## RELAZIONE ILLUSTRATIVA

Lo schema di decreto legislativo recepisce la direttiva (UE) 2016/1148 (cd. Direttiva NIS - Network and Information Security) sulla sicurezza delle reti e dei sistemi informativi nell'Unione adottata il 6 luglio 2016, che per la prima volta affronta in modo organico e trasversale gli aspetti in materia di *cyber security*, rafforzando la resilienza e la cooperazione in Europa.

Lo schema di decreto legislativo consegue tre obiettivi principali:

- promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali;
- migliorare le capacità nazionali di *cyber security*;
- rafforzare la cooperazione a livello nazionale e in ambito UE.

A tal fine lo schema di decreto legislativo, allo scopo di assicurare la continuità dei servizi essenziali (energia, trasporti, salute, finanza, ecc.) e dei servizi digitali (motori di ricerca, servizi cloud, piattaforme di commercio elettronico), prevede l'adozione di misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici e l'obbligo di notifica di incidenti con impatto rilevante sulla fornitura dei servizi. Parallelamente individua le Autorità competenti NIS e i rispettivi compiti svolti in cooperazione con le omologhe Autorità degli Stati Membri dell'UE, nonché il CSIRT (Computer Security Incident Response Team) italiano con compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri CSIRT europei e il 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.

Si riporta di seguito la descrizione dell'articolato della proposta di decreto.

Il CAPO I "Disposizioni generali" contiene gli articoli da 1 a 5.

L'Articolo 1 definisce le finalità e l'ambito di applicazione del decreto. Nell'ottica di rafforzare la sicurezza informatica nazionale per un livello comune elevato di sicurezza, sono individuati gli obiettivi specifici che mirano a migliorare l'organizzazione e le capacità tecniche nazionali, nonché a ridurre il rischio di incidenti informatici che possano inficiare i servizi digitali, ed in particolare i servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali. Gli obiettivi specifici riguardano: l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi che rientrano nell'ambito di applicazione del decreto; la designazione delle Autorità competenti NIS e del Punto di contatto unico nonché del CSIRT; l'adozione di misure di sicurezza e l'obbligo di notifica degli incidenti informatici, con impatto rilevante sulla fornitura dei servizi, da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali; la cooperazione con gli Stati membri dell'UE. La norma stabilisce che le disposizioni del decreto non si applicano ai fornitori di reti e servizi di comunicazione elettronica né ai fornitori di servizi fiduciari e che le stesse non inficiano la normativa vigente riguardante le infrastrutture critiche europee, la lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile nonché gli attacchi contro i sistemi di informazione in termini di definizione

dei reati e delle relative sanzioni. E' 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. L'articolo stabilisce infine che, in presenza di specifico atto giuridico dell'Unione avente ad oggetto obblighi per le Imprese interessate dal decreto, tale atto continua ad applicarsi se gli obblighi in esso fissati sono almeno equivalenti a quelli del decreto.

L' Articolo 2 stabilisce che il trattamento dei dati personali sia effettuato ai sensi del decreto legislativo del 30 giugno 2003 n. 196, recante il codice in materia di dati personali.

L'articolo 3 riporta le definizioni adottate nell'ambito del decreto conformemente a quelle indicate dalla Direttiva NIS, introducendo ulteriori definizioni al fine di chiarire il contesto nazionale di riferimento, tra le quali vanno ricordate quelle relative a: Autorità competente NIS, CSIRT, Punto di contatto unico e Autorità di contrasto.

L'articolo 4 stabilisce che sia istituito un elenco degli operatori di servizi essenziali con sede nel territorio nazionale. Tali operatori sono individuati entro il 9 novembre 2018 a cura delle Autorità competenti NIS, sulla base del tipo di servizio offerto e dalla relativa dipendenza dalla rete e dai sistemi informativi nonché della gravità degli effetti che un incidente informatico potrebbe produrre sulle attività sociali e/o economiche fondamentali. Oltre ai predetti criteri le Autorità competenti NIS possono riferirsi ai documenti prodotti al riguardo dal Gruppo di cooperazione di cui all'articolo 10. Si stabilisce, in particolare, che gli operatori che prestano attività di assistenza sanitaria siano individuati con decreto del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano, mentre quelli che forniscono e distribuiscono acque destinate al consumo umano, siano individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano. L'articolo stabilisce, inoltre, che qualora un operatore di servizi essenziali fornisca servizi in più Stati dell'Unione Europea, l'identificazione degli operatori di servizi essenziali richiede un coordinamento tra gli Stati coinvolti. Si stabilisce che da parte del punto di contatto unico siano comunicate alla Commissione Europea, entro il 9 novembre 2018 e, successivamente ogni due anni, le informazioni necessarie per la valutazione della coerenza dell'approccio in merito all'identificazione degli operatori di servizi essenziali. Viene definito il contenuto minimo che, in ogni caso, le predette informazioni devono comprendere.

L'articolo 5 individua, ai fini dell'identificazione degli operatori di servizi essenziali, gli elementi da considerare per valutare l'impatto negativo di malfunzionamenti dovuti ad incidenti informatici sulla fornitura di servizi essenziali. Tra questi, sono previsti il numero di utenti, la quota di mercato dell'operatore, l'area interessata dal malfunzionamento ed eventuali altri fattori di tipo settoriale.

Il CAPO dedicato al contesto strategico e istituzionale contiene gli articoli dal 6 al 9.

L'articolo 6 prevede l'adozione da parte del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CSIRT), della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale, con particolare riguardo ai settori collegati ai servizi essenziali, indicati in allegato II e ai servizi digitali

riportati nell'allegato III. Con la medesima procedura prevede altresì l'adozione di linee di indirizzo per l'attuazione della stessa strategia. La strategia deve prevedere in particolare le misure di preparazione, risposta e recupero dei servizi a seguito di incidenti informatici, la definizione di un piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione in materia di sicurezza informatica. La Presidenza del Consiglio dei ministri trasmette la strategia nazionale di sicurezza cibernetica alla Commissione europea entro tre mesi dalla sua adozione. Viene inoltre prevista la possibilità che sia esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.

L'articolo 7 individua le Autorità competenti responsabili dell'attuazione del decreto con riferimento ai settori di cui all'allegato II e i servizi di cui all'allegato III del medesimo decreto. Il Dipartimento delle Informazioni per la Sicurezza - DIS della Presidenza del Consiglio dei Ministri è designato quale punto di contatto per svolgere funzioni di collegamento verso l'Unione Europea e gli Stati membri, anche nell'ambito del Gruppo di cooperazione di cui all'articolo 10 e della rete di CSIRT di cui all'articolo 11. Le autorità competenti NIS e il Punto di contatto unico consultano, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi. Le designazioni del punto di contatto unico e delle autorità NIS sono comunicate dalla Presidenza del Consiglio dei ministri alla Commissione europea ed adeguatamente pubblicizzate.

L'articolo 8 istituisce, presso la Presidenza del Consiglio dei Ministri, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-bis, del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51, del decreto legislativo 7 marzo 2005, n. 82. L'organizzazione e il funzionamento del CSIRT italiano sono disciplinati con decreto del Presidente del Consiglio dei Ministri ai sensi dell'articolo 7 del decreto legislativo 30 luglio 1999, n. 303. Per lo svolgimento delle funzioni di cui al presente articolo, la Presidenza del Consiglio dei ministri si avvale 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, per i quali si applica l'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e quindici da assumere in aggiunta alle ordinarie facoltà assunzionali della Presidenza del Consiglio dei ministri; nelle more dell'adozione del predetto decreto del Presidente del Consiglio dei Ministri, le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro. Il CSIRT italiano assicura la conformità ai requisiti di cui all'allegato I, punto 1, svolge i compiti di cui all'allegato I, punto 2, si occupa dei settori di cui all'allegato II e dei servizi di cui all'allegato III e dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale. Il CSIRT italiano definisce le procedure per la prevenzione e la gestione degli incidenti informatici e garantisce la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT di cui all'articolo 11. La Presidenza del Consiglio dei ministri comunica alla Commissione europea il mandato del CSIRT italiano e le modalità di trattamento degli incidenti a questo affidati. Il CSIRT italiano, per lo svolgimento delle proprie funzioni, può avvalersi anche dell'Agenzia per l'Italia digitale. E' disciplinata quindi la decorrenza del trasferimento al CSIRT italiano delle funzioni svolte dal Ministero dello sviluppo economico in qualità di CERT nazionale ai sensi dell'articolo 16-bis, del decreto legislativo 1° agosto 2003, n. 259, nonché di quelle svolte da

Agenzia per l'Italia digitale in qualità di CERT-PA, ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

L'articolo 9 prevede la collaborazione delle Autorità competenti NIS con il punto di contatto unico e con il CSIRT Nazionale ed istituisce, inoltre, un Comitato tecnico di raccordo, composto da rappresentanti delle amministrazioni statali competenti NIS, e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano. Si stabilisce, infine, che gli operatori di servizi essenziali e i fornitori di servizi digitali inviino le notifiche relative ad incidenti al CSIRT Italiano che ne dà informazione alle autorità competenti NIS e al punto di contatto unico.

Il CAPO III "COOPERAZIONE" contiene gli articoli 10 e 11.

L'articolo 10 prevede la partecipazione al Gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione) ed elenca i compiti del medesimo Gruppo, tra cui lo scambio di buone pratiche e lo scambio di informazioni sulle notifiche degli incidenti, sulla sensibilizzazione e formazione e in materia di ricerca e sviluppo.

L'articolo 11 prevede la partecipazione del CSIRT italiano alla rete di CSIRT, composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE, assicurando in particolare lo scambio di informazioni sugli incidenti informatici.

Il CAPO IV "Sicurezza della rete e dei sistemi informativi degli operatori dei servizi essenziali" contiene gli articoli 12 e 13.

L'articolo 12 prevede che operatori di servizi essenziali adottino misure tese a ridurre i rischi informatici e minimizzare gli impatti sulla continuità dei servizi essenziali tenendo in debita considerazione i documenti prodotti al riguardo dal Gruppo di cooperazione di cui all'articolo 10 e di eventuali linee guida predisposte dalle Autorità competenti NIS, fatta salva la possibilità per le medesime Autorità di definire specifiche misure, sentiti gli operatori di servizi essenziali. Questi ultimi sono inoltre tenuti a notificare al CSIRT (il quale supporta gli operatori per agevolare il trattamento efficace dell'incidente), e per conoscenza alla autorità competente NIS, senza ingiustificato ritardo, gli incidenti con impatto rilevante sulla continuità dei servizi essenziali. A tal fine sono individuati i parametri da tenere in considerazione per valutare la rilevanza del suddetto impatto, ovvero il numero degli utenti coinvolti, la durata dell'incidente e l'area geografica interessata. Viene altresì previsto che le notifiche vengano tempestivamente inoltrate dal CSIRT italiano all'organo istituito presso il Dipartimento delle informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri, adottate sentito il CISR, delle attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento. Viene precisato che la notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente. Le modalità di notifica degli incidenti possono essere oggetto di specifiche linee guida predisposte dalle Autorità competenti NIS. L'articolo prevede altresì un coordinamento con altre Autorità o CSIRT europei qualora l'incidente sia esteso a più Stati Membri. Ove possibile, l'Autorità competente NIS d'intesa con il CSIRT

Italiano italiano, previa valutazione da parte dell'organo di cui all'art. 12, comma 6, può divulgare le informazioni sentito lo stesso operatore interessato dall'incidente.

L'articolo 13 stabilisce che l'Autorità competente valuti il rispetto degli obblighi imposti agli operatori di servizi essenziali. A tal fine, questi ultimi sono altresì tenuti a fornire ogni utile informazione e dimostrazione dell'effettiva attuazione delle policy di sicurezza informatica e ad applicare eventuali istruzioni vincolanti predisposte dall'Autorità competente dalle autorità competenti NIS.

Il CAPO V "Sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali" contiene gli articoli da 14 a 16.

L'articolo 14 fissa obblighi a carico dei fornitori di servizi digitali di cui all'allegato 3. Tali obblighi riguardano l'adozione di misure tecnico-organizzative per la gestione dei rischi e per la riduzione dell'impatto di eventuali incidenti informatici, nonché la notifica al CSIRT italiano e, per conoscenza, alla relativa Autorità competente NIS, senza ingiustificato ritardo, di incidenti con impatto significativo. Viene precisato che la notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente. L'articolo definisce, altresì, i parametri utili a valutare l'impatto dell'incidente notificato e i casi in cui si applica l'obbligo di notifica di un incidente e quello di notifica di qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di un operatore di servizi essenziali che si avvalga di un fornitore di servizi digitali. L'articolo prevede altresì un coordinamento con altre Autorità competenti o CSIRT europei qualora l'incidente sia esteso a più Stati Membri. Ove necessario, l'Autorità competente NIS d'intesa con il CSIRT Italiano, previa valutazione da parte dell'organo di cui all'art. 12, comma 6, può divulgare le informazioni relative all'incidente notificato, sentito lo stesso fornitore. L'articolo precisa altresì che i fornitori di servizi digitali sono tenuti all'applicazione degli atti di esecuzione della Commissione Europea che precisano gli obblighi sopra descritti. Le disposizioni del Capo V non si applicano alle microimprese e alle piccole imprese quali definite nella raccomandazione della Commissione europea n. 2003/361/CE.

L'articolo 15 stabilisce che, qualora sia dimostrato il mancato rispetto degli obblighi imposti ai fornitori di servizi digitali, l'autorità competente può adottare misure di vigilanza ex post adeguate alla natura dei servizi e delle operazioni successivamente al verificarsi di un incidente. A tal fine si stabilisce che i fornitori di servizi digitali sono tenuti a fornire ogni utile informazione e a porre rimedio a qualsiasi mancato adempimento. L'articolo prevede altresì il coordinamento delle Autorità competenti di più Stati membri qualora il fornitore di servizi essenziali operi in diversi Stati membri.

L'articolo 16, regolando la disciplina della giurisdizione, stabilisce che un fornitore di servizi digitali è considerato soggetto allo Stato membro in cui ha lo stabilimento principale e di seguito che un fornitore di servizi digitali è considerato avere il proprio stabilimento principale in uno Stato membro quando ha la sua sede sociale n in tale Stato membro con la conseguenza che i fornitori di servizi digitali che hanno la sede sociale in Italia sono soggetti alla giurisdizione italiana. Inoltre, si prevede che Nel caso in cui un fornitore di servizi digitali, non stabilito nell'UE, nel caso in cui

fornisca servizi negli Stati membri, è sia tenuto a designare un rappresentante in uno Stato membro ed è soggetto e assoggettato alla sua giurisdizione.

Il CAPO VI "NORMAZIONE E NOTIFICA VOLONTARIA" contiene gli articoli 17 e 18.

L'articolo 17 prevede che, ai fini di un'attuazione armonizzata degli obblighi a carico degli operatori di servizi essenziali e dei fornitori di servizi digitali, sia promossa l'adozione di norme europee o internazionali senza privilegiare particolari tecnologie; dispone inoltre che le Autorità competenti tengano altresì conto delle linee guida e dei pareri formulati dall'Agenzia ENISA.

L'articolo 18 prevede la possibilità, per i soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali ai sensi dell'allegato III, di notificare, su base volontaria, al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi da essi forniti. Le notifiche obbligatorie sono trattate prioritariamente rispetto alle notifiche volontarie che, a loro volta, vengono trattate solo se tale trattamento non costituisca un onere sproporzionato o eccessivo.

Il CAPO VII "Disposizioni finali" contiene gli articoli da 19 a 22.

L'articolo 19 stabilisce che le attività di ispezione e verifica – che restano ordinariamente regolate, quanto al loro esercizio, dalla legge n. 241/1990 – necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte dalle autorità competenti NIS.

L'articolo 20 individua le Autorità competenti – tra le quali sono ricomprese anche le Regioni e le Province autonome di Trento e Bolzano, rispettivamente, per l'attività di assistenza sanitaria e la fornitura e distribuzione di acqua potabile – ed il regime di accertamento ed irrogazione delle sanzioni di cui al presente decreto, regolando altresì l'applicazione della legge 24 novembre 1981, n. 689.

L'articolo 21 stabilisce che in caso di violazione da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali degli obblighi previsti nel decreto, le Autorità competenti applicano una sanzione amministrativa il cui importo varia da dodicimila euro a centocinquantamila euro, differenziando per operatori di servizi essenziali e fornitori di servizi digitali nonché per tipo di violazione e disponendo circa la reiterazione delle condotte. Quanto alla minor gravità delle sanzioni relative ai fatti commessi da un fornitore di servizio digitale, si rimanda al criterio sotteso al "considerando" 49 della direttiva NIS, secondo cui, «I fornitori di servizi digitali dovrebbero garantire un livello di sicurezza commisurato al grado di rischio per la sicurezza dei servizi digitali da essi forniti, data l'importanza dei loro servizi per le operazioni di altre imprese all'interno dell'Unione. In pratica, per gli operatori di servizi essenziali che spesso sono essenziali per il mantenimento delle attività sociali ed economiche critiche, il grado di rischio è più elevato che per i fornitori di servizi digitali. Pertanto, gli obblighi di sicurezza per i fornitori di servizi digitali dovrebbero essere meno rigidi». Da ciò deriva, sulla base del principio stabilito dall'articolo 21 della direttiva, secondo cui, «Le sanzioni previste sono effettive, proporzionate e dissuasive», l'esigenza di differenziare le sanzioni per i comportamenti collegati alle attività imposte dal diverso modello di governance previsto dalla direttiva per i fornitori di servizi digitali, tenendo tuttavia

presente che per talune violazioni (ad es. quelle di cui ai commi 3 e 6, concernenti l'obbligo di notifica si è prevista la stessa sanzione, senza differenziarla in base alla natura del operatore in quanto si è ritenuta di pari gravità. In particolare, gli obblighi che rilevano per l'applicazione delle sanzioni, sia per gli operatori di servizi essenziali che per i fornitori di servizi digitali, riguardano la mancata o ritardata notifica degli incidenti, la mancata definizione o rispetto delle misure di sicurezza, la mancata condivisione delle informazioni richieste dall'Autorità competente NIS e della dimostrazione dell'attuazione delle politiche di sicurezza, nonché il mancato rispetto delle istruzioni emanate dall'Autorità competente NIS per porre rimedio al mancato adempimento degli obblighi riportati negli articoli dal 12 al 15.

L'articolo 22 reca le disposizioni finanziarie.

Lo schema di decreto consta di tre allegati, concernenti, rispettivamente, i "Requisiti e compiti dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)", gli "Operatori di servizi essenziali" e i "Tipi di servizi digitali". In particolare, l'allegato I, che riporta i requisiti e i compiti del CSIRT italiano, stabilisce che il CSIRT deve assicurare la disponibilità dei propri servizi di comunicazione creando delle ridondanze che evitino la presenza di "singoli punti di guasto", ovvero punti della rete particolarmente critici, il cui malfunzionamento possa comportare l'interruzione dei servizi.

## RELAZIONE TECNICA

Lo schema di decreto legislativo recepisce la direttiva (UE) 2016/1148 (cd. Direttiva NIS) sulla sicurezza delle reti e dei sistemi informativi nell'Unione adottata il 6 luglio 2016 che per la prima volta affronta in modo organico e trasversale gli aspetti in materia di cyber security, rafforzando la resilienza e la cooperazione in Europa.

In particolare, lo schema di decreto definisce obblighi a carico degli operatori di servizi essenziali (di cui all'allegato II) e dei fornitori di servizi digitali (di cui all'allegato III), prevedendo l'adozione di misure a tutela della sicurezza delle proprie reti e sistemi informatici e di notifica degli incidenti con impatto rilevante sulla continuità dei servizi.

**Articolo 7**

L'articolo 7, comma 1, individua tra le Amministrazioni centrali dello Stato e le Regioni e province autonome per i settori sanità e acque destinate al consumo umano, le Autorità competenti NIS al fine di assicurare il rispetto dei suddetti obblighi, in cooperazione con gli altri Stati Membri UE. Tale ruolo di autorità per le amministrazioni in precedenza citate è di nuova istituzione, dal momento che attualmente sono svolte unicamente dal MISE e dall'Agenzia per l'Italia digitale, rispettivamente, le funzioni di CERT nazionale ex articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259 e di CERT-PA ex articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

Le attività di attuazione e controllo attribuite alle Autorità competenti NIS delineate, in particolare, negli articoli 13 e 15 individuano nuove funzioni relative al settore della sicurezza informatica nei confronti degli operatori di servizi essenziali – che saranno individuati dalle medesime Autorità entro il 9 novembre 2018, ai sensi dell'articolo 4, comma 1, del decreto – e dei fornitori di servizi digitali.

Infine, al Punto di contatto Unico individuato nel Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri è affidato il ruolo di interfaccia verso le Istituzioni Europee nell'ottica di garantire la cooperazione transfrontaliera delle Autorità competenti NIS con le Autorità competenti degli altri Stati membri, nonché con il Gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

Per quanto riguarda il Punto di contatto unico, individuato nel Dipartimento delle informazioni per la sicurezza (DIS) dall'articolo 7, comma 3, dello schema di decreto legislativo, vengono individuate le nuove funzioni 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 di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

Le autorità competenti NIS di settore e il punto di contatto unico utilizzeranno per le attività di ispezione, accertamento e irrogazione delle sanzioni, oltre alle capacità tecnico-organizzative già esistenti, ulteriori risorse finanziarie come meglio di seguito dettagliato, per svolgere in modo efficiente ed efficace i compiti loro assegnati, così da conseguire gli obiettivi della direttiva attraverso il personale già operante presso le autorità NIS di settore. Ciò anche per la valutazione di conformità degli operatori dei servizi essenziali agli obblighi loro imposti e i relativi effetti sulla

sicurezza della rete e dei sistemi informativi, oltre che per richiedere ai medesimi operatori informazioni e prove per valutare la sicurezza della loro rete.

Per quanto concerne le attività svolte in qualità di autorità NIS di settore dal Ministero delle infrastrutture e dei trasporti, dal Ministero dello sviluppo economico, dal Ministero dell'economia e delle finanze, dal Ministero della salute e dal Ministero dell'ambiente e della tutela del territorio e del mare tra le quali rientrano anche le attività ispettive e sanzionatorie, ciò determinerà un maggior impegno finanziario dettagliato come di seguito:

a) con riferimento al Ministero delle infrastrutture e dei trasporti:

- per la necessità di rispondere adeguatamente alla rilevanza operativa della tematica della cyber security nel suo impatto – a seguito della direttiva (UE) 1148/2016 c.d. "NIS" – sul comparto infrastrutture e trasporti (sottosettori aereo, ferroviario, per vie d'acqua e su strada, come meglio definiti nell'Allegato II del decreto in oggetto);

- per la necessità di ottimizzare il rapporto tra risorse finanziare concretamente ad oggi stimate (peraltro con i vincoli derivanti dal contesto economico nazionale) ed efficacia delle attività correlate alla migliore applicazione della Direttiva NIS;

- per l'implementazione/valorizzazione delle forme di collaborazione con gli appositi Apparati dello Stato, in un'ottica di sinergie operative e di conseguente contenimento dei costi.

Si precisa, altresì, che l'importo in argomento è relativo all'anno in corso; da ciò deriva che esso va rapportato agli adempimenti previsti per il 2018 ed, in particolare, alla mappatura delle infrastrutture critiche informatiche del comparto infrastrutture/trasporti; sarà necessario ed opportuno un monitoraggio delle progressive necessità finanziarie per lo svolgimento delle più ampie attività derivanti dalla piena declinazione di tutte le attività che, nel tempo, deriveranno dalla direttiva NIS.

In particolare, il predetto importo è a decorrere dal 2018, così suddivisibile:

- Euro 100.000 per l'acquisto di beni e servizi, tra i quali strumentazione informatica utile per l'implementazione - nel contesto di una sala operativa di cyber security MIT, con un adeguata resilienza operativa - di un'adeguata infrastruttura client/server, conforme alle vigenti normative sia in materia di tutela dei dati sensibili che per la trasmissione e trattazione di informazioni anche di tipo classificato, specie in ottica di interscambio con le altre strutture dell'architettura nazionale di presidio cyber, nonché di presidio/controllo della sicurezza cyber delle comunicazioni tramite smartphone (ad esempio, sicurezza delle comunicazioni di servizio tra appartenenti agli organismi che operano nei settori di cui all'allegato II);

- Euro 30.000 per attività di ispezione/analisi in loco delle infrastrutture informatiche del comparto infrastrutture/trasporti di cui al sopracitato allegato II (ad esempio, gestori aeroportuali/aeroporti; imprese ferroviarie; impianti portuali, sistemi ITS), nonché attività di collaborazione con gli enti europei (vds. ENISA) ed italiani (vds. Enti Vigilati, CSIRT nazionale ed il punto di contatto unico);

- Euro 20.000 per attività di formazione/aggiornamento del personale MIT addetto al settore;

b) con riferimento al Ministero dello sviluppo economico:

- per la necessità di rispondere adeguatamente alla rilevanza operativa della tematica della cyber security nel suo impatto – a seguito della direttiva (UE) 1148/2016 c.d. "NIS" – sui comparti energia (sottosettori energia elettrica, gas e petrolio) e infrastrutture digitali (sottosettori IXP, DNS, TLD), come meglio definiti nell'Allegato II del decreto in oggetto;

- per la necessità di ottimizzare il rapporto tra risorse finanziare concretamente ad oggi stimate (peraltro con i vincoli derivanti dal contesto economico nazionale) ed efficacia delle attività correlate alla migliore applicazione della Direttiva NIS;

- per l'implementazione/valorizzazione delle forme di collaborazione con gli appositi Apparati dello Stato, in un'ottica di sinergie operative e di conseguente contenimento dei costi.

Si precisa, altresì, che l'importo in argomento è relativo all'anno in corso; da ciò deriva che esso va rapportato agli adempimenti previsti per il 2018 ed, in particolare, alla mappatura delle infrastrutture critiche informatiche dei comparti energia e infrastrutture digitali; sarà necessario ed opportuno un monitoraggio delle progressive necessità finanziarie per lo svolgimento delle più ampie attività derivanti dalla piena declinazione di tutte le attività che, nel tempo, deriveranno dalla direttiva NIS.

In particolare, il predetto importo è a decorrere dal 2018 - così suddivisibile:

- Euro 100.000 per l'acquisto di beni e servizi, tra i quali strumentazione informatica utile per l'implementazione di un'adeguata infrastruttura client/server, conforme alle vigenti normative sia in materia di tutela dei dati sensibili che per la trasmissione e trattazione di informazioni, specie in ottica di interscambio con le altre strutture dell'architettura nazionale di presidio cyber, nonché di presidio/controllo della sicurezza cyber delle comunicazioni tramite smartphone (ad esempio, sicurezza delle comunicazioni di servizio tra appartenenti agli organismi che operano nei settori di cui all'allegato II);

- Euro 20.000 per attività di ispezione/analisi in loco delle infrastrutture informatiche del comparto energia di cui al sopracitato allegato II (ad esempio, imprese elettriche, gestori di oleodotti, di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio, imprese fornitrici di gas, gestori di impianti di raffinazione e trattamento di gas naturale), nonché attività di collaborazione con gli enti europei (vds. ENISA) ed italiani (vds. Enti Vigilati, CSIRT nazionale ed il punto di contatto unico);

- Euro 30.000 per attività di formazione/aggiornamento del personale MISE addetto ai settori di riferimento;

c) con riferimento al Ministero dell'economia e delle finanze Il decreto in oggetto regolamenta il controllo dei fornitori dei seguenti servizi digitali da parte degli organi NIS:

1. Mercato online

2. Motore di ricerca online

3. Servizi di cloud computing

Con particolare riferimento al punto 3, la società SOGEI eroga tali servizi per il MEF-Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi (DAG) attraverso gli istituti contrattuali definiti nella Convenzione per la realizzazione e gestione delle attività informatiche dello Stato sottoscritta, per l'appunto, tra il DAG e la SOGEI S.p.A. In virtù di ciò ed in considerazione di quanto contemplato nel decreto in oggetto, la Società SOGEI S.p.A. si configura quale fornitore di servizi digitali ed il MEF, per il tramite del DAG, Autorità Competente NIS che dovrà essere dotata di poteri e mezzi necessari per valutare la conformità degli operatori di servizi essenziali, quale SOGEI S.p.A., agli obblighi loro imposti dall'articolo 14 e i relativi effetti sulla sicurezza della rete e dei sistemi informativi. In tale scenario e conformemente al decreto in oggetto, il DAG dovrebbe far fronte alle attività necessarie per la definizione delle specificazioni degli elementi che i fornitori di servizi digitali, nella fattispecie SOGEI S.p.A., devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente. Per quanto appena esposto, da una rapida e macroscopica valutazione, si rende pertanto necessario un effort economico che possa contemplare professionalità specifiche nella materia della sicurezza informatica e delle reti in misura pari a 4 FTE, spazi e strumenti idonei per un onere complessivo pari a 300.000 annui a decorrere dal 2018.

d) con riferimento Ministero della salute:
   - Euro 100.000 per l'acquisto di beni c servizi, tra i quali strumentazione informatica utile per l'implementazione
   - Euro 30.000 per attività di ispezione/analisi in loco delle infrastrutture informatiche
   - Euro 20.000 per attività di formazione/aggiornamento del personale addetto al settore;

   L'onere complessivo è pari a 150.000 annui a decorrere dal 2018

e) con riferimento dal Ministero dell'ambiente e della tutela del territorio e del mare
   - Euro 100.000 per l'acquisto di beni e servizi, tra i quali strumentazione informatica utile per l'implementazione
   - Euro 30.000 per attività di ispezione/analisi in loco delle infrastrutture informatiche
   - Euro 20.000 per attività di formazione/aggiornamento del personale addetto al settore;
   - con riferimento dal Ministero dell'ambiente e della tutela del territorio e del mare;
   - L'onere complessivo è pari a 150.000 annui a decorrere dal 2018.

Per quanto concerne le attività svolte dal Dipartimento informazioni per la sicurezza (DIS), quale punto unico di contatto, ciò comporta un maggior impegno finanziario per:

- necessità di rispondere adeguatamente alle nuove funzioni attribuite al DIS, quale Punto di contatto unico, a seguito del recepimento della direttiva (UE) 1148/2016 c.d. "direttiva NIS". In particolare, si tratta delle funzioni 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 di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11 dello schema di decreto legislativo, nonché la gestione delle notifiche di incidenti trasmesse dal CSIRT italiano ai sensi dell'art. 9 del provvedimento;

- implementazione di un'architettura di tracciamento e *handling* delle attivazioni e delle comunicazioni da e per il Punto di contatto unico, anche al fine di garantire la gestione simultanea e in tempo reale di una pluralità di casi. L'importo in argomento (euro 100.000) è relativo all'anno in corso. Da ciò deriva che sarà necessario ed opportuno un monitoraggio delle progressive necessità finanziarie per lo svolgimento delle più ampie attività derivanti dalla piena attuazione della direttiva NIS.

In particolare, il predetto importo è, a decorrere dall'anno 2018, così suddivisibile:

- Euro 70.000 per acquisizione di attività professionali per lo sviluppo specialistico e la gestione della piattaforma informatica necessaria per il funzionamento della predetta architettura;
- Euro 30.000 per l'acquisto di beni e servizi, tra i quali strumentazione informatica hardware e software;

All'onere del presente articolo pari a 1.000.000 euro si provvede ai sensi dell'articolo 22.

**Articolo 8**

Per garantire le necessarie attività di prevenzione e trattamento degli incidenti informatici è costituito il CSIRT (Computer Security Incident Response Team) italiano, struttura tecnico-operativa i cui compiti sono definiti nell'allegato I e che opera in cooperazione con gli omologhi CSIRT dell'UE.

Al CSIRT italiano gli operatori di servizi essenziali e i fornitori di servizi digitali devono notificare incidenti informatici con impatto significativo sulla continuità dei servizi. Nelle more della definizione del funzionamento e organizzazione del CSIRT italiano, le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA.

Il CSIRT italiano viene istituito con apposito DPCM ai sensi del decreto legislativo 300/1999 presso la Presidenza del Consiglio dei Ministri, mediante unificazione del Computer Emergency Response Team (CERT) nazionale, individuato ai sensi dell'articolo 16-bis, del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, operante presso l'Agenzia per l'Italia digitale secondo le relative previsioni statutarie ai sensi dell'articolo 51, del decreto legislativo 7 marzo 2005, n. 82.

Per le spese di personale del CSIRT italiano si provvede nel limite di spesa di 1.300.000 euro annui riferito a un contingente massimo di 30 unità di personale di cui, fino a 15, reperibili con i consueti istituti del fuori ruolo o del comando, ai sensi dell'articolo 17, comma 14, della legge n. 127/1997, e con previsione di apposita facoltà assunzionale fino a 15 unità del predetto contingente individuato.

Per le spese di funzionamento è autorizzata la spesa di 700.000 euro a decorrere dal 2018. 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). Per i predetti interventi è autorizzata una spesa complessiva di 2.000.000 per l'anno 2018.

Pertanto l'onere complessivo del presente articolo è pari a 4.000.000 euro per l'anno 2018 e 2.000.000 annui a decorrere dall'anno 2019, alla relativa copertura si provvede ai sensi dell'articolo 22.

**ARTICOLO 9**

L'istituzione prevista dall'articolo 9, comma 1, secondo periodo, di un Comitato tecnico di raccordo presso la Presidenza del Consiglio dei ministri, composto da rappresentanti delle amministrazioni statali competenti NIS e da rappresentanti delle Regioni e Province autonome non comporta nuovi o maggiori oneri per le amministrazioni interessate, in quanto non sono né compensi, né gettoni, né rimborsi spese.

**ARTICOLO 12**

Con riferimento agli obblighi in materia di sicurezza e notifica degli incidenti imposti agli operatori per i servizi essenziali, per i quali l'allegato II fornisce un elenco, va considerato che è la stessa direttiva che fa obbligo agli operatori di servizi essenziali ed ai fornitori di servizi digitali di garantire la sicurezza delle reti e dei sistemi informativi di cui fanno uso. Si tratta, in particolare, di rete e sistemi informativi privati gestiti dal loro personale IT interno oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di sicurezza e di notifica dovrebbero applicarsi agli operatori di servizi essenziali e ai fornitori di servizi digitali indipendentemente dal fatto che la manutenzione delle loro reti e dei loro sistemi informativi sia eseguita al loro interno o sia esternalizzata.

Nel contesto della direttiva sopra illustrato, oltre che per evitare di imporre un onere finanziario e amministrativo sproporzionato agli operatori di servizi essenziali e ai fornitori di servizi digitali, gli obblighi di sicurezza, anche grazie all'azione di vigilanza delle autorità NIS di settore nei rispettivi ambiti di competenza ed in relazione agli operatori dei servizi essenziali rientranti nel campo di applicazione della propria attività, saranno proporzionati al rischio corso dalla rete e dal sistema informativo di cui si tratta, tenendo conto dello stato dell'arte di tali misure.

Per quanto concerne il Ministero dell'economia e delle finanze, il Ministero della salute e il Ministero dell'ambiente e della tutela del territorio e del mare, autorità competenti NIS per i settori bancario, infrastrutture dei mercati finanziari, assistenza sanitaria, fornitura e distribuzione di acqua

potabile di cui all'articolo 7, gli stessi svolgono i compiti loro assegnati con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, considerando peraltro l'intervento negli stessi ambiti delle Regioni e delle province autonome, nonché della Banca d'Italia e della Consob per i settori riferibili al precitato Ministero dell'economia e delle finanze con conseguente efficientamento dell'attività di vigilanza e sanzionatoria.

Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Gli operatori dei servizi essenziali provvedono agli adempimenti previsti dal presente articolo a valere sulle risorse finanziarie disponibili sui propri bilanci.

**ARTICOLO 21**

Per quanto concerne le sanzioni previste dall'articolo 21, si rappresenta che le stesse sono di nuova istituzione e che i proventi derivanti dalla loro irrogazione verranno destinati all'Erario secondo la disciplina generale prevista in materia.

**ARTICOLO 22**

Agli oneri derivanti dagli articoli 7 e 8 pari a euro 5.000.000 per l'anno 2018 e euro 3.000.000 annui a decorrere dall'anno 2019 si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234.

Dall'attuazione del presente decreto, ad esclusione degli articoli 7 e 8, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni pubbliche provvedono con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196, ha avuto esito

[X] POSITIVO [ ] NEGATIVO

Il Ragioniere Generale della

21 FEB. 2018

## ANALISI TECNICO-NORMATIVA

**NOME PROVVEDIMENTO**

**SCHEMA DI DECRETO LEGISLATIVO RECANTE RECEPIMENTO DELLA DIRETTIVA (UE) 1148/2016 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**

**Referente**

**UFFICIO LEGISLATIVO - MISE**

### PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

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

Lo schema di decreto legislativo recepisce la direttiva (UE) 2016/1148 (cd. Direttiva NIS - *Network and Information Security*) sulla sicurezza delle reti e dei sistemi informativi nell'Unione adottata il 6 luglio 2016, che per la prima volta affronta in modo organico e trasversale gli aspetti in materia di cyber security, rafforzando la resilienza e la cooperazione in Europa.

Lo schema di decreto legislativo consegue tre obiettivi principali:

- promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali;
- migliorare le capacità nazionali di cyber security;
- rafforzare la cooperazione a livello nazionale e in ambito UE.

A tal fine lo schema di decreto legislativo, allo scopo di assicurare la continuità dei servizi essenziali (energia, trasporti, salute, finanza, ecc.) e dei servizi digitali (motori di ricerca, servizi *cloud*, piattaforme di commercio elettronico), prevede l'adozione di misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici e l'obbligo di notifica di incidenti con impatto rilevante sulla fornitura dei servizi. Parallelamente individua le Autorità competenti NIS e i rispettivi compiti svolti in cooperazione con le omologhe Autorità degli Stati Membri dell'UE, nonché il CSIRT (*Computer Security Incident Response Team*) nazionale con compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri CSIRT europei. A tal fine, vengono introdotte o modificate le previsioni sull'ambito di applicazione soggettivo, obblighi di registrazione e istituzione di Organismo per la registrazione, requisiti professionali ed organizzativi dei distributori, esercizio dell'attività transfrontaliera.

*2) Analisi del quadro normativo nazionale.*

Con il recepimento della Direttiva 2009/140/UE, avvenuto con d.lgs. 70/2012, sono state introdotte per la prima volta, nel codice delle comunicazioni elettroniche (d.lgs. 259/2003, articoli 16-*bis* e 16-*ter*), 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.

Parallelamente, la legge n. 124 del 2007, modificata e integrata dalla legge 7 agosto 2012, n. 133, ha disciplinato le funzioni del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) e quelle del Dipartimento delle informazioni per la sicurezza (DIS) al quale, il relativo articolo 4, comma 3, lettera d-*bis*), ha attribuito il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Con D.P.C.M. 24 gennaio 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" è stata delineata l'architettura deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, individuando ruoli e compiti dei soggetti compresi in essa compresi e prevedendo la definizione di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico, successivamente adottato con D.P.C.M. 27 gennaio 2014 unitamente al "Piano nazionale per la protezione cibernetica e la sicurezza informatica" che 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) .

Il D.P.C.M. 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali), nell'abrogare il D.P.C.M. 24 gennaio 2013, ha provveduto ad ~~al fine di~~ aggiornare, anche nelle more del recepimento della direttiva (UE) 2016/1148, la predetta architettura istituzionale alla luce delle previsioni recate dall'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge n. 198 del 2015, (che ha attribuito al CISR funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, così da ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento. Ha proceduto, altresì, ad una razionalizzazione e semplificazione della predetta architettura istituzionale, prevedendo che le funzioni di coordinamento e raccordo delle attività di prevenzione, preparazione e gestione di eventuali situazioni di crisi di natura cibernetica siano attestate presso strutture che assicurino un più diretto ed efficace collegamento con il Comitato interministeriale per la sicurezza della Repubblica.

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

I ruoli e le funzioni già previsti nella predetta normativa nazionale sono confermati nello schema di decreto legislativo finalizzato al recepimento della Direttiva (UE) 2016/1148 - in attuazione delle previsioni recate dalla legge di delegazione europea 25 ottobre 2017 n. 163 - volta a conseguire un livello comune elevato di sicurezza delle reti e dei sistemi informativi in ambito nazionale affrontando in modo organico e trasversale gli aspetti in materia di *cyber security*.
Il provvedimento integra la normativa vigente individuando le Autorità competenti NIS al fine di assicurare il rispetto degli obblighi di sicurezza a carico degli operatori di servizi essenziali e dei fornitori di servizi digitali. Per garantire inoltre le necessarie attività di prevenzione e trattamento degli incidenti informatici è costituito il CSIRT (*Computer Security Incident Response Team*) Italiano, struttura tecnico-operativa che supporta gli operatori e i fornitori di servizi sopra citati nella prevenzione e risposta ad incidenti informatici, le cui funzioni sono svolte dal CERT nazionale

unitamente al CERT-PA. Sia le Autorità NIS che il CSIRT italiano cooperano con i rispettivi omologhi in ambito europeo. Rispetto alla normativa vigente il decreto introduce il Punto di contatto Unico individuato nel Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri, al quale è affidato il ruolo di interfaccia verso le Istituzioni Europee.

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

L'intervento è compatibile con i principi costituzionali vigenti in materia.

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

Il provvedimento risulta compatibile con le competenze e le funzioni delle regioni e degli enti locali, coinvolti nel settore sanitario e ambientale come di seguito indicato.
Relativamente al settore sanitario l'Autorità competente è individuata nel Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e nelle Regioni e Province autonome di Trento e Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza.
Per quanto riguarda il settore della fornitura e distribuzione dell'acqua potabile, l'Autorità competente è individuata nel Ministero dell'ambiente e della tutela del territorio e del mare e nelle Regioni e Province autonome di Trento e Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

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

L'intervento, come sopra evidenziato, laddove coinvolge le funzioni delle regioni e degli enti locali, risulta compatibile con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'art. 118, comma 1, della Costituzione.

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

La materia è attualmente disciplinata a livello di legislazione primaria (decreto legislativo) e secondaria (D.P.C.M. 24 gennaio 2013, sostituito dal D.P.C.M. 17 febbraio 2017, adottati ai sensi dell'art. 1 comma 3-*bis* della legge 3 agosto 2007, n. 124). I citati decreti presidenziali prevedono l'adozione di una Strategia nazionale di sicurezza cibernetica, in relazione alla quale l'art. 6 del decreto legislativo individua specifici contenuti per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto.
Il decreto legislativo prevede, inoltre, all'art. 8, comma 2, l'adozione di un D.P.C.M. ai sensi dell'art. 17, comma 4-*bis* della legge n. 400/88 per l'organizzazione e il funzionamento del CSIRT Italiano. L'articolo 4 infine prevede che le Autorità competenti NIS identifichino per ciascun settore della Direttiva gli operatori di servizi essenziali con sede nel territorio nazionale.

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

Non esistono progetti di legge all'esame del Parlamento su materia analoga.

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

Non risulta che sussistono giudizi di costituzionalità sul medesimo o analogo oggetto né altra giurisprudenza rilevante in merito.

## PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

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

L'intervento si pone quale strumento di recepimento (obbligatorio) della direttiva (UE) 2016/1148.

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

Non risulta che siano in corso procedure di infrazione in materia.

3) ***Analisi della compatibilità dell'intervento con gli obblighi internazionali***

L'intervento non appare in contrasto con altre Convenzioni internazionali.
L'intervento è compatibile con le altre Convenzioni firmate dall'Italia.

4) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia delle Comunità Europee sul medesimo o analogo oggetto.***

Non esistono indicazioni giurisprudenziali della Corte di Giustizia sul medesimo o analogo oggetto.

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

L'intervento non ha alcuna interferenza con gli indirizzi prevalenti della Corte europea dei Diritti dell'Uomo.

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

Gli Stati membri sono vincolati a recepire la medesima direttiva nei limiti entro cui l'Italia è tenuta a intervenire sul quadro normativo nazionale.

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

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

L'articolo 3 traspone le definizioni della Direttiva e introduce cinque nuove definizioni, al fine di chiarire il contesto su cui incide la disciplina introdotta dalla Direttiva:

1) la definizione di Autorità competenti NIS, quali autorità competenti per settore in materia di sicurezza delle reti e dei sistemi informativi nei rispettivi settori e servizi individuati negli allegati II e III della Direttiva, individuandole all'articolo 7, comma 1;

2) la definizione del CSIRT quale gruppo di intervento per la sicurezza informatica in caso di incidente, individuandolo all'articolo 8;

3) la definizione di punto di contatto unico, 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;

4) la definizione di autorità di contrasto, quale organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155;

5) la definizione di "direttive del Presidente del Consiglio dei Ministri" quali le direttive del Presidente del Consiglio dei ministri adottate sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR).

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

Il decreto legislativo fa corretto riferimento alla legislazione nazionale vigente.

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

Non è stato effettuato ricorso alla tecnica della novella integrando e modificando la normativa vigente in materia.

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

È disposta l'abrogazione del comma 4, secondo periodo, dell'articolo 16-*bis*, del decreto legislativo 1° agosto 2003, n. 259, che individua presso il Ministero dello sviluppo economico il *Computer Emergenncy Response Team* (CERT) nazionale, dalla data di entrata in vigore del DPCM di organizzazione funzionamento del CSIRT italiano (articolo 8).

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

L'intervento non ha effetto retroattivo né di riviviscenza di norma precedentemente abrogate o di interpretazione autentica o derogatoria rispetto alla normativa vigente.

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

Sul medesimo oggetto non sono state conferite ulteriori deleghe, anche a carattere integrativo o correttivo.

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

Il decreto legislativo prevede l'adozione di un D.P.C.M. ai sensi dell'art. 17, comma 4-*bis* della legge n. 400/88 per l'organizzazione e il funzionamento del CSIRT Italiano (art. 8, comma 2, del decreto legislativo). Inoltre, l'articolo 4, prevede che le Autorità competenti NIS identifichino per ciascun settore della Direttiva gli operatori di servizi essenziali con sede nel territorio nazionale. Infine, l'articolo 12, comma 7, prevede che le Autorità competenti NIS possano predisporre Linee guida e specifiche misure di sicurezza.

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

Non è stata rilevata la necessità di tale intervento.

# RELAZIONE AIR

**NOME PROVVEDIMENTO**

**SCHEMA DI DECRETO LEGISLATIVO RECANTE RECEPIMENTO DELLA DIRETTIVA 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**

**Referente**

**UFFICIO LEGISLATIVO - MISE**

ELENCO ARTICOLI OGGETTO DELLA RELAZIONE CON RELATIVA RUBRICA

(vedi relazione illustrativa)

***SEZIONE 1 - Contesto e obiettivi dell'intervento di regolamentazione***

*La sezione illustra il contesto in cui si colloca l'iniziotiva di regolazione, l'analisi dei problemi esistenti, le ragioni di opportunità dell'intervento di regolazione, le esigenze e gli obiettivi che l'intervento intende perseguire. In particolare, la sezione contiene i seguenti elementi:*

A) *la rappresentazione del problema da risolvere e delle criticità constatate, anche con riferimento al contesto internazionale ed europeo, nonché delle esigenze sociali ed economiche considerate;*

Gli incidenti informatici di sicurezza, che quotidianamente sono causa di gravi danni economici alle imprese europee e danneggiano l'economia nel suo complesso, minano la fiducia di cittadini e imprese nella società digitale. Il furto di segreti commerciali, informazioni aziendali e dati personali, l'interruzione dei servizi - anche di quelli essenziali - provocano ogni anno danni economici per centinaia di miliardi di euro.

Inoltre l'interconnessione delle reti e dei sistemi informativi facilita i movimenti transfrontalieri di beni, servizi e persone. Gravi perturbazioni a carico di questi sistemi in uno Stato membro possono avere ripercussioni negli altri Stati membri e in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi sono quindi essenziali per il mercato unico digitale e per l'armonioso funzionamento del mercato interno.

I rischi stanno aumentando in maniera esponenziale. Secondo alcuni studi l'impatto economico della cibercriminalità sarebbe aumentato di cinque volte tra il 2013 e il 2017 e potrebbe ancora quadruplicarsi entro il 2019. Gravi attacchi recenti mostrano un considerevole aumento del *cybercrime:* nel maggio 2017 l'attacco *ronsomware WonnoCry* ha colpito più di 400.000 computer in più di 150 Paesi. Un mese dopo l'attacco *ronsomware Petyo* ha colpito l'Ucraina e molte imprese nel mondo (Bruxelles, 13.9.2017 -JOIN(2017) 450 final COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO Resilienza, deterrenza e difesa: verso una *cibersicurezza* forte per l'UE).

Già dal 2004 l'Unione europea (UE) si è dotata di un'Agenzia europea per la sicurezza delle reti e dell'informazione (*European Union for Network and Informotion Security Agency* - ENISA) con l'obiettivo di favorire l'incremento del livello di sicurezza delle reti e dell'informazione nell'UE nonché

lo sviluppo di una cultura in materia a vantaggio di cittadini, consumatori, imprese e del settore pubblico nell'Unione Europea. In particolare l'ENISA agisce come centro di competenza per lo scambio di informazioni e *best practice* tra settore pubblico e privato, analizzando i rischi attuali ed emergenti.

Il noto attacco che, nella primavera del 2007, ha colpito l'Estonia ha fatto crescere in Europa la consapevolezza dei potenziali rischi e della conseguente necessità di rafforzare le capacità nazionali e il coordinamento a livello europeo.

La Commissione Europea ha, quindi, intensificato le attività sulla sicurezza dello spazio "cyber" prima con la comunicazione del 2009 – "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni" e con la Direttiva 2009/140/CE, che ha modificato il quadro regolamentare in materia di comunicazioni elettroniche; poi con l'Agenda Digitale – "Trust and security pillar" nel 2010 e con la comunicazione del 2011 "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale", e infine con la comunicazione del 2013 la "Strategia dell'Unione europea per la cyber security: un cyber spazio aperto e sicuro" e, al contempo, la proposta di Direttiva NIS.

La Direttiva NIS nasce proprio dalla consapevolezza dell'inadeguatezza dell'approccio puramente facoltativo ad assicurare una protezione sufficiente contro i rischi e gli incidenti a carico della sicurezza delle reti e dell'informazione nell'UE, soprattutto in considerazione della rapida evoluzione delle minacce alla sicurezza sempre più sofisticate e sempre meno prevedibili.

Lo scopo della direttiva proposta è assicurare un elevato livello comune di sicurezza delle reti e dell'informazione nell'Unione. A tal fine è necessario rafforzare la sicurezza delle reti e dei sistemi informativi privati su cui si fonda il funzionamento delle nostre società e delle nostre economie.

A livello europeo la Direttiva NIS è volta a superare i diversi livelli di capacità tecnica degli Stati Membri UE per tendere ad un livello comune di sicurezza considerato che la sicurezza complessiva dell'intero ecosistema digitale dipende dall'anello più debole della catena.

Anche il contesto internazionale si presenta molto variegato: a fronte di Paesi nei quali le problematiche di cyber security sono state affrontate già da tempo in modo strutturato, esistono invece situazioni nelle quali invece le politiche in materia di cyber security non si sono ancora sviluppate in modo adeguato. Solo nel 2017 i numerosi attacchi informatici hanno causato danni economici per un importo pari a 146,3 miliardi di euro a 978 milioni di utenti di 20 Paesi (Fonte "2017 Norton Cyber Security Insight Report").

Anche in Italia gli incidenti di cibersicurezza causano ingenti danni alle imprese e ai cittadini. Nel 2017 oltre 16 milioni di utenti della rete sono "caduti in trappole informatiche" con conseguenti perdite economiche per circa 3,5 miliardi di euro (Fonte "2017 Norton Cyber Security Insight Report").

Negli ultimi anni la consapevolezza del rischio informatico è notevolmente cresciuta in Italia e molte iniziative sono state avviate per contrastare la minaccia informatica. Con il recepimento della Direttiva 2009/140/UE, avvenuto con d.lgs. 70/2012, sono state introdotte per la prima volta, nel codice delle comunicazioni elettroniche (d.lgs. 259/2003, articoli 16-bis e 16-ter), 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.

Con la legge n. 124 del 2007, modificata e integrata dalla legge 7 agosto 2012, n. 133, è stato istituito il Sistema di informazione per la sicurezza della Repubblica e sono stati disciplinati i ruoli e le attribuzioni, nell'ambito del più complessivo assetto, del Presidente del Consiglio dei ministri, del Comitato interministeriale per la sicurezza della Repubblica (CISR), del Dipartimento delle informazioni per la sicurezza (DIS) e dei Servizi di informazione (AISE e AISI). In particolare, l'art. 1, comma 3-bis, ha previsto che il Presidente del Consiglio dei ministri, sentito il CISR, impartisca al DIS e ai Servizi direttive in materia di protezione cibernetica e sicurezza informatica nazionali. L'articolo 4, comma 3, lettera d-*bis*), ha poi attribuito in capo al DIS, anche sulla base delle direttiva di cui all'art. 1, comma 3-bis, il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Con l'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito in legge n. 198/2015, è stato previsto che il Presidente del Consiglio dei ministri, in situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, possa avvalersi del CISR appositamente convocato con funzioni di consulenza, proposta e deliberazione.

Con D.P.C.M. 24 gennaio 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" è stata delineata l'architettura deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, individuando ruoli e compiti dei soggetti ~~compresi~~ in essa compresi e prevedendo ~~la definizione~~ l'adozione di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico, successivamente adottato con D.P.C.M. 27 gennaio 2014 unitamente al "Piano nazionale per la protezione cibernetica e la sicurezza informatica" che 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) .

Il D.P.C.M. 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali), nell'abrogare il D.P.C.M. 24 gennaio 2013, ha provveduto ad ~~al fine di~~ aggiornare, anche nelle more del recepimento della direttiva (UE) 2016/1148, la predetta architettura istituzionale alla luce delle previsioni recate dal citato articolo 7-*bis*, così da ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento. Ha proceduto, altresì, ad una razionalizzazione e semplificazione della predetta architettura istituzionale, prevedendo che le funzioni di coordinamento e raccordo delle attività di prevenzione, preparazione e gestione di eventuali situazioni di crisi di natura cibernetica siano attestate presso strutture che assicurino un più diretto ed efficace collegamento con il Comitato interministeriale per la sicurezza della Repubblica. A tali fini, il D.P.C.M. 17 febbraio 2017 prevede la collocazione istituzionale presso il DIS del Nucleo per la sicurezza cibernetica (NSC).

Lo schema di decreto legislativo si inquadra pertanto nel contesto normativo sopra descritto e si pone l'obiettivo di ridurre il rischio di incidenti informatici che possano determinare l'indisponibilità di servizi essenziali causando ingenti danni economici e possibili importanti ripercussioni alla dimensione economico-sociale della vita dei cittadini italiani.

B) *l'indicazione degli obiettivi (di breve, media o lungo periodo) perseguiti con l'intervento normativo*

Lo schema di decreto legislativo recepisce la direttiva (UE) 2016/1148 (cd. Direttiva NIS) sulla sicurezza delle reti e dei sistemi informativi nell'Unione adottata il 6 luglio 2016, che per la prima volta affronta in modo organico e trasversale gli aspetti in materia di cyber security, rafforzando la resilienza e la cooperazione in Europa.

Lo schema di decreto legislativo consegue tre obiettivi generali principali:

- promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali;
- migliorare le capacità nazionali di cyber security;
- rafforzare la cooperazione a livello nazionale e in ambito UE.

A tal fine con lo schema di decreto legislativo si intende conseguire gli obiettivi specifici descritti di seguito, in relazione al contesto e alle specificità nazionali:

- sebbene la consapevolezza dei rischi informatici sia in crescita, notevoli sono ancora le azioni che devono essere messe in campo per rafforzare la sicurezza informatica; una delle criticità dell'assetto regolamentare attuale è la mancanza di obblighi specifici in capo al settore privato che si autoregola in base alla propria percezione del rischio. Lo schema di decreto punta proprio a definire tali obblighi allo scopo di assicurare la continuità dei servizi essenziali (energia, trasporti, salute, finanza, ecc.) e dei servizi digitali (motori di ricerca, servizi cloud, piattaforme di commercio elettronico). Gli operatori di tali settori dovranno adottare misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici e l'obbligo di notifica di incidenti con impatto rilevante sulla fornitura dei servizi.

- in Italia nel gennaio 2014 è stata adottata la strategia nazionale in materia di sicurezza informatica che stabilisce le politiche per la crescita del sistema di contrasto alle minacce cibernetiche. Uno degli obiettivi del decreto legislativo riguarda **l'adozione della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.** Tali nuovi principi andranno ad integrare la strategia attualmente adottata;

- per verificare la coerenza delle misure adottate dal settore privato ai risultati dell'analisi dei rischi e per vigilare sulla corretta applicazione delle stesse, il decreto legislativo individua più Autorità competenti NIS che operano in cooperazione con le omologhe Autorità degli Stati Membri dell'UE;

- in Italia attualmente operano il CERT Nazionale, presso il Ministero dello sviluppo economico, rivolto al settore privato, ivi inclusi i cittadini, agendo anche come punto di contatto a livello internazionale, e il CERT-PA che si rivolge alle Pubbliche Amministrazioni. In sede CISR è stata decisa l'unificazione dei due CERT, al fine di assicurare un'operatività maggiormente coesa verso l'intera "constituency" pubblica e privata. Tra i principali compiti dei CERT si evidenziano

quelli di prevenzione e coordinamento nella risposta ad attacchi informatici. Il decreto si pone l'obiettivo della costituzione del CSIRT (*Computer Security Incident Response Team*) ~~nazionale~~ italiano, presso la Presidenza del Consiglio dei ministri, con compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri CSIRT europei.

- la funzione di coordinamento nelle materie della sicurezza informatica ricoperta dal DIS ai sensi della normativa vigente risulta confermata ed estesa dal decreto legislativo in oggetto che individua proprio nel DIS il Punto di contatto unico con funzioni 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 di cui all'art. 10 e la rete di CSIRT di cui all'art. 11.

C) *la descrizione degli indicatori che consentiranno di verificore il grado di raggiungimento degli obiettivi indicati e di monitorare l'attuazione dell'intervento nell'ambito della VIR;*

Sulla base di quanto rappresentato alla lettera B) si riportano di seguito i possibili indicatori per un efficace monitoraggio dell'attuazione dei principali obiettivi dello schema di provvedimento:

- il numero e gli esiti delle verifiche condotte dalle Autorità competenti NIS di cui agli articoli da 13 e 15 del provvedimento
- il numero delle notifiche pervenute alle Autorità competenti
- il numero di segnalazioni gestite dal CSIRT Italiano relativamente ai settori e ai servizi contemplati dal decreto legislativo.
- le iniziative previste nell'ambito del Gruppo di cooperazione e della rete di CSIRT di cui all'articolo 10 e 11 del provvedimento.

D) *l'indicazione delle categorie dei soggetti, pubblici e privati, destinatari dei principali effetti dell'intervento regolatorio.*

I soggetti pubblici interessati dal provvedimento sono:

- il Punto di contatto unico di cui all'articolo 7, commi 4 e 5, verso le Istituzioni dell'UE individuato nel Dipartimento delle Informazioni per la Sicurezza – DIS;
- il CSIRT Italiano, gruppo di intervento per la sicurezza informatica in caso di incidente, di cui all'articolo 8, istituito presso la Presidenza del Consiglio dei ministri, mediante unificazione del Computer Emergency Response Team (CERT) nazionale, individuato ai sensi dell'articolo 16-bis, del decreto legislativo 1° agosto 2003, n.259, e del CERT-PA, operante presso l'Agenzia per l'Italia digitale;
- le Autorità competenti NIS, in particolare:

a) il Ministero dello sviluppo economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;

b) il Ministero delle infrastrutture e trasporti per i il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;

c) il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari;

d) il Ministero della salute per l'attività di assistenza sanitaria, così come definita dall'articolo 3, comma 1, lett. a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

I soggetti privati interessati dal presente decreto sono:

- gli operatori di servizi essenziali individuati ~~ente~~ entro il 9 novembre 2018, ai sensi dell'articolo 4, dalle Autorità competenti NIS per ciascun settore e sottosettore di cui all'allegato II. In particolare i settori interessati sono:
    - energia, con riferimento ai sottosettori dell'energia elettrica, petrolio e gas;
    - trasporti, con riferimento ai sottosettori del trasporto aereo, ferroviario, per vie d'acqua, su strada;
    - settore bancario;
    - infrastrutture dei mercati finanziari;
    - settore sanitario, con riferimento al sottosettore istituti sanitari, compresi ospedali e cliniche private;
    - fornitura e distribuzione di acqua potabile;
    - infrastrutture digitali.

- i fornitori dei seguenti servizi digitali di cui all'allegato III :
    - mercato on line;

- motori di ricerca on line;
- servizi di cloud computing

**SEZIONE 2 - Procedure di consultazione precedenti l'intervento**

*La sezione descrive le consultazioni effettuate con destinatari pubblici e privati dell'iniziativa di regolazione o delle associazioni rappresentative degli stessi, indicando le modalità seguite, i soggetti consultati e le risultanze emerse ai fini dell'analisi d'impatto. La sezione indica, eventualmente, le ragioni del limitato o mancato svolgimento delle consultazioni. Nelle consultazioni di cui alla presente sezione non rientrano i pareri di organi istituzionali.*

Trattandosi del recepimento di una direttiva dell'UE caratterizzata, tra l'altro, dall'ampia presenza di disposizioni che per la prima volta introducono misure volte ad incrementare il livello comune di sicurezza nell'Unione Europea, sono state condotte numerose iniziative che hanno visto il coinvolgimento del settore pubblico e privato. Le procedure di valutazione e consultazione, nonché di impatto della regolamentazione sono state oggetto di lunga discussione e partecipazione nella fase ascendente della produzione normativa europea, attraverso il coinvolgimento diretto dei principali *stakeholder* ai tavoli di concertazione e discussione presso le sedi comunitarie, nonché attraverso consultazioni pubbliche e *survey* rivolte al settore privato interessato dal provvedimento.

Nel 2012 si è svolta una consultazione pubblica online sul tema "Migliorare la sicurezza delle reti dell'informazione nell'UE". Le parti interessate si sono espresse generalmente a favore della necessità di migliorare la sicurezza delle reti e dell'informazione in tutta l'Unione. In particolare, l'82,8% ritiene che gli utenti delle informazioni e dei sistemi non siano consapevoli dell'esistenza di minacce e incidenti di sicurezza; il 66,3% sarebbe in linea di massima a favore dell'introduzione di obblighi regolamentari in materia di gestione dei rischi per la sicurezza delle reti e dell'informazione e, secondo l'84,8%, gli obblighi dovrebbero essere fissati al livello dell'UE. Un numero elevato di partecipanti alla consultazione ritiene che sarebbe importante adottare obblighi in particolare nei seguenti settori: banche e finanza (91,1%), energia (89,4%), trasporti (81,7%), sanità (89,4%), servizi internet (89,1%) e amministrazioni pubbliche (87,5%). I partecipanti si sono espressi a favore dell'introduzione dell'obbligo di segnalazione delle violazioni di sicurezza delle reti e dell'informazione alle autorità nazionali competenti.

Gli Stati membri sono stati consultati in una serie di riunioni del Consiglio, nonché in occasione di riunioni bilaterali convocate su richiesta di singoli Stati membri.

Si sono tenute anche discussioni con il settore privato nell'ambito del partenariato europeo pubblico-privato per la resilienza e nel corso di riunioni bilaterali.

**SEZIONE 3 - Valutazione dell'opzione di non intervento di regolamentazione (opzione zero)**

*La sezione descrive la valutazione dell'opzione del non intervento («opzione zero»), indicando i prevedibili effetti di tale scelta, con particolare riferimento ai destinatari e agli obiettivi di cui alla sezione 1, compresa la possibilità di ricorrere all'attivazione dei meccanismi di regolazione spontanea della società civile, ossia alle azioni volontarie e di autoregolazione.*

Trattandosi del recepimento di una direttiva europea, i cui contenuti sono stati già ampiamente concertati in sede dell'UE, non è percorribile la cd. opzione zero, in quanto l'adozione dell'atto di recepimento è obbligatoria per tutti gli Stati membri, nel termine del ~~5~~ 9 maggio 2018.

***SEZIONE 4 - Opzioni alternative all'intervento regolatorio***

*La sezione descrive le opzioni alternative di intervento regolatorio, inclusa quella proposta, esaminate nel corso dell'istruttoria, con particolare attenzione alle ipotesi formulate dai soggetti interessati nelle fasi di consultazione. In caso di recepimento di direttive europee, tra le opzioni è inclusa quella corrispondente al livello minimo di regolazione previsto dalle direttive.*

*La sezione illustra, inoltre, i risultati della comparazione tra le opzioni esaminate, eventualmente basata anche sulla stima degli effetti attesi. La comparazione tiene conto, in ogni caso, della prevedibile efficacia e della concreta attuabilità delle stesse, del rispetto dei principi di sussidiarietà e proporzionalità, nonché della necessità di assicurare il corretto funzionamento concorrenziale del mercato e la tutela delle libertà individuali.*

Trattandosi del recepimento di una direttiva europea i cui contenuti, come detto, concertati in sede comunitaria, sono sostanzialmente vincolanti per gli Stati membri, non sono state considerate opzioni alternative di intervento, non contemplate dalla disciplina in questione.

Ciò premesso, limitatamente ai casi in cui la direttiva stessa garantiva agli Stati membri l'opzione di una scelta tra più alternative, il decreto legislativo ha recepito tutte le indicazioni espresse dal CISR.

Inoltre, per quanto riguarda il tempo massimo entro cui gli operatori di servizi essenziali sono tenuti alla notifica di un incidente informatico significativo alle rispettive Autorità competenti NIS, si è ritenuto opportuno trasporre la dizione della Direttiva "senza indebito ritardo" nella locuzione "senza ingiustificato ritardo". Tale scelta appare coerente considerato che è fondamentale conoscere prima possibile il verificarsi di un attacco per poterne ridurre l'impatto e limitare l'estensione ad altri settori oltre a quello interessato. Tale intervallo di tempo è stato inoltre valutato sufficiente per consentire all'operatore interessato dall'incidente di valutarne la gravità.

Infine, per quanto riguarda i criteri su cui è basata l'articolazione delle sanzioni amministrative previste dall'articolo 20 del decreto, si precisa che la proposta formulata è basata sui possibili impatti derivanti dal mancato adempimento degli obblighi posti dal decreto. In particolare, si è tenuto conto dell'importanza della notifica di un incidente per poter ridurre l'impatto e ripristinare i servizi nel minor tempo possibile, nonché del fondamentale ruolo giocato dagli operatori di servizi essenziali per il mantenimento delle attività economiche e sociali dei cittadini.

***SEZIONE 5 - Giustificazione dell'opzione regolatorio proposta e valutazione degli oneri amministrativi e dell'impatto sulle PMI***

*La sezione descrive l'intervento regolatorio prescelto, riportando:*

*A) gli svantaggi e i vantaggi dell'opzione prescelto, per i destinatari diretti e indiretti, a breve e a medio-lungo termine, adeguatamente misurati e quantificati, anche con riferimento alla possibile incidenza*

*sulla organizzaziane e sulle attività delle pubbliche amministrazioni, evidenzianda i relativi vantaggi collettivi netti e le relative fonti di informazione;*

I vantaggi e gli svantaggi connessi al recepimento della direttiva sono stati analizzati nell'impatto della regolamentazione già a livello ascendente nell'ambito dei lavori dell'Unione Europea.

Ciò premesso, sebbene l'opzione normativa sia motivata dall'obbligo di recepimento della direttiva, la normativa introdotta consentirà di 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. Gli investimenti necessari sia da parte del settore pubblico che privato consentiranno di evitare notevoli perdite economiche derivanti dalla gestione e risoluzione di attacchi informatici, migliorando la prevenzione con l'adozione di misure di sicurezza sia tecniche che organizzative da parte delle imprese e rafforzando le capacità tecniche nazionali di supporto in ambito pubblico. L'incremento della sicurezza informatica comporterà una migliore disponibilità dei servizi essenziali in settori quali la salute, l'energia e i trasporti, nonché dei servizi digitali, quali il mercato on line, i servizi cloud, motori di ricerca. I vantaggi collettivi netti, quindi, incideranno sul mantenimento delle attività sociali ed economiche fondamentali e sulle sempre crescenti esigenze di digitalizzazione a beneficio dei cittadini.

B) *l'individuazione e la stima degli effetti dell'opzione prescelta sulle micro, piccole e medie imprese;*

Per i fornitori di servizi digitali si sottolinea che il provvedimento, come previsto anche dalla Direttiva, non si applica alle microimprese e alle piccole imprese quali definite nella raccomandazione della Commissione Europea 2003/361/CE.

Tale esclusione non è prevista per gli operatori di servizi essenziali. Al riguardo si evidenzia, come si evince da diversi studi di analisi economica condotti al riguardo, che gli investimenti derivanti alle PMI dall'applicazione del decreto legislativo sarebbero di gran lunga inferiori rispetto alle spese di ripristino post-attacco informatico.

C) *l'indicazione e lo stima degli oneri informativi e dei relativi costi amministrativi, introdotti o eliminati a carico di cittadini e imprese. Per onere informativo si intende qualunque adempimento comportonte raccolta, elaborazione, trasmissione, conservazione e produzione di informazioni e documenti allo pubblico amministrazione;*

Non sussistono oneri informativi e relativi costi amministrativi introdotti a carico di cittadini.

Quanto agli operatori del settore va segnalata l'introduzione degli oneri informativi connessi all'attività notifica degli incidenti informatici di cui agli articoli 12 e 14 e all'attività di controllo da parte delle Autorità competenti NIS ai sensi degli articoli 13 e 15.

D) *le condizioni e i fattori incidenti sui prevedibili effetti dell'intervento regolatorio, di cui comunque occorre tener conto per l'attuazione (misure di politica economico ed ospetti economici e finanziari suscettibili di incidere in modo significativo sull'ottuazione dell'opzione regolatoria prescelta; disponibilità di adeguate risorse amministrative e gestionoli; tecnologie utilizzabili, situazioni ambientali e ospetti socio-culturali da considerore per quanto concerne l'attuazione dello norma prescelta, ecc.).*

*Si ravvisano le seguenti condizioni o fattori incidenti sugli effetti dell'intervento regolatorio di cui tener conto ai fini dell'attuazione dello stesso:*

Non sussistono condizioni o fattori esterni, attualmente prevedibili, che possano incidere sulla corretta attuazione della disciplina introdotta con il decreto legislativo di recepimento della direttiva (UE)2016/1148. Le nuove funzioni e i nuovi compiti introdotti, pur producendo un impatto sull'organizzazione dei soggetti pubblici coinvolti appare almeno parzialmente bilanciata dalla possibilità di gestire la propria dotazione organica e le relative attività , attraverso i finanziamenti di cui alla lettera A della sezione 5 della presente relazione.

***SEZIONE 6 – Incidenza sul corretto funzionamento concorrenziale del mercato e sulla competitività del Paese***

L'intervento normativo, in linea con la direttiva che impone a tutti gli Stati membri di adeguarsi alle nuove disposizioni in materia di sicurezza informatica, non incide negativamente sul corretto funzionamento concorrenziale del mercato e sulla competitività del Paese.

***SEZIONE 7 - Modalità attuative dell'intervento di regolamentazione***

*La sezione descrive:*

*A) i soggetti responsabili dell'attuazione dell'intervento regolatorio:*

Ai sensi dell'articolo 7, comma 2, del decreto legislativo le Autorità competenti NIS sono responsabili dell'attuazione del decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigilano sull'applicazione del decreto a livello nazionale esercitando altresì le relative potestà ispettive e sanzionatorie.

*B) le azioni per la pubblicità e per l'informazione dell'intervento (con esclusione delle forme di pubblicità legale degli atti già previste dall'ordinamento):*

Il decreto non prevede particolari forme di informazione e pubblicità, se non quelle già eventualmente previste per il recepimento, da parte dei singoli Stati membri, della normativa dell'UE.

In ogni caso, alle stesse verrà data pubblicità tramite la pubblicazione del provvedimento sui istituzionali delle Autorità pubbliche interessate dal provvedimento.

*C) strumenti e modalità per il controllo e il monitoraggio dell'intervento regolatorio:*

La Direttiva prevede che la Commissione europea monitori l'attuazione delle disposizioni. Il provvedimento affida al Punto di contatto unico, **individuato nel Dipartimento delle informazioni per la sicurezza (DIS) ai sensi dell'art. 7, comma 3,** il compito di trasmettere alla Commissione Europea le informazioni necessarie per la valutazione dell'attuazione del decreto.

*D) i meccanismi eventualmente previsti per la revisione dell'intervento regolatorio:*

L'intervento non prevede meccanismi di revisione.

E) *gli aspetti prioritori da monitorare in fase di attuazione dell'intervento regolotorio e considerare ai fini della VIR:*

A cura **del Ministero dello Sviluppo Economico** verrà elaborata la prescritta relazione della verifica dell'impatto regolatorio, attraverso l'analisi, in termini di incremento/decremento degli indicatori descritti alla sezione 1, lettera C, rispetto all'attività espletata al momento delle modifiche proposte.

***SEZIONE 8 - Rispetto dei livelli mlnimi di regolazione europea***

L'intervento proposto:

- non introduce né mantiene requisiti, standard, obblighi e oneri non necessari per il recepimento della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016;
- non estende l'ambito soggettivo o oggettivo di applicazione delle regole rispetto a quanto previsto dalla citata direttiva;
- in attuazione della direttiva stabilisce le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della direttiva, introducendo sanzioni effettive, proporzionate e dissuasive;
- non introduce né mantiene sanzioni, procedure o meccanismi più gravosi o complessi di quelli necessari per l'attuazione della predetta direttiva ma, viceversa, differenzia le sanzioni per i comportamenti collegati alle attività imposte dal diverso modello di governance previsto dalla direttiva per i fornitori di servizi digitali, tenendo tuttavia presente che per talune violazioni, ad es. quelle concernenti l'obbligo di notifica, si prevede la stessa sanzione, senza differenziarla in base alla natura del operatore in quanto ritenuta di pari gravità.

Pertanto i livelli minimi di regolazione europea esplicitati nella direttiva oggetto di recepimento sono stati rispettati.