

Il **Fondo per il recepimento della normativa europea** è stato istituito dalla legge 29 luglio 2015, n. 115 (Legge europea 2014) attraverso l'introduzione dell'articolo 41-*bis* della legge 234/2012, al fine di consentire il tempestivo adeguamento dell'ordinamento interno agli obblighi imposti dalla normativa europea, nei soli limiti occorrenti per l'adempimento di tali obblighi e soltanto in quanto non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni dalla legislazione vigente.

Articolo 8
(Gruppi di intervento per la sicurezza informatica in caso incidente - CSIRT)

Il **CSIRT-***Computer Emergency Response Team* è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita (art. 9).

In particolare, la direttiva 2016/1148, dispone l'obbligo per gli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi. Prevede inoltre la creazione di una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace. Ai sensi dell'art. 11 dello schema di decreto legislativo, il CSIRT italiano partecipa inoltre alla rete CISRT composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

A tal fine, lo schema di decreto legislativo istituisce presso la Presidenza del Consiglio dei ministri un nuovo organismo, il **CSIRT italiano**, al quale sono attribuite – a decorrere dall'entrata in vigore del relativo decreto del Presidente del Consiglio dei ministri di organizzazione e funzionamento - le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID).

Le funzioni attribuite dall'art. 8 al CSIRT italiano sono, in particolare, così definite (dall'art. 8, co. 4 dello schema di decreto legislativo):

- assicurare la conformità ai requisiti di disponibilità dei servizi di comunicazione e di mezzi di contatto dettati all'allegato I, punto l (v. *infra*), e svolgere i compiti di monitoraggio degli incidenti, di emissione di preallarmi, di intervento e di analisi e definizione di prassi standardizzate, cooperando altresì con il settore privato;
- svolgere la propria attività nell'ambito dei settori dell'energia e dei trasporti, del settore bancario e delle infrastrutture dei mercati finanziari, nonché dei settori sanitario, della fornitura dell'acqua potabile e delle infrastrutture digitali - di cui all'allegato II (v. *infra*) - e dei servizi digitali di cui all'allegato III (v. *infra*;
- definire le procedure per la prevenzione e la gestione degli incidenti informati;

- garantire la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT.

L'istituenda struttura dispone di un'infrastruttura di informazione e comunicazione "appropriata, sicura e resiliente a livello nazionale". Il CSIRT italiano, per lo svolgimento delle proprie funzioni, può avvalersi anche dell'Agenzia per l'Italia digitale-AGID.

Per quanto riguarda l'assetto dell'istituendo organismo, è previsto che per lo svolgimento delle funzioni del CSIRT italiano, la Presidenza del Consiglio dei ministri si avvalga di un contingente massimo di **trenta unità di personale** di cui**:**

- **quindici** scelti tra dipendenti di altre amministrazioni pubbliche, in **posizione di comando o fuori ruolo**;

- **quindici** da assumere, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facoltà assunzionali della Presidenza del Consiglio dei ministri.

Si ricorda che in base alla direttiva 2016/1148, i CSIRT nazionali devono disporre di personale sufficiente per garantirne l'operatività 24 ore su 24.

Per le spese di personale è previsto un limite **annuo di 1.300.000 di euro** a decorrere dal 2018 la cui copertura finanziaria è posta in capo al Fondo per il recepimento della normativa europea.

Inoltre, per le spese di funzionamento del CSIRT italiano è autorizzata la spesa di **2.700.000 euro per l'anno 2018**, di cui 2.000.000 per le spese di investimenti, e di **700.000 annui a decorrere dall'anno 2019**. Anche a tali oneri si provvede attraverso la contestuale riduzione del Fondo per il recepimento della normativa europea.

Nella relazione tecnica si specifica che, per quanto concerne gli investimenti - una tantum - occorre prevedere i costi di attrezzaggio di idonei locali (dotati, oltre che dei necessari spazi operativi, di idonee infrastrutture di sicurezza fisica e ambientale) fra cui devono essere compresi una sala operativa adeguatamente attrezzata (postazioni individuali più parete "*videowall*"), un locale tecnico (sala server, sala apparati), almeno una sala riunioni isolata ed un laboratorio per acquisizioni ed analisi forensi. Per quanto riguarda la dotazione *hardware* è necessario acquisire nuove capacità di calcolo e memorizzazione (*cloud* privato, *network storage* di adeguata capacità), predisporre il potenziamento degli strumenti realizzati e in corso di realizzazione, nonché prevedere la dotazione di dispositivi di acquisizione ed analisi di dati/immagini da hard disk e reti per il supporto alle attività di analisi forense. Per quanto riguarda la dotazione di software, ivi compreso il potenziamento delle licenze attuali (sistemi operativi *server* e *workstation*, strumenti di *office automation*, *software specifici*).

L'onere di spesa complessivo derivante dall'art. 8 è dunque pari a **4.000.000 euro** per l'anno 2018 e **2.000.000 euro annui a decorrere** dall'anno 2019. Alla relativa copertura si provvede, come si è detto, nell'ambito del Fondo per il recepimento della normativa europea.

Il **Fondo per il recepimento della normativa europea** è stato istituito dalla legge 29 luglio 2015, n. 115 (Legge europea 2014) attraverso l'introduzione dell'articolo 41-*bis* della legge 234/2012, al fine di consentire il tempestivo adeguamento dell'ordinamento interno agli obblighi imposti dalla normativa europea, nei soli limiti occorrenti per l'adempimento di tali obblighi e soltanto in quanto non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni dalla legislazione vigente.

Per quanto riguarda le funzioni oggetto di trasferimento, si ricorda che presso il **Ministero dello sviluppo economico** è attualmente operante, ai sensi dell'art. 16-*bis* del Codice delle comunicazioni elettroniche (D. lgs. 259/2003), il *Computer Emergency Response Team* CERT nazionale, con compiti di assistenza tecnica in caso di segnalazioni da parte di utenti e di diffusione di informazioni anche riguardanti le contromisure adeguate per i tipi più comuni di incidente.

Nel Codice delle comunicazioni elettroniche (d.lgs. 259/2003, articoli 16-bis e 16- ter), sono state previste per la prima volta – con l'attuazione della direttiva 2009/140/UE, avvenuto con d.lgs. 70/2012 - norme finalizzate al rafforzamento della sicurezza informatica delle reti e dei servizi di comunicazione elettronica, individuando presso il Ministero dello sviluppo economico il CERT (*Computer Emergency Response Team*) Nazionale con compiti di supporto a cittadini e imprese nella prevenzione e risposta agli incidenti informatici.

Il CERT nazionale è stato istituito con l'obiettivo, in particolare, di incrementare la consapevolezza e la cultura della sicurezza nell'utilizzo di servizi *on line*, fornendo informazioni tempestive su potenziali minacce informatiche, raccomandazioni e consigli utili per la prevenzione, contromisure per la risoluzione di incidenti informatici con impatto significativo. Il CERT opera sulla base di un modello cooperativo pubblico-privato.

All'**Agenzia per l'Italia Digitale** (AgID) compete attualmente il coordinamento, tramite il *Computer Emergency Response Team* Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, delle iniziative di prevenzione e gestione degli incidenti di sicurezza informatici.

In particolare, all'AgID spetta – ai sensi dell'art. 51 del Codice dell'amministrazione digitale (CAD), di cui al d. lgs. n. 82 del 2005 - l'attuazione, per quanto di competenza e in raccordo con le altre autorità competenti in materia, del Quadro strategico nazionale per la sicurezza dello spazio cibernetico e del Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, la promozione delle intese con le analoghe strutture internazionali e la segnalazione al Ministro per la semplificazione e la pubblica

amministrazione del mancato rispetto delle Linee guida da parte delle pubbliche amministrazioni. Con le Linee guida sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture.

Le pubbliche amministrazioni sono chiamate ad aderire ogni anno ai programmi di sicurezza preventiva coordinati e promossi da AgID secondo le procedure dettate dalla medesima AgID con le Linee guida e predispongono, nel rispetto delle Linee guida adottate dall'AgID, piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività.

Il D.P.C.M. 27 gennaio 2014 unitamente al "Piano nazionale per la protezione cibernetica e la sicurezza informatica" ha previsto, tra l'altro, l'avvio delle attività del CERT Nazionale presso il Ministero dello sviluppo economico e del CERT-PA presso l'Agenzia per l'Italia Digitale (AGID).

Le relative funzioni sono **trasferite al nuovo organismo** (**CSIRT italiano**, istituito **presso la Presidenza del Consiglio**) a decorrere dalla data di entrata in vigore del relativo decreto di organizzazione e funzionamento del CSIRT, da adottare ai sensi dell'art. 7 del d. lgs. 303/1999, che disciplina l'ordinamento e l'organizzazione della Presidenza del Consiglio dei Ministri.

Nel dettaglio, l'art. 7 del d. lgs. 303/1999 prevede che per lo svolgimento delle funzioni istituzionali e per i compiti di organizzazione e gestione il Presidente del Consiglio dei ministri individua con **propri decreti** le **aree funzionali omogenee** da affidare alle strutture in cui si articola il Segretariato generale. Con propri decreti, il Presidente determina le strutture della cui attività si avvalgono i Ministri o Sottosegretari da lui delegati.

Tali decreti indicano il numero massimo degli uffici in cui si articola ogni Dipartimento e dei servizi in cui si articola ciascun ufficio. All'organizzazione interna delle strutture medesime provvedono, nell'ambito delle rispettive competenze, il Segretario generale ovvero il Ministro o Sottosegretario delegato.

Per lo svolgimento di particolari compiti per il raggiungimento di risultati determinati o per la realizzazione di specifici programmi, il Presidente del Consiglio istituisce, con proprio decreto, apposite **strutture di missione**, la cui durata temporanea, comunque non superiore a quella del Governo che le ha istituite, è specificata dall'atto istitutivo. Per le attribuzioni che implicano l'azione unitaria di più dipartimenti o uffici a questi equiparabili, il Presidente del Consiglio può istituire con proprio decreto apposite **unità di coordinamento interdipartimentale**.

Potrebbe essere valutata l'opportunità di stabilire espressamente un termine per l'adozione di tale regolamento al fine di evitare incertezze in sede applicativa anche alla luce degli obblighi recati dalla direttiva 2016/1148, cui viene data attuazione con il provvedimento in esame.

Articolo 9
(Cooperazione a livello nazionale)

La direttiva 2016/1148 prevede che, se sono separati, l'autorità competente, il punto di contatto unico e i CSIRT dello stesso Stato membro **collaborano per l'adempimento degli obblighi** della direttiva.

In particolare, gli Stati membri sono tenuti a garantire che le autorità competenti o i CSIRT ricevano le notifiche di incidenti trasmesse ai sensi della direttiva. Ove uno Stato membro decida che i CSIRT non ricevano le notifiche, questi ultimi hanno accesso, nella misura necessaria per l'esecuzione dei loro compiti, ai dati sugli incidenti notificati dagli operatori di servizi essenziali o dai fornitori di servizi digitali. Gli Stati membri sono tenuti a garantire che le autorità competenti o i CSIRT informino i punti di contatti unici in merito alle notifiche di incidenti trasmesse ai sensi della direttiva.

Essendo state definiti soggetti distinti per tali funzioni dallo schema di decreto legislativo in esame (v. *supra*), l'art. 9 dispone che le autorità competenti NIS, il punto di contatto unico e il CSIRT italiano collaborino per l'adempimento degli obblighi previsti dal provvedimento.

A tal fine è prevista l'istituzione, presso la **Presidenza del Consiglio dei ministri**, di un **Comitato tecnico di raccordo**, composto da rappresentanti dei dicasteri competenti (v. art. 7) e da rappresentanti delle regioni e province autonome in numero non superiore a due, designati in sede di Conferenza Stato-regioni.

L'organizzazione del Comitato è definita con **decreto del Presidente del Consiglio dei ministri**, da adottare su proposta dei Ministri per la semplificazione e la pubblica amministrazione e dello sviluppo economico, sentita la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano.

Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi spese.

Gli operatori di servizi essenziali e i fornitori di servizi digitali inviano le **notifiche relative ad incidenti** al CSIRT italiano il quale deve informare le autorità competenti NIS e il punto di contatto unico in merito a tali notifiche.

Articolo 10
(Gruppo di cooperazione)

Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni fra Stati membri, di sviluppare la fiducia e nell'ottica di conseguire un livello comune elevato di sicurezza delle reti e dei servizi informativi nell'Unione, la direttiva 2016/1148 istituisce un **gruppo di cooperazione**.

Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali, ed è composto da rappresentanti degli Stati membri, della Commissione e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori i rappresentanti delle parti interessate. Il segretariato è assicurato dalla Commissione europea.

In base all'art. 10 dello schema di decreto legislativo il **punto di contatto unico** – individuato nel DIS dal provvedimento in esame (art. 7) - è chiamato a partecipare alle attività del **gruppo di cooperazione** composto da rappresentanti degli Stati membri, della Commissione europea e dell'ENISA.

Il punto di contatto unico, infatti, svolge – in base alla direttiva - una **funzione di collegamento** per garantire la **cooperazione transfrontaliera** delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione.

In particolare, il gruppo di cooperazione – come previsto dalla direttiva - contribuisce in particolare a:

a) condividere buone pratiche sullo scambio di informazioni relative alla notifica di incidenti di cui all'articolo 12 e all'articolo 14;

b) scambiare migliori pratiche con gli Stati membri e, in collaborazione con l'ENISA, fornire supporto per la creazione di capacità in materia di sicurezza delle reti e dei sistemi informativi;

c) discutere le capacità e lo stato di preparazione degli Stati membri e valutare, su base volontaria, le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi e l'efficacia dei CSIRT e individuare le migliori pratiche;

d) scambiare informazioni e migliori pratiche in materia di sensibilizzazione e formazione;

e) scambiare informazioni e migliori pratiche in materia di ricerca e sviluppo riguardo alla sicurezza delle reti e dei sistemi informativi;

f) scambiare, ove opportuno, esperienze in materia di sicurezza delle reti e dei sistemi informativi con le istituzioni, gli organi e gli organismi pertinenti dell'Unione europea;

g) discutere le norme e le specifiche con i rappresentanti delle pertinenti organizzazioni di normazione europee;

h) fornire informazioni in relazione ai rischi e agli incidenti;

i) discutere il lavoro svolto riguardo a esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, programmi di istruzione e formazione, comprese le attività svolte dall'ENISA;

l) con l'assistenza dell'ENISA, scambiare migliori pratiche connesse all'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere riguardo a rischi e incidenti.

Le autorità competenti NIS, attraverso il punto di contatto unico, assicurano la partecipazione al gruppo di cooperazione al fine di elaborare ed adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti. Il punto di contatto unico, ove necessario, chiede alle autorità competenti NIS interessate, nonché al CSIRT, la partecipazione al gruppo di cooperazione.

Entro il **9 agosto 2018** e in seguito ogni anno, il punto di contatto unico trasmette una **relazione sintetica** al gruppo di cooperazione in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati e alle azioni intraprese ai sensi degli articoli 12 e 14 (obblighi in materia di sicurezza e notifica degli incidenti degli operatori dei servizi essenziali e dei fornitori di servizi digitali).

Articolo 11
(Rete di CSIRT)

La direttiva 2016/1148 prevede la creazione di una **rete di gruppi di intervento** per la sicurezza informatica in caso di incidente («rete CSIRT *Computer Emergency Response Team* ») per "contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace".

Ai sensi dell'art. 11 dello schema di decreto legislativo, dunque, il CSIRT italiano partecipa alla rete CISRT composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

Si ricorda che il **CSIRT** è definito dalla direttiva 2016/1148 quale gruppo di intervento per la sicurezza informatica in caso di incidente. Il **CSIRT italiano**, è istituito presso la Presidenza del Consiglio dei ministri e gli sono attribuite le funzioni del CERT nazionale e del CERT-PA.

Il CSIRT italiano a tal fine è chiamato a

a) **scambiare informazioni** sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT;

b) su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, **scambiare e discutere informazioni non sensibili** sul piano commerciale connesse a tale incidente e i rischi associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;

c) scambiare e mettere a disposizione su base volontaria **informazioni non riservate su singoli incidenti**;

d) su richiesta di un rappresentante di un CSIRT di un altro Stato membro, discutere e, ove possibile, **individuare un intervento coordinato** per un incidente rilevato nella giurisdizione di quello stesso Stato membro;

e) fornire sostegno agli altri Stati membri nel far fronte a **incidenti transfrontalieri** sulla base dell'assistenza reciproca volontaria;

f) discutere, esaminare e individuare ulteriori **forme di cooperazione operativa**, anche in relazione a: categorie di rischi e di incidenti; preallarmi; assistenza reciproca; principi e modalità di coordinamento, quando gli Stati membri intervengono in relazione a rischi e incidenti transfrontalieri;

g) informare il gruppo di cooperazione in merito alle proprie attività e a **ulteriori forme di cooperazione operativa** discusse e chiedere orientamenti in merito;

h) discutere gli **insegnamenti appresi dalle esercitazioni** in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA;

i) formulare orientamenti volti ad **agevolare la convergenza delle pratiche operative** in relazione all'applicazione delle disposizioni in materia di cooperazione operativa.

Articolo 12
(Obblighi in materia di sicurezza e notifica degli incidenti per gli operatori dei servizi essenziali)

L'articolo 12**, sostanzialmente riproduttivo dell'articolo 14 della direttiva,** definisce gli **obblighi** in capo agli **operatori dei servizi essenziali** in particolare con riferimento alle misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti nonché alle modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti. Gli adempimenti previsti per gli operatori dei servizi essenziali devono essere realizzati a valere sulle risorse finanziarie disponibili sui rispettivi bilanci e senza nuovi o maggiori oneri a carico della finanza pubblica.

Per la predisposizione sia delle misure tecniche e organizzative dirette ad assicurare un livello di sicurezza delle reti e dei sistemi informativi adeguato al rischio esistente, sia per le misure dirette a prevenire e minimizzare gli incidenti a carico della sicurezza delle reti e dei sistemi informativi gli operatori tengono conto delle linee guida predisposte dal gruppo di cooperazione delle linee guida per la notifica degli incidenti in grado di determinare un impatto transfrontaliero (comma 3). Peraltro anche le autorità competenti NIS (*Network and information security*) possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali (comma 4).

Qualora gli operatori non provvedano alla predisposizione delle misure tecniche ed organizzative sia con riferimento alla gestione dei rischi, sia con riferimento alla prevenzione degli incidenti e per minimizzarne le conseguenze, salvo che il fatto costituisca reato, l'articolo 21, commi 1 e 2, prevede l'irrogazione di una sanzione amministrativa compresa tra 12 e 120 mila euro.

Andrebbe valutata l'opportunità di riformulare la fattispecie di cui al comma 2 dell'articolo 21 facendo riferimento, come indicato nel testo dell'articolo 12, comma 2, "alle misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali".

Passando agli aspetti **più prettamente procedurali** gli operatori di servizi essenziali in caso di incidenti che abbiano un impatto rilevante sui servizi forniti sono tenuti **a informarne, senza ingiustificato ritardo, il CSIRT** (*Computer security incident response team*) italiano, mediante

notifica, **nonché**, per conoscenza **la competente autorità NIS** (comma 5). Tale comunicazione non espone l'operatore ad ulteriori responsabilità oltre a quelle derivanti dall'incidente (comma 7). L'omessa notifica invece comporta, qualora il fatto non costituisca reato, una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro (articolo 21, comma 3).

Inoltre sono garantite dal CSIRT all'operatore la sicurezza e la salvaguardia degli interessi commerciali, nonché la riservatezza delle informazioni fornite nella notifica (comma 7). Il CSIRT, se le circostanze lo consentono, fornisce all'operatore di servizi essenziali, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente (comma 11).

Il CSIRT inoltra quindi la notifica all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento (comma 6).

Per valutare la rilevanza dell'incidente si tiene conto: del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all'area interessata dall'incidente (comma 8).

Quanto ai **contenuti della notifica,** essa deve includere le informazioni che consentono al CSIRT italiano di determinare un **eventuale impatto transfrontaliero dell'incidente** (comma 7, primo periodo)**.**

Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, il CSIRT italiano informa gli eventuali altri Stati membri interessati in cui l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali (comma 9) inoltre, su richiesta dell'autorità competente NIS o del CSIRT italiano, il punto di contatto unico trasmette, previa verifica dei presupposti, le notifiche ai punti di contatto unici degli altri Stati membri interessati (comma 12).

Per quanto riguarda **la diffusione di informazioni al pubblico** concernenti l'incidente essa può essere prevista "qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso", previa valutazione dell'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento, a cura della competente autorità NIS, d'intesa col CSIRT e previa consultazione dell'operatore di servizi essenziali (comma 13).

Andrebbe valutata la possibilità di prevedere, qualora ricorrano le condizioni indicate dal comma 13, la diffusione al pubblico delle informazioni e non la mera possibilità di diffusione delle stesse.

Articolo 13
(Attuazione e controllo)

L’articolo 13, riproduttivo dei contenuti dell’articolo 15 della direttiva, individua **i poteri di controllo delle autorità NIS** nei confronti degli **operatori di servizi essenziali** in merito al rispetto degli obblighi previsti dall’articolo 12, anche sotto il profilo degli effetti sulla sicurezza della rete e dei sistemi informativi.

L’autorità, indicando **lo scopo delle richieste e specificando il tipo di informazioni da fornire**, può richiedere sia le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza, sia la prova dell'effettiva attuazione delle politiche di sicurezza, anche attraverso le risultanze di un apposito *audit* curato dal medesimo NIS o da un revisore abilitato.

I fornitori di servizi essenziali sono tenuti a fornire le informazioni richieste e, qualora non lo facciano, sono soggetti, salvo che il fatto non costituisca reato, a una sanzione amministrativa pecuniaria compresa tra 12 mila e 120 mila euro (articolo 21, comma 4).

Qualora dalla valutazione degli elementi forniti emergano delle carenze l’autorità NIS **può emanare istruzioni vincolanti** per gli operatori di servizi essenziali al fine di porvi rimedio. Qualora l’operatore non osservi le istruzioni fornite, salvo che il fatto non costituisca reato, è assoggettato ad una sanzione amministrativa pecuniaria compresa tra 15 mila e 150 mila euro (articolo 21, comma 5).

Se l’incidente comporta violazione dei dati personali l’autorità competente opera in stretta cooperazione con il Garante per la protezione dei dati personali.

Articolo 14
(Obblighi di notifica in materia di sicurezza e notifica degli incidenti per i fornitori dei servizi digitali)

L’articolo 14**, sostanzialmente riproduttivo dell’articolo 16 della direttiva,** definisce gli **obblighi** in capo agli **fornitori dei servizi digitali** in particolare con riferimento alle misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti nonché alle modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi indicati dall’allegato III (mercato *online*, motori di ricerca *online*, servizi di *cloud computing*).

Come indicato dal cinquantasettesimo considerando della direttiva, a differenza di quanto previsto per i servizi essenziali, gli Stati membri non dovrebbero identificare i fornitori di servizi digitali, in quanto la direttiva dovrebbe applicarsi a **tutti i fornitori di servizi digitali rientranti nel suo campo di applicazione**. Inoltre, la direttiva e i relativi atti di esecuzione dovrebbero assicurare un elevato livello di **armonizzazione per i fornitori di servizi digitali con riguardo agli obblighi di notifica e di sicurezza**. Ciò dovrebbe consentire che i fornitori di servizi digitali siano trattati in modo uniforme in tutta l' Unione, in modo proporzionato alla loro natura e al grado di rischio cui potrebbero essere esposti.

I fornitori dei servizi digitali individuano ed adottano le misure tecniche e organizzative dirette ad assicurare un livello di sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall’allegato III **adeguato al rischio esistente**, tenendo conto di cinque elementi indicati già nella direttiva e riprodotti nel testo dello schema: la sicurezza dei sistemi e degli impianti; il trattamento degli incidenti; la gestione della continuità operativa; monitoraggio, audit e test; la conformità con le norme internazionali (commi 1 e 2).

Qualora essi non provvedano, salvo che il fatto costituisca reato, l’articolo 22 prevede l’irrogazione di una sanzione amministrativa compresa tra 8 mila e 80 mila euro (articolo 22, comma 1, ultimo periodo).

I fornitori di servizi digitali applicano inoltre le disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente le misure tecnico-organizzative dirette ad assicurare un livello di sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall’allegato III (comma 12).

Andrebbe valutato se anche per l’omessa applicazione delle disposizioni di attuazione degli atti di esecuzione della Commissione sia opportuna la previsione di una sanzione amministrativa.

Come gli operatori di servizi essenziali anche i fornitori di servizi digitali adottano misure dirette a prevenire e minimizzare gli incidenti a carico della sicurezza delle reti e dei sistemi informativi sui servizi indicati dall'allegato III sopra ricordati offerti all'interno dell'Unione europea, per garantirne la continuità (comma 3), e anche in tal caso, qualora non adempiano a questo obbligo si prevede l'irrogazione di una sanzione amministrativa compresa tra 8 mila e 80 mila euro e sempre che il fatto non costituisca reato (articolo 22, comma 2, ultimo periodo) .

Passando agli aspetti più prettamente procedurali i fornitori di servizi digitali in caso di incidenti che abbiano un impatto rilevante sulla fornitura dei servizi di cui all'allegato III sono tenuti **a informarne senza ingiustificato ritardo il CSIRT** (*Computer security incident response team*) italiano, mediante notifica, **nonché**, per conoscenza **la competente autorità NIS** (comma 4). Tale comunicazione non espone chi la pone in essere ad ulteriori responsabilità oltre a quelle derivanti dall'incidente (comma 5). L'omessa notifica invece comporta, ai sensi dell'articolo 21, comma 6, qualora il fatto non costituisca reato, una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

I fornitori di servizi digitali applicano inoltre le disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente i parametri, ivi compresi formati e procedure, relativi agli obblighi di notifica.

Andrebbe valutato se anche per l'omessa applicazione delle disposizioni di attuazione degli atti di esecuzione della Commissione sia opportuna la previsione di una sanzione amministrativa.

Tuttavia l'obbligo di notificare un incidente si applica ai fornitori di servizi digitali solo nel caso in cui abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente con riferimento ai parametri individuati al fine di valutare la rilevanza dell'incidente (comma 7) e si precisa che, fatto salvo questo obbligo, non sono imposti ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali (comma 13).

A tal fine sono tenuti in particolare considerazione: il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi; la durata dell'incidente; la diffusione geografica relativamente all'area interessata dall'incidente; la portata della perturbazione del funzionamento del servizio; la portata dell'impatto sulle attività economiche e sociali (comma 6).

Inoltre la disposizione prevede anche il caso in cui un operatore di servizi essenziali **dipenda da una terza parte fornitrice di servizi digitali** per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali: in tal caso è compito

dell’operatore stesso notificare **qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di tale operatore** (comma 8). Anche il mancato adempimento di questo obbligo, salvo che il fatto non costituisca reato, comporta l’irrogazione di una sanzione amministrativa pecuniaria compresa tra 12 mila e 120 mila euro (articolo 21, comma 7).

Qualora l’incidente riguardi due o più Stati membri, il CSIRT italiano, previa valutazione dell'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento, informa gli altri Stati membri coinvolti. Il CSIRT italiano, in tale circostanza tutela la sicurezza e gli interessi commerciali del fornitore di servizi digitali, nonché la riservatezza delle informazioni fornite nella notifica (commi 9 e 10).

Per quanto riguarda **la diffusione di informazioni al pubblico** concernenti l’incidente essa può essere prevista non solo “qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso” come nel caso degli operatori di servizi essenziali, ma anche “qualora sussista comunque un interesse pubblico alla divulgazione dell'incidente”. I profili procedurali sono analoghi a quelli previsti dall’articolo 12. Anche in tal caso, previa valutazione dell’organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento, la competente autorità NIS, d’intesa col CSIRT e previa consultazione dell’operatore di servizi essenziali può procedere direttamente a fornire informazione al pubblico. Si prevede tuttavia che l’autorità NIS possa chiedere al fornitore di servizi digitali di provvedervi (comma 11).

Andrebbe valutata la possibilità di prevedere, qualora ricorrano le condizioni indicate dal comma 11, la diffusione al pubblico delle informazioni e non la mera possibilità di diffusione delle stesse.

Il comma 14 esclude l’applicazione delle disposizioni di cui agli articoli 14, 15 e 16 alle microimprese e alle piccole imprese come definite dalla raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.

Ai sensi dell’articolo 2 della Raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE si definisce **microimpresa** un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di euro. È definita **piccola impresa**

quella che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo che non superiori a 10 milioni di euro.

Articolo 15
(Attuazione e controllo)

L’articolo 15, riproduttivo dei contenuti dell’articolo 17 della direttiva, individua **i poteri di controllo delle autorità NIS** nei confronti degli **fornitori dei servizi digitali** in merito al rispetto degli obblighi previsti dall’articolo 14.

In particolare si prevede che nel caso in cui sia dimostrato il mancato rispetto degli obblighi di cui all'articolo 14 da parte dei fornitori di servizi digitali, l'autorità competente NIS può adottare misure di vigilanza *ex post* adeguate alla natura dei servizi e delle operazioni.

La dimostrazione del mancato rispetto degli obblighi può essere prodotta anche dall'autorità competente di un altro Stato membro in cui è fornito il servizio (comma 1).

La disposizione prevede quindi gli obblighi in capo ai fornitori di servizi digitali che sono tenuti a fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza nonché a porre rimedio ad ogni mancato adempimento degli obblighi di cui all'articolo 14 (comma 2).

Il mancato adempimento di questi obblighi di informazione e di intervento comporta, salvo che il fatto non costituisca reato l’irrogazione di una sanzione amministrativa pecuniaria tra 12 mila e 120 mila euro (articolo 22, comma 8).

Il comma 3 prevede un meccanismo di collaborazione tra le diverse autorità statali nel caso in cui un fornitore di servizi digitali abbia lo stabilimento principale o un rappresentante in uno Stato membro, ma la sua rete o i suoi sistemi informativi siano ubicati in uno o più altri Stati membri.

In tal caso l'autorità competente dello Stato membro dello stabilimento principale o del rappresentante e le autorità competenti dei suddetti altri Stati membri cooperano e si assistono reciprocamente in funzione delle necessità. Tale assistenza e cooperazione può comprendere scambi di informazioni tra le autorità competenti interessate e richieste di adottare le misure di vigilanza indicate al comma 2 (comma 3).

Articolo 16
(Giurisdizione e territorialità)

L’**articolo 16** individua, sostanzialmente riproducendo il contenuto dell’articolo 18 della direttiva, i criteri per definire a quale giurisdizione sia assoggettato il fornitore di servizi digitali.

Si prevede in particolare, ai fini del presente decreto, che i fornitori di servizi digitali sono considerati soggetti alla giurisdizione dello Stato membro in cui hanno lo stabilimento principale.

Un fornitore di servizi digitali è comunque considerato avere il proprio stabilimento principale in uno Stato membro **quando ha la sua sede sociale in tale Stato membro**.

Con riferimento ai fornitori di servizi digitali che non sono stabiliti nell'Unione europea, ma offrono servizi di cui all'allegato III all'interno dell'Unione europea, si prevede **l’obbligo di designare un rappresentante** nell'Unione europea, che è stabilito in uno di quegli Stati membri in cui sono offerti i servizi.

In tal caso il fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante.

La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.

Articolo 17
(Normazione)

L'**articolo 17**, corrispondente all'articolo 19 della direttiva, è diretto a favorire la progressiva convergenza della normativa relativa alla sicurezza delle reti e dei sistemi informativi .

In particolare si prevede che le autorità NIS, senza imporre o creare discriminazioni a favore dell'uso di un particolare tipo di tecnologia, promuovano l'adozione armonizzata di **norme e specifiche europee o accettate a livello internazionale** relative alla sicurezza della rete e dei sistemi informativi.

Tale normazione armonizzata è prevista:

- per gli operatori di servizi essenziali, ai fini della predisposizione delle misure tecniche e organizzative dirette ad assicurare un livello di sicurezza delle reti e dei sistemi informativi adeguato al rischio esistente,
- per le misure dirette a prevenire e minimizzare gli incidenti a carico della sicurezza delle reti e dei sistemi informativi,
- per i fornitori dei servizi digitali con riguardo alle misure tecniche e organizzative dirette ad assicurare un livello di sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III (mercato *online*, motori di ricerca *online*, e servizi di *cloud computing*) adeguato al rischio esistente, tenendo conto dei parametri indicati dall'articolo 14, comma 2 (comma 1).

Le autorità competenti NIS tengono conto dei pareri e delle linee guida predisposte dall'ENISA, in collaborazione con gli Stati membri, riguardanti i settori tecnici da prendere in considerazione in relazione al comma l, nonché le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.

Articolo 18
(Notifica volontaria)

L’**articolo 18**, corrispondente all’articolo 20 della direttiva, disciplina le notifiche volontarie di incidenti aventi impatti rilevanti sulla continuità dei servizi prestati da soggetti **che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali**.

La trattazione di queste notifiche **non è obbligatoria** ed è effettuata soltanto qualora tale trattamento **non costituisca un onere sproporzionato o eccessivo**. Inoltre le notifiche obbligatorie sono trattate prioritariamente rispetto a quelle volontarie.

Qualora la notifica volontaria formi oggetto di trattazione sono richiamate le procedure di cui all’articolo 12, per cui la notifica è effettuata senza ingiustificato ritardo al CSIRT (*Computer security incident response team*) italiano, mediante notifica, nonché, per conoscenza alla competente autorità NIS e deve includere le informazioni che consentono al CSIRT italiano di determinare un eventuale impatto transfrontaliero dell'incidente.

Il CSIRT inoltra quindi la notifica all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento. Anche in tal caso, per valutare la rilevanza dell’incidente, si tiene conto: del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all’area interessata dall’incidente.

Il CSIRT, se le circostanze lo consentono, fornisce all'operatore, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente.

Per quanto riguarda la diffusione di informazioni al pubblico concernenti l’incidente, come previsto dal richiamato articolo 12, essa è prevista “qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso”, previa valutazione dell’organo istituito presso il Dipartimento informazioni per la sicurezza incaricato delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento, a cura della competente autorità NIS, d’intesa col CSIRT e previa consultazione dell’operatore.

La notifica volontaria non può comunque avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Articolo 19
(Poteri ispettivi)

L’**articolo 19** attribuisce alle autorità competenti NIS i poteri ispettivi e di verifica necessari per le misure previste dagli articoli 12, 13, 14 e 15 facendo salve le competenze degli organi preposti alla tutela dell’ordine e della sicurezza pubblica.

La disposizione concerne esclusivamente l’organizzazione interna delle competenze e pertanto non ha una diretta corrispondenza in norme della direttiva.

Il comma 2 individua le modalità di coordinamento per lo svolgimento per le medesime attività ispettive e di verifica con riguardo alle reti e i sistemi informativi utilizzati dagli operatori nel settore dell’assistenza sanitaria ed in quello della fornitura e distribuzione di acqua potabile.

Posto che tali ambiti rientrano nella competenza delle Regioni e delle province autonome è previsto un accordo tra Governo, regioni e province autonome volto a definire “i criteri uniformi in ambito nazionale” per lo svolgimento delle citate attività di ispezione e verifica.

Articoli 20-21
(Sanzioni amministrative)

Gli **articoli 20 e 21** disciplinano le **autorità competenti**, le **fattispecie oggetto di sanzione amministrativa**, il regime **della reiterazione delle violazioni e** la **procedura applicabile** per l'irrogazione**.**

Con riferimento alla **competenza** per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto si prevede che essa spetti alle autorità competenti NIS di cui all'articolo 7 per i rispettivi settori e sottosettori di riferimento (articolo 20).

Con riferimento alle **singole fattispecie oggetto di sanzione**, previste dai commi 1 a 8, dell'articolo 21, si rinvia alla trattazione delle medesime effettuata per le specifiche disposizioni alle quali le singole sanzioni afferiscono.

La direttiva 2016/1148 prevede, a questo riguardo, che gli Stati membri stabiliscano le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della medesima adottando tutti i provvedimenti necessari per la loro applicazione**. Le sanzioni previste sono effettive, proporzionate e dissuasive**.

Gli Stati membri notificano tali norme e provvedimenti alla Commissione **entro il 9 maggio 2018** e provvedono a darle immediata notifica di ogni successiva modifica.

In termini generali le sanzioni individuate per la violazione degli obblighi previsti in capo agli operatori di servizi essenziali e ai fornitori di servizi digitali variano tra un minimo di 8 mila euro ad un massimo di 150 mila euro.

Con la legge 2018-133 del 26 febbraio del 2018 contenente diverse disposizioni d'adattamento al diritto dell'Unione europea nel settore della sicurezza **la Francia ha recepito la direttiva 2016/1148** (ed è allo stato il primo Paese ad aver proceduto al recepimento). Con specifico riferimento alle sanzioni esse sono riferite alle fattispecie corrispondenti a quelle previste nelle disposizioni di recepimento nazionali ma sono stabilite in cifra fissa (quindi senza indicare una sanzione minima e massima). Le ammende variano da un livello minimo di 50 mila euro a un massimo di 125 mila euro.

Il comma 9 dell'articolo 21 prevede che in caso di **reiterazione** la sanzione prevista è aumentata fino al triplo. Secondo quanto previsto dall'articolo 8-bis della legge n. 689 del 1981 si ha reiterazione quando, nei cinque anni successivi alla commissione di una violazione amministrativa,

accertata con provvedimento esecutivo, lo stesso soggetto commette un'altra violazione della stessa indole. Si ha reiterazione anche quando più violazioni della stessa indole commesse nel quinquennio sono accertate con unico provvedimento esecutivo. Per violazioni della stessa indole si intendono le violazioni della medesima disposizione e quelle di disposizioni diverse che, per la natura dei fatti che le costituiscono o per le modalità della condotta, presentano una sostanziale omogeneità o caratteri fondamentali comuni.

Quanto alle **procedure applicabili all'accertamento e all'irrogazione delle sanzioni** si applicano le disposizioni contenute nel capo I e II della legge n.689 del 1981.

La legge 24 novembre 1981, n. 689 *(Modifiche al sistema penale)* definisce la sanzione amministrativa pecuniaria dichiarando che consiste "nel pagamento di una somma di denaro non inferiore a 10 euro e non superiore a 15.000 euro", tranne che per le sanzioni proporzionali, che non hanno limite massimo. Fuori dei casi espressamente stabiliti dalla legge, il limite massimo della sanzione amministrativa pecuniaria non può, per ciascuna violazione superare il decuplo del minimo (art. 10).

L'articolo 11 della legge 689/1981, in relazione ai criteri per l'applicazione delle sanzioni amministrative pecuniarie, stabilisce che nella determinazione della sanzione amministrativa pecuniaria fissata dalla legge **tra un limite minimo ed un limite massimo** (e nell'applicazione delle sanzioni accessorie facoltative), si ha riguardo alla gravità della violazione, all'opera svolta dall'agente per l'eliminazione o attenuazione delle conseguenze della violazione, nonché alla personalità dello stesso e alle sue condizioni economiche.

L'applicazione della sanzione amministrativa avviene secondo il seguente procedimento: accertamento, contestazione-notifica al trasgressore; pagamento in misura ridotta o inoltro di memoria difensiva all'autorità amministrativa: archiviazione o emanazione di ordinanza ingiunzione di pagamento da parte dell'autorità amministrativa; eventuale opposizione all'ordinanza ingiunzione davanti all'autorità giudiziaria (giudice di pace o tribunale); accoglimento dell'opposizione, anche parziale o rigetto (sentenza ricorribile per cassazione); eventuale esecuzione forzata per la riscossione delle somme.

Dal punto di vista procedimentale, occorre innanzitutto che la violazione sia accertata dagli organi di controllo competenti o dalla polizia giudiziaria (art. 13). La violazione deve essere immediatamente contestata o comunque notificata al trasgressore entro 90 giorni (art. 14); entro i successivi 60 giorni l'autore può conciliare pagando una somma ridotta pari alla terza parte del massimo previsto o pari al doppio del minimo (cd. oblazione o pagamento in misura ridotta, art. 16). In caso contrario, egli può, entro 30 giorni, presentare scritti difensivi all'autorità competente; quest'ultima, dopo aver esaminato i documenti e le eventuali memorie presentate, se ritiene sussistere la violazione contestata determina l'ammontare della sanzione con ordinanza motivata e ne ingiunge il pagamento

(cd. ordinanza-ingiunzione, art. 18). Entro 30 giorni dalla sua notificazione l'interessato può presentare opposizione all'ordinanza ingiunzione (che, salvo eccezioni, non sospende il pagamento), inoltrando ricorso all'autorità giudiziaria competente (art. 22, 22-bis). L'esecuzione dell'ingiunzione non viene sospesa e il giudizio che con esso si instaura si può concludere o con un'ordinanza di convalida del provvedimento o con sentenza di annullamento o modifica del provvedimento. Il giudice ha piena facoltà sull'atto, potendo o annullarlo o modificarlo, sia per vizi di legittimità che di merito. In caso di condizioni economiche disagiate del trasgressore, l'autorità che ha applicato la sanzione può concedere la rateazione del pagamento (art. 26) Decorso il termine fissato dall'ordinanza ingiunzione, in assenza del pagamento, l'autorità che ha emesso il provvedimento procede alla riscossione delle somme dovute con esecuzione forzata in base alle norme previste per l'esazione delle imposte dirette (art. 27). Il termine di prescrizione delle sanzioni amministrative pecuniarie è di 5 anni dal giorno della commessa violazione (art. 28).

Articolo 22
(Disposizioni finanziarie)

L’**articolo 22** contiene le disposizioni finanziarie. Gli unici oneri previsti in relazione alla disciplina contenuta riguardano quanto previsto dagli articoli 7 ed 8, rispetto ai quali si stimano oneri pari a 5 milioni di euro per l’anno 2018 e 3 milioni di euro a decorrere dall’anno 2019.Con riferimento alle altre disposizioni del decreto è invece prevista la clausola di invarianza finanziaria.

La maggior parte delle esigenze di spesa sono da ricondursi alle spese per il funzionamento del CSIRT (di cui all’articolo 8) rispetto al quale la relazione tecnica prevede una spesa per il personale pari a 1.300.000 euro annui (per un contingente massimo di 30 unità di personale) cui si aggiungono 700.000 euro annui per le spese di funzionamento. Nel 2018 si prevedono al medesimo fine spese di investimento pari a 2 milioni di euro necessari a fornire le necessarie dotazioni tecniche alla struttura.

Le spese di cui all’articolo 7, pari a 1 milione di euro annui, sono ripartiti tra i diversi NIS mentre 100 mila euro sono assegnati al Dipartimento informazioni per la sicurezza.

La copertura della spesa è assicurata mediante una corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all’articolo 41-bis della legge n. 234 del 2012.

L’articolo 41-bis della legge n. 234 del 2012 prevede che al fine di consentire il tempestivo adeguamento dell'ordinamento interno agli obblighi imposti dalla normativa europea, nei soli limiti occorrenti per l'adempimento degli obblighi medesimi e in quanto non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, è autorizzata la spesa di 10 milioni di euro per l'anno 2015 e di **50 milioni di euro annui a decorrere dall'anno 2016**. Il Fondo è istituito nello stato di previsione del Ministero dell’economia e delle finanze.

Allegato I
(Requisiti e compiti del CSIRT)

Il **CSIRT-***Computer Emergency Response Team* è definito dalla direttiva 2016/1148, all'articolo 9, quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

All'art. 8 lo schema di decreto legislativo istituisce, a tal fine, presso la **Presidenza del Consiglio dei ministri** un nuovo organismo, il **CSIRT italiano**, al quale sono attribuite – a decorrere dall'entrata in vigore del relativo decreto del Presidente del Consiglio dei ministri di organizzazione e funzionamento - le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID) e a cui sono specificatamente attribuite 30 unità di personale.

Le funzioni attribuite al CSIRT italiano sono definite (dall'art. 8, co. 4 dello schema di decreto legislativo) rinviando in gran parte ai requisiti indicati all'Allegato I.

Tale Allegato individua infatti i requisiti per il CSIRT (punto 1) e i relativi compiti (punto 2) riprendendo testualmente l'Allegato I della direttiva 2016/1148 che detta i requisiti e i compiti dei CSIRT.

I **requisiti**, di cui il CSIRT è chiamato ad assicurare la conformità dell'art. 8 dello schema di decreto legislativo e della direttiva, prevedono:

- che sia garantito un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione devono essere chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano;
- i locali del CSIRT e i sistemi informativi di supporto devono essere ubicati in siti sicuri;
- ai fini della continuità operativa, il CSIRT deve essere dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi; dispone di personale sufficiente per garantirne l'operatività 24 ore su 24; opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili "sistemi ridondanti e spazi di lavoro di *backup*".
- il CSIRT ha la possibilità, se lo ritiene, di partecipare a reti di cooperazione internazionale.

I **compiti**, che il CSIRT è chiamato ad assicurare ai sensi dell'art. 8, co. 4 e della direttiva, dello schema di decreto legislativo, sono così definiti:

- monitoraggio degli incidenti a livello nazionale;
- emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- intervento in caso di incidente;
- analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;
- partecipazione alla rete dei CSIRT.

Il CSIRT è chiamato inoltre a stabilire relazioni di cooperazione con il settore privato.

Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nelle procedure di trattamento degli incidenti e dei rischi e nei sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Allegato II
(*Operatori di servizi essenziali*)

Con riferimento al settore dell'**energia,** l'allegato individua differenti **operatori di servizi essenziali,** suddivisi nei seguenti **sottosettori**:

a) Energia elettrica.

- Gli operatori di servizi essenziali ivi individuati sono:

  - l'**impresa elettrica,** ossia la persona fisica o giuridica che svolge almeno una delle funzioni seguenti: generazione, trasporto, distribuzione, fornitura o acquisto di energia elettrica, che è responsabile per i compiti commerciali, tecnici o di manutenzione legati a queste funzioni (cfr. art. 2, co. 25-*terdecies*, del D. Lgs. n. 79/1999, *Attuazione della direttiva 96/92/CE recante norme comuni per il mercato interno dell'energia elettrica*, come modificato dal D.Lgs. n. 93/2011, recante attuazione delle direttive 2009/72/CE, 2009/73/CE e 2008/92/CE relative a norme comuni per il mercato interno dell'energia elettrica, del gas naturale e ad una procedura comunitaria sulla trasparenza dei prezzi al consumatore finale industriale di gas e di energia elettrica, nonché abrogazione delle direttive 2003/54/CE e 2003/55/CE.
  - i **gestori del sistema di distribuzione**, identificati nelle persone fisiche o giuridiche responsabili della **gestione**, della **manutenzione** e dello **sviluppo** del sistema di **distribuzione** in una data zona e delle relative interconnessioni con altri sistemi, nonché di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di distribuzione di energia elettrica (cfr. art. 2, co. 25-*ter*, del citato D. Lgs. n. 79/1999);
  - i **gestori del sistema di trasmissione,** identificati nelle persone fisiche o giuridiche responsabili della **gestione**, della **manutenzione** e dello **sviluppo** del sistema di **trasmissione** in una data zona e delle relative interconnessioni con altri sistemi, e di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di trasmissione di energia elettrica (cfr. art. 2, co. 25-bis, del citato D. Lgs. n. 79/1999).

In Italia, **Terna S.p.A.** è **concessionaria dello Stato** (per venticinque anni a decorrere dal 1° novembre 2005) del servizio pubblico di trasmissione e dispacciamento dell'energia elettrica ed è **proprietaria** e **gestrice** della **Rete elettrica di Trasmissione Nazionale (RTN), detenendo la quasi totalità delle linee della RTN medesima**. Terna ha il compito di garantire la sicurezza, continuità, affidabilità e minor costo del servizio elettrico e la società a tal fine si impegna a gestire le attività di esercizio, manutenzione e sviluppo della Rete elettrica nazionale. La società esercita le sue funzioni di gestore della Rete attraverso **TERNA Rete Elettrica Nazionale S.p.A**., società da essa totalmente partecipata.

b) Petrolio.

- Gli operatori di servizi essenziali ivi individuati sono:
  - i gestori di oleodotti;
  - i gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio.

c) Gas.

- Gli **operatori di servizi essenziali** ivi individuati, secondo le definizioni contenute nel D.Lgs. n. 164/2000, *Attuazione della direttiva 98/30/CE recante norme comuni per il mercato interno del gas naturale*, come modificato dal D. Lge. 93/2011sono:
  - le **imprese fornitrici,** ossia le persone fisiche o giuridiche che svolgono funzioni di fornitura;
  - i **gestori del sistema di distribuzione**, identificati nelle persone fisiche o giuridiche che svolgono la funzione di distribuzione e sono responsabili della **gestione**, della **manutenzione** e, se necessario, dello **sviluppo** del sistema di distribuzione in una data zona ed, eventualmente, delle relative interconnessioni con altri sistemi, nonché di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di distribuzione di gas naturale;
  - i **gestori del sistema di trasmissione**, identificati nelle persone fisiche o giuridiche che svolgono l'attività di trasporto e sono responsabili della **gestione**, della **manutenzione** e, se necessario, dello **sviluppo** del sistema di trasporto in una data zona ed, eventualmente, delle relative interconnessioni con altri sistemi, nonché di assicurare la capacità a lungo termine del sistema di soddisfare richieste ragionevoli di trasporto di gas naturale.

- i **gestori dell'impianto di stoccaggio**, intesi quali persone fisiche o giuridiche che svolgono l'attività di stoccaggio e sono responsabili della gestione di un impianto di stoccaggio di gas naturale
- i **gestori del sistema GNL,** ossia le persone fisiche o giuridiche responsabili della liquefazione del gas naturale o dell'importazione, o dello scarico, e della rigassificazione di GNL, e responsabili della gestione di un impianto di GNL
- le **imprese di gas naturale,** ossia le persone fisica o giuridiche, esclusi i clienti finali, che svolgono almeno una delle seguenti funzioni: produzione, trasporto, distribuzione, fornitura, acquisto o stoccaggio di gas naturale, compresa la rigassificazione di GNL e che sono responsabili per i compiti commerciali, tecnici o di manutenzione legati a queste funzioni
- i gestori di impianti di raffinazione e trattamento di gas naturale.

In Italia, **Snam Rete Gas** è la società, interamente controllata dalla *holding* Snam, che progetta, realizza e gestisce le infrastrutture per il servizio pubblico di **trasporto**, **dispacciamento**, **telecontrollo** e **misura** del gas: Snam Rete Gas è **operatore indipendente** secondo quanto previsto dal D. Lgs. n. 93/2011, di recepimento delle direttive 2009/72/CE e 2009/73/CE relative alle norme comuni per il mercato interno dell'energia elettrica e del gas naturale.

Trasporti

Trasporto aereo.

Per **vettore aereo** si intende un'impresa di trasporto aereo titolare di una licenza di esercizio valida o documento equivalente.

Per **gestore aeroportuale** si intende il soggetto al quale le disposizioni legislative, regolamentari o contrattuali affidano, insieme con altre attività o in via esclusiva, il compito di amministrare e di gestire le infrastrutture aeroportuali o della rete aeroportuale e di coordinare e di controllare le attività dei vari operatori presenti negli aeroporti e nella rete aeroportuale di interesse.

Per **aeroporto** qualsiasi terreno appositamente predisposto per l'atterraggio, il decollo e le manovre di aeromobili, inclusi gli impianti annessi che esso può comportare per le esigenze del traffico e per il servizio degli aeromobili nonché gli impianti necessari per fornire assistenza ai servizi aerei commerciali.

A questo proposito con il decreto del Presidente della Repubblica 17 settembre 2015, n. 201 sono stati individuati gli aeroporti di interesse nazionale, a norma dell'articolo 698 del codice della navigazione. Il **Piano** classifica come "**aeroporti di interesse nazionale" 38 aeroporti**, suddivisi in **10 bacini territoriali** di traffico e, in tale ambito, gli aeroporti che presentano particolare rilevanza strategica nonché i gate intercontinentali (Roma Fiumicino, primario hub nazionale, Milano Malpensa e Venezia).

Nell'elenco allegato al Regolamento (UE) 1315/2013 sono riportati 33 aeroporti 11 afferenti alla Rete *core* (centrale) europea e 23 della rete globale.

per **operatori attivi nel controllo della gestione del traffico** che forniscono servizi per il controllo del traffico aereo, definito come un servizio finalizzato a prevenire collisioni tra aeromobili e nell'area di manovra tra aeromobili e ostacoli nonché ad accelerare il flusso di traffico aereo e mantenerlo ordinato.

Ai sensi dell'articolo 691-bis del codice della navigazione l'ENAV "fatta salva l'attuazione delle previsioni della normativa comunitaria" rappresenta il principale destinatario dei compiti connessi alla gestione del traffico aereo. Tra le altre funzioni spetta infatti ad ENAV svolgere i servizi di controllo del traffico aereo, comprensivi dei servizi di controllo di area, dell'avvicinamento e dell'aeroporto; i servizi di informazioni volo; i servizi consultivi sul traffico aereo; i servizi di allarme. Ad Enav spetta anche il compito di disciplinare e controllare, per gli aeroporti di competenza, la movimentazione degli aeromobili, degli altri mezzi e del personale sull'area di manovra e di assicurare l'ordinato movimento degli aeromobili sui piazzali, sotto la vigilanza dell'ENAC e coordinandosi col gestore aeroportuale.

I servizi del traffico aereo sono svolti da personale in possesso di apposita licenza o certificazione. Sotto il profilo organizzativo Enav garantisce l'assistenza alla navigazione a tutti gli aeromobili che sorvolano il Paese oppure che atterrano presso un aeroporto nazionale, attraverso quattro Centri di Controllo d'Area (ACC) che si trovano a Roma, Milano, Padova e Brindisi e che hanno competenza su specifici ambiti territoriali. Enav è inoltre responsabile dei servizi alla navigazione aerea di 45 aeroporti civili italiani attraverso le Torri di controllo da cui sono gestiti decolli, atterraggi nonché la movimentazione al suolo degli aeromobili.

Trasporto ferroviario.

Per **gestore dell'infrastruttura ferroviaria** si intende il soggetto incaricato, in particolare, della realizzazione, della gestione e della

manutenzione dell'infrastruttura ferroviaria, compresa la gestione del traffico, il controllo-comando e il segnalamento. In Italia il gestore dell'infrastruttura ferroviaria nazionale è **Rete ferroviaria italiana**. Accanto alla rete nazionale sono presenti in Italia reti ferroviarie, sia interconnesse con la rete ferroviaria nazionale, che non interconnesse con la stessa (in tal caso denominate reti isolate), le quali sono **gestite** da **soggetti diversi dal gestore della rete nazionale** (ad esempio la società Ferrovienord gestisce 320 chilometri di rete nella regione Lombardia);

Per **impresa ferroviaria si intende** qualsiasi impresa pubblica o privata titolare di una licenza, la cui attività principale consiste nella prestazione di servizi per il trasporto sia di merci sia di persone per ferrovia e che garantisce obbligatoriamente la trazione; sono comprese anche le imprese che forniscono solo la trazione. L'elenco delle imprese ferroviarie titolari di licenza con indicazione della tipologia e del relativo stato è disponibile qui. .

Trasporto per vie d'acqua.

Nel settore **del trasporto per via d'acqua**, in base alla direttiva 2016/1148, gli obblighi di sicurezza per le compagnie, le navi, gli impianti portuali, i porti e i servizi di gestione del traffico navale, riguardano tutte le operazioni, compresi i sistemi di radio e telecomunicazione, i sistemi informatici e le reti. Una parte delle procedure obbligatorie da seguire prevede la segnalazione di tutti gli incidenti.

Le **compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri** e **merci** sono definite, secondo l'allegato II ai sensi dell'allegato I del regolamento (CE) n. 725/2004 che ha modificato la Convenzione SOLAS dell'Organizzazione Marittima internazionale (IMO) per la salvaguardia della vita umana in mare. In tale allegato si rinvia, per la definizione di "società" alla Regola IX/1 della Convenzione SOLAS[6].

Il decreto del Ministro dei trasporti 18 dicembre 1995, che recepisce il capitolo IX della Convenzione SOLAS, specifica, all'articolo 2, lettera g, che per **compagnia** si intende **l'armatore della nave o qualsiasi altra entità o persona, che abbiano assunto dall'armatore la responsabilità dell'esercizio della nave** e che, nell'assumere tale responsabilità, si siano

[6] La Convenzione definisce, alla regola IX/1, la compagnia di navigazione in tal modo: "Company means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code". Come si vede la definizione coincide letteralmente con quanto indicato nel decreto ministeriale.

dichiarati d'accordo di rilevare tutti gli obblighi e responsabilità imposte dal Codice ISM.

Sono escluse le singole navi gestite dalla compagnia.

Nei *considerando* della direttiva 2016/1148 si evidenzia che nell'identificare gli operatori nel settore del trasporto per via d'acqua, gli Stati membri dovrebbero tener conto dei codici internazionali e delle linee guida attuali e futuri sviluppati in particolare dall' Organizzazione marittima internazionale, al fine di fornire ai singoli operatori marittimi un approccio coerente.

Alla luce di tali considerazioni andrebbe valutata l'opportunità di rinviare direttamente al citato decreto ministeriale, ai fini dell'individuazione delle compagnie di navigazione.

In relazione agli **organi di gestione dei porti,** viene definita come **porto** quella specifica area terrestre e marittima, comprendente impianti ed attrezzature intesi ad agevolare le operazioni commerciali di trasporto marittimo, che ha al suo interno uno o più impianti portuali dotati di un piano di sicurezza approvato a norma del regolamento (CE) n. 725/2004, e che forniscono servizi alle navi di cui alla regola 2, cap. XI-2 Convenzione SOLAS o alle navi di cui all'articolo 3, comma 2, del regolamento. Vi sono compresi i **relativi impianti portuali,** cioè i luoghi in cui avviene l'interfaccia nave/porto, che comprende aree quali le zone di ancoraggio, di ormeggio e di accosto dal mare.

Nel nostro ordinamento, la legge n. 84/1994 prevede una pluralità di **soggetti che operano nei porti**: le 15 Autorità di Sistema Portuale (AdSP) alle quali appartengono i porti di maggiore rilevanza nazionale (elencati in Allegato A della legge), gli uffici territoriali portuali costituiti dalle AdSP, presso ciascun porto sede di Autorità portuale, le organizzazioni portuali legislativamente costituite in alcuni porti italiani, le autorità marittime che sono preposte alle zone marittime come definite dall'art. 16 del Codice della navigazione.

I gestori di servizi di assistenza al traffico marittimo sono i gestori del «servizio di assistenza al traffico marittimo (VTS)», finalizzato a migliorare la sicurezza della navigazione e l'efficienza del traffico marittimo e a tutelare l'ambiente, in grado di interagire con le navi che transitano nell'area coperta dal VTS.

Trasporto su strada

Per **autorità stradale responsabile del controllo della gestione del traffico** si intende (in base regolamento delegato UE 2015/962) qualsiasi autorità pubblica responsabile della pianificazione, del controllo o della gestione delle strade che rientrano nella sua competenza territoriale.

Gestori di sistemi di trasporto intelligenti

I **sistemi di trasporto intelligenti (ITS)** sono definiti (articolo l, comma l, lettera a), del decreto del Ministro delle infrastrutture e dei trasporti 11 febbraio 2013) come le tecnologie informatiche e della comunicazione applicate ai sistemi di trasporto, alle infrastrutture, ai veicoli e alla gestione del traffico e della mobilità. Alla lett. c) sono definiti i **fornitori** di servizi ITS come i fornitori pubblici o privati di servizi ITS. L'art. 10 del decreto ha disposto l'istituzione presso il Ministero delle infrastrutture e dei trasporti, del Comitato di indirizzo e coordinamento delle iniziative in materia di ITS, denominato ComITS.

Infrastrutture digitali

IXP

è il **punto di interscambio internet**, una infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; in sostanza la sua funzione è quella di interconnettere le reti. Un IXP non fornisce accesso alla rete, né funziona da fornitore o carrier di transito. Non fornisce neppure altri servizi non correlati all'interconnessione, per quanto ciò non impedisca a un operatore IXP di fornire servizi non correlati. Lo scopo di un IXP è quindi connettere reti tecnicamente e organizzativamente separate. Per descrivere una rete tecnicamente indipendente si usa l'espressione sistema autonomo.

DNS

è il **sistema dei nomi di dominio**, un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio.

TLD

il **registro dei nomi di dominio di primo livello** *(top-level domain),* il soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello. L'Internet Assigned Numbers Authority (IANA)**,** è l'organismo che ha responsabilità nell'assegnazione degli indirizzi IP, e classifica attualmente i domini di primo livello. Si tratta ad esempio dei domini nazionali (come *.it* per l'Italia), ovvero di quelli generici (ad esempio *.com* oppure *.gov*).

Per il settore sanitario, sottosettore Istituti sanitari (compresi ospedali e cliniche private), sono identificati i *Prestatori di assistenza sanitaria*, definiti - ai sensi dell'articolo 3, comma 1, lettera *h)*, del D. Lgs. 38/2014 di recepimento della Direttiva 2011/24/UE sull'assistenza sanitaria

transfrontaliera in ambito UE. - “una qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro dell'Unione europea”.

Settore bancario: per *ente creditizio* si intende un'impresa la cui attività consiste nel raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto.

Infrastrutture dei mercati finanziari: per *gestori delle sedi di negoziazione* si intende gestori di un mercato regolamentato, di un sistema multilaterale di negoziazione (alternativo ai mercati regolamentati) il cui esercizio è riservato ad imprese di investimento, banche e gestori dei mercati regolamentati, o di un sistema organizzato di negoziazione.

Per *controparte centrale* si intende il soggetto che si interpone tra le controparti di contratti negoziati su uno o più mercati finanziari agendo come acquirente nei confronti di ciascun venditore e come venditore nei confronti di ciascun acquirente, evitando che questi siano esposti al rischio di inadempienza della propria controparte contrattuale e garantendo il buon fine dell’operazione.

Allegato III
(*Definizioni di servizio digitale)*

L’allegato III rega le definizioni di servizio digitale, ai sensi dell'articolo l, paragrafo l, lettera b), della direttiva (UE) 2015/1535, cui rinvia l’art. 3, co. 1 lett. h) dello schema di decreto.

Mercato online

un servizio digitale che consente ai consumatori e/o ai professionisti, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online

Motore di ricerca online

un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto.

Servizi di cloud computing

Si tratta di servizi che coprono un'ampia gamma di attività che possono essere fornite sulla base di modelli diversi. La direttiva UE n. 2016/1148 nell’espressione *cloud computing* comprende i servizi che consentono l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

Documenti all'esame delle istituzioni dell'UE

È all'esame delle Istituzioni legislative europee la proposta (COM(2017)477) di riforma del quadro giuridico dell'ENISA, l'Agenzia per la sicurezza delle reti e dell'informazione, istituita nel 2003, il cui temporaneo mandato (2013-2020) concerne il **sostegno** alle **Istituzioni europee**, agli **Stati membri**, e alle **imprese** nell'**affrontare**, **risolvere** e in particolare **prevenire** i problemi di sicurezza delle reti e dell'informazione.
Attualmente il mandato dell'ENISA concerne cinque settori di intervento:

- **competenza**: fornire **informazioni** e **competenze** sulle principali questioni relative alla sicurezza delle reti e dell'informazione;
- **politica**: sostenere l'**elaborazione** e l'**attuazione** delle politiche dell'Unione;
- **capacità**: contribuire allo sviluppo delle **capacità** in tutta l'Unione (ad esempio attraverso **attività di formazione**, **raccomandazioni**, attività di sensibilizzazione);
- **comunità**: promuovere la comunità della sicurezza delle reti e delle informazioni (ad esempio sostegno alle **squadre di pronto intervento** informatico delle istituzioni, degli organi e delle agenzie europee (Computer Emergency Response Teams - CERT), coordinamento delle esercitazioni paneuropee di cibersicurezza);
- **facilitazione**: ad esempio **collaborazione con i portatori d'interessi** e avvio di relazioni internazionali.

La proposta, presentata dalla Commissione europea il 22 febbraio 2018, reca inoltre l'istituzione di un sistema di certificazione della cibersicurezza dei prodotti e dei servizi TIC nell'Unione.

Deve ricordarsi che già nel corso dei negoziati relativi alla direttiva NIS, i colegislatori dell'UE hanno deciso di attribuire importanti funzioni all'ENISA nell'applicazione di tale disciplina. In particolare, l'Agenzia assicura le funzioni di **segretariato della rete di CSIRT** e di **assistenza al gruppo di cooperazione** nell'esecuzione dei suoi compiti. Inoltre, la direttiva dispone che l'ENISA assista gli Stati membri e la Commissione mettendo loro a disposizione le proprie competenze e consulenze e agevolando lo scambio di migliori pratiche.

La proposta, proprio al fine di una coerente attuazione della direttiva NIS, conferisce all'Agenzia (significativamente ridenominata Agenzia dell'UE per la cibersicurezza) un **mandato permanente** volto a consolidare il ruolo di punto di riferimento nell'ecosistema della sicurezza cibernetica con particolare riguardo all'assistenza degli Stati membri nell'applicazione del diritto dell'UE, nella capacità operativa di fronte a determinate minacce (ad esempio tramite l'organizzazione di **esercitazioni paneruopee** e di meccanismi **condivisione** e **analisi** delle informazioni relative ai rischi di

attacchi informatici), e nella realizzazione del citato **sistema di certificazione** dei prodotti TIC.

Non vi sono disposizioni della disciplina tuttora all'esame dell'UE volte a modificare la direttiva NIS che si intende attuare con il provvedimento del Governo.