Relazione
ai sensi dell'art. 6, comma 4, della legge n. 234/2012

Oggetto dell'atto:
Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi (CSoA).

- **Codice della proposta:** COM(2023) 209 del 18/04/2023
- **Codice interistituzionale:** 2023/0109(COD)
- **Amministrazione con competenza prevalente:** Agenzia per la cybersicurezza nazionale

***

Premessa: finalità e contesto

La proposta di regolamento nasce in un contesto socioeconomico caratterizzato dalla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione (c.d. TIC) cui, tuttavia, ha fatto seguito anche un aumento degli incidenti di cyber, con la conseguenza per gli Stati membri di dover affrontare crescenti rischi in tale ambito e un panorama di minacce globalmente complesso.
Quanto al contesto geopolitico, la diffusione delle TIC ha, altresì, avuto come conseguenza che le operazioni informatiche siano sempre più integrate nelle strategie ibride e di guerra, come dimostrato anche nel conflitto militare tra la Russia e l'Ucraina, preceduto e accompagnato da una strategia di operazioni informatiche ostili, anche da parte di soggetti non statuali coinvolti nelle tensioni geopolitiche.
Negli ultimi anni, dunque, il numero di attacchi informatici è aumentato sensibilmente, compreso quello degli attacchi alle catene di approvvigionamento con finalità di cyberspionaggio, di *ransomware* o di perturbazione.
Tali incidenti hanno la potenzialità di ostacolare, e in alcuni casi impedire, l'erogazione di servizi pubblici e lo svolgimento di attività economiche, anche in settori critici o altamente critici, di generare consistenti perdite finanziarie, di minare la fiducia degli utenti, nonché di causare gravi danni all'economia dell'Unione, e possono persino avere conseguenze sulla salute degli esseri umani o essere potenzialmente letali.
Inoltre, gli incidenti di cyber sono imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si manifestano simultaneamente o si diffondono istantaneamente in numerosi paesi.
In tale contesto, dunque, la minaccia di possibili incidenti su vasta scala in grado di provocare perturbazioni e danni significativi a infrastrutture critiche richiede una maggiore preparazione a tutti i livelli dell'ecosistema di cybersicurezza dell'UE e la creazione di un meccanismo di solidarietà rafforzata a livello di Unione al fine di migliorare il rilevamento delle minacce e degli incidenti di cyber, nonché la preparazione e la risposta agli stessi.
In aggiunta al richiamato contesto, nonostante la potenziale dimensione transfrontaliera delle minacce e degli incidenti di cyber conseguente all'interconnessione delle infrastrutture digitali, evidenzia una limitata condivisione di informazioni pertinenti tra gli Stati membri che richiede, pertanto, il miglioramento delle capacità collettive al fine di ridurre drasticamente il tempo necessario per rilevare le minacce informatiche, prima che possano provocare danni e comportare

costi su vasta scala, anche attraverso l'istituzione di una rete di centri operativi di sicurezza (*Security Operations Centre*, SOC) transfrontalieri per migliorare le capacità di rilevamento e di risposta.

- quadro normativo:

Già nella "Strategia dell'UE in materia di cibersicurezza per il decennio digitale" (JOIN(2020) 18 final), adottata nel dicembre 2020, si evidenziava l'importanza di rafforzare lo scambio di informazioni, nonché il rilevamento e la conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione, e di intensificare la solidarietà migliorando la preparazione e le capacità degli Stati membri e dell'Unione di rispondere agli incidenti di cyber significativi e su vasta scala, anche attraverso la costituzione un'infrastruttura paneuropea di SOC (c.d. "cyberscudo europeo").

Con particolare riferimento ai SOC, nell'ambito del "Programma di lavoro 2021-2022 sulla cybersicurezza", che fa parte del "Programma Europa digitale", sono stati pubblicati un invito a manifestare interesse per l'appalto congiunto di strumenti e infrastrutture per l'istituzione di SOC transfrontalieri e un invito a presentare proposte per sovvenzioni al fine di consentire lo sviluppo delle capacità dei SOC al servizio di organizzazioni pubbliche e private.

Nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dallo stesso nella sessione del 23 maggio 2022 (9364/22), è stata, inoltre, rilevata l'esigenza che la Commissione europea formuli una proposta su un nuovo Fondo di risposta alle emergenze di cybersicurezza.

Il 10 novembre 2022 è stata, poi adottata la "Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE" (JOIN(2022) 49 final) nella quale è stata annunciata l'iniziativa dell'UE per la cyber solidarietà finalizzata a realizzare il citato cyberscudo europeo, a creare un meccanismo per le emergenze di cybersicurezza, ad istituire un meccanismo europeo di riesame degli incidenti di cyber finalizzato al riesame e alla valutazione di specifici incidenti significativi o su vasta scala.

Fanno, inoltre, parte delle misure normative poste in essere per rafforzare la cybersicurezza, anche la proposta di regolamento di modifica del regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti (COM(2023) 208 final) che consentirà la futura adozione di sistemi di certificazione europei per i "servizi di sicurezza gestiti" che coprono settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza, nonché la comunicazione della Commissione con la quale è stata presentata un'Accademia per le competenze in materia di cybersicurezza nell'ambito dell'Anno europeo delle competenze 2023, per garantire un approccio più coordinato volto a colmare il divario di talenti nel settore, condizione preliminare per rafforzare la resilienza dell'Europa.

Il richiamato quadro normativo è completato dagli atti dell'Unione già adottati per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cybersicurezza, costituito, in particolare, dalla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio (direttiva "NIS2"), dalla raccomandazione (UE) 2017/1584 della Commissione, dalla direttiva 2013/40/UE del Parlamento europeo e del Consiglio e dal regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, nonché dal regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

- finalità generali;

Nel contesto su richiamato, dunque, il 18 aprile u.s., la Commissione ha presentato la presente proposta legislativa, c.d. "*Cyber Solidarity Act*" (CSoA), che va a concretizzare la richiesta rivolta dai Ministri dell'UE competenti per la materia digitale per il rafforzamento della solidarietà e della mutua assistenza a livello europeo in materia cyber, nonché alcuni dei contenuti della Comunicazione Congiunta sulla EU *Cyber Defence Policy* (CDP) dello scorso novembre, su richiamati, per quanto concerne, in particolare la:

- creazione di una infrastruttura di "*Security Operation Center*" (SOC) nazionali, integrati a livello regionale. La proposta legislativa avanzata dalla Commissione è volta a definire i criteri di idoneità,

i requisiti di interoperabilità e i meccanismi di finanziamento dell'iniziativa in questione. Tra le previsioni di funzionamento dei SOC è previsto l'obbligo di condivisione delle informazioni a livello UE in casi eccezionali legati ad incidenti cibernetici su larga scala;
- definizione di "Procedure di emergenza cyber", come seguito del progetto pilota condotto da ENISA (l'Agenzia dell'Unione Europea per la Cybersicurezza), che includerebbe anche il meccanismo di riserva di capacità nella gestione degli incidenti cyber su larga scala, garantito da operatori fiduciari del settore privato, che potranno essere dispiegati su richiesta dello Stato membro interessato ovvero di Istituzioni, organismi ed agenzie UE. Anche in questo caso, la proposta legislativa inquadra i criteri di idoneità e le modalità di acquisizione dei servizi, nonché le modalità di finanziamento dell'iniziativa. Tali operatori dovranno essere certificati sulla base dello schema che sarà adottato per la certificazione dei "*managed security service*", ai sensi del regolamento (UE) 2019/881 (cd. "*Cyber Security Act*");
- realizzazione di un "meccanismo di esame degli incidenti cyber" per valutare ed esaminare specifici incidenti di cyber. Su richiesta della Commissione o delle autorità nazionali nell'ambito della rete CyCLONe (Cyber Crises Liaison Organisation Network) o della rete dei CSIRT (Computer Security Incident Response Team), l'ENISA sarà responsabile per l'esame di specifici incidenti cyber significativi o su larga scala e sarà chiamata a presentare una relazione che includa le lezioni apprese e raccomandazioni per migliorare la risposta dell'Unione.

- elementi qualificanti ed innovativi:

Elementi qualificanti ed innovativi della proposta di regolamento sono l'istituzione del "cyberscudo europeo", del "meccanismo europeo di cybersicurezza" e del "meccanismo europeo di riesame degli incidenti di cyber".
Più in particolare, quanto al "cyberscudo europeo", questo sarà costituito dai centri operativi di sicurezza nazionali ("SOC nazionali") e transfrontalieri ("SOC transfrontalieri"). Ogni Stato membro partecipante designa un SOC nazionale, che funge da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello nazionale per raccogliere e analizzare informazioni sulle minacce e sugli incidenti di cyber e per contribuire a un SOC transfrontaliero. A seguito di un invito a manifestare interesse, un SOC nazionale può essere selezionato dall'ECCC (European Cybersecurity Competence Centre) per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture e ricevere una sovvenzione per la gestione di tali strumenti e infrastrutture. Se diventa beneficiario del sostegno dell'Unione, un SOC nazionale si impegna a candidarsi per partecipare a un SOC transfrontaliero entro due anni.
I SOC transfrontalieri sono costituiti da un consorzio di almeno tre Stati membri, rappresentati dai SOC nazionali, che si impegnano a collaborare per coordinare le rispettive attività di rilevamento e monitoraggio delle minacce informatiche. A seguito di un invito iniziale a manifestare interesse, un consorzio ospitante può essere selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture e per ricevere una sovvenzione per la gestione di tali strumenti e infrastrutture. I SOC nazionali che partecipano a un SOC transfrontaliero condividono tra loro informazioni pertinenti relative alle minacce informatiche. Quando ottengono informazioni relative a un incidente cyber su vasta scala, potenziale o in corso, i SOC transfrontalieri forniscono le informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT e alla Commissione europea, in considerazione dei rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.
Quanto al "meccanismo per le emergenze di cybersicurezza, tale misura prevede azioni per sostenere la preparazione, la risposta agli incidenti di cyber significativi o su vasta scala e la ripresa immediata dagli stessi, o l'attenuazione di minacce informatiche significative, e azioni di assistenza reciproca. Tali azioni includono la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici.
Ai fini dell'attuazione delle richiamate azioni di risposta agli incidenti proposte, la presente proposta di regolamento istituisce una "riserva dell'UE per la cybersicurezza", che consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia, di cui potranno usufruire anche le autorità di

gestione delle crisi informatiche degli Stati membri e i CSIRT, nonché le istituzioni, gli organi e gli organismi dell'Unione. La responsabilità generale dell'attuazione della riserva dell'UE per la cybersicurezza è in capo alla Commissione europea che può affidare all'ENISA, in tutto o in parte, il funzionamento e l'amministrazione della medesima.
Quanto, invece, al meccanismo di riesame degli incidenti cyber, la proposta di regolamento prevede che, su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA debba riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente cyber significativo o su vasta scala.
Il "cyberscudo europeo" e il "meccanismo per le emergenze di cybersicurezza" saranno sostenuti dai finanziamenti del "programma Europa digitale", che la presente proposta di regolamento modificherà al fine di predisporre le suddette azioni, fornire un sostegno finanziario per il loro sviluppo e chiarire le condizioni per beneficiarne.

A. Rispetto dei principi dell'ordinamento europeo

1. Rispetto del principio di attribuzione, con particolare riguardo alla correttezza della base giuridica

- La proposta rispetta il principio di attribuzione in quanto conforme all'articolo 5.2 del trattato sull'Unione europea (TUE) ai sensi del quale l'Unione europea agisce esclusivamente nei limiti delle competenze che le sono attribuite nei trattati dell'UE.

Le azioni poste in essere con la presente proposta di regolamento, infatti, non vanno oltre quanto necessario per raggiungere gli obiettivi generali e specifici del regolamento e lasciano impregiudicate le competenze degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica, prevenzione, indagine, accertamento e perseguimento dei reati, così come gli obblighi giuridici dei soggetti che operano in settori critici e altamente critici di adottare misure di cybersicurezza, conformemente alla direttiva NIS 2.
La base giuridica della presente proposta è correttamente individuata nell'articolo 173, paragrafo 3, e nell'articolo 322, paragrafo 1, lettera a), del Trattato sul funzionamento dell'Unione europea (TFUE), tenuto conto del fatto che il presente regolamento mira a rafforzare la posizione competitiva del settore industriale e di quello dei servizi in Europa nell'ambito dell'economia digitalizzata e a sostenerne la trasformazione digitale, consolidando il livello di cybersicurezza nel mercato unico digitale.
Quanto all'articolo 322, paragrafo 1, lettera a), del TFUE, la presente proposta contiene norme specifiche in materia di riporto che derogano al principio dell'annualità di cui al regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio (il "regolamento finanziario").

2. Rispetto del principio di sussidiarietà

- La proposta rispetta il principio di sussidiarietà in quanto conforme all'articolo 5.3 del trattato sull'Unione europea (TUE) che esclude l'intervento dell'Unione quando una questione può essere regolata in modo efficace dagli Stati membri stessi a livello centrale, regionale o locale.

Infatti, la forte natura transfrontaliera delle minacce alla cybersicurezza e il numero crescente di rischi e incidenti, che hanno effetti di ricaduta a livello transfrontaliero e trasversalmente per i settori e i prodotti, fanno sì che gli obiettivi del presente intervento non possano essere raggiunti efficacemente dai soli Stati membri e richiedano dunque un'azione comune e la solidarietà a livello di Unione.
Il sostegno e le azioni a livello di Unione per migliorare il rilevamento delle minacce alla cybersicurezza nonché per accrescere la preparazione e le capacità di risposta apportano un valore aggiunto in quanto evitano la duplicazione degli sforzi nell'Unione e negli Stati membri. Ciò permetterà di sfruttare le risorse esistenti in modo più efficace e di intensificare il coordinamento e lo scambio di informazioni sugli insegnamenti tratti. Il "meccanismo per le emergenze di cybersicurezza" prevede, inoltre, la fornitura di sostegno ai paesi terzi associati al programma Europa digitale attingendo dalla riserva dell'UE per la cybersicurezza.
Il sostegno fornito tramite le varie iniziative che verranno attivate e finanziate a livello di Unione

integrerà e non duplicherà le capacità nazionali per quanto riguarda il rilevamento, la conoscenza situazionale, la preparazione e la risposta alle minacce e agli incidenti informatici.

3. Rispetto del principio di proporzionalità

- La proposta rispetta il principio di proporzionalità in quanto conforme all'articolo 5.4 del trattato sull'Unione europea (TUE) che stabilisce che il contenuto e la forma dell'azione dell'Unione devono limitarsi a quanto necessario per il conseguimento degli obiettivi dei trattati.

Infatti, le misure delle opzioni strategiche considerate dalla proposta di regolamento non superano quanto necessario per conseguire gli obiettivi generali e specifici dallo stesso prefissati.
La proposta è presentata in forma di regolamento del Parlamento europeo e del Consiglio in quanto tale strumento giuridico è ritenuto il più idoneo, con le sue disposizioni giuridiche direttamente applicabili, a fornire il grado di uniformità necessario per l'istituzione e il funzionamento di un "cyberscudo europeo" e di un "meccanismo per le emergenze di cybersicurezza", garantendo il sostegno del programma Europa digitale per la loro istituzione, nonché condizioni chiare per l'utilizzo e l'assegnazione di tale sostegno.
Più specificamente, le azioni contenute nella proposta normativa in esame non vanno oltre quanto necessario per raggiungere gli obiettivi generali e specifici del regolamento.

B. Valutazione complessiva del progetto e delle sue prospettive negoziali

1. Valutazione del progetto e urgenza

La valutazione delle finalità generali del progetto è complessivamente positiva in quanto la proposta di regolamento mira a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti cyber, nonché di preparazione e risposta agli stessi. Ciò consentirà di rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cybersicurezza nel mercato unico digitale.
Inoltre, contribuendo alla sicurezza delle informazioni digitali, la presente proposta concorrerà a tutelare il diritto alla libertà e alla sicurezza, in conformità dell'articolo 6 della Carta dei diritti fondamentali dell'Unione europea, e il diritto al rispetto della vita privata e della vita familiare, in conformità dell'articolo 7 della stessa. Proteggendo le imprese dagli attacchi informatici che possono causare danni economici, la proposta contribuirà, inoltre, a garantire la libertà d'impresa in conformità dell'articolo 16 della Carta dei diritti fondamentali dell'UE e il diritto di proprietà in conformità dell'articolo 17 della stessa. Infine, proteggendo l'integrità delle infrastrutture critiche dagli attacchi informatici, la proposta contribuirà a garantire il diritto alla protezione della salute, in conformità dell'articolo 35 della Carta dei diritti fondamentali dell'Unione europea, e il diritto all'accesso ai servizi d'interesse economico generale, in conformità dell'articolo 36 della stessa.
La proposta di regolamento è, inoltre, di particolare urgenza in quanto gli incidenti cyber significativi - che, come su illustrato, sono aumentati con il diffondersi dell'uso delle TIC - possono comportare perturbazioni tali da impedire a uno o più Stati membri colpiti di gestirle autonomamente e, per tale ragione, occorre urgentemente approntare un meccanismo di una solidarietà rafforzata a livello di Unione utile a migliorare il rilevamento delle minacce e degli incidenti cyber, nonché la preparazione e la risposta agli stessi.

2. Conformità del progetto all'interesse nazionale

Le disposizioni contenute nella proposta di regolamento possono ritenersi conformi all'interesse nazionale in quanto in linea con le iniziative poste in essere dal nostro Paese in materia di cybersicurezza.
Le misure approntate dalla proposta di regolamento e, in particolare, il "meccanismo per le emergenze di cybersicurezza", potrà fornire agli Stati membri che si trovano attualmente ad affrontare singolarmente crescenti rischi di cybersicurezza, un sostegno di emergenza per la preparazione, la risposta e la ripresa immediata/il ripristino del funzionamento dei servizi essenziali, integrando le loro misure e le loro risorse.
Inoltre, come su richiamato, tali azioni lasciano impregiudicate le competenze degli Stati membri

in materia di sicurezza nazionale, sicurezza pubblica, prevenzione, indagine, accertamento e perseguimento dei reati.

3. Prospettive negoziali ed eventuali modifiche ritenute necessarie od opportune

Attualmente non è stato ancora avviato il negoziato del CSoA in seno all'*Horizontal Working Party in Cyber Issues* (*HWPCI*) del Consiglio. Tale trattazione costituirà tuttavia una priorità per la prossima Presidenza del Consiglio dell'UE, che sarà assunta dalla Spagna nel secondo semestre dell'anno 2023.

Si precisa, pertanto, che la proposta nella sua versione originale è suscettibile di essere modificata nel corso del negoziato nell'ambito delle competenti sedi istituzionali europee e che la posizione della delegazione italiana potrà evolvere, agli esiti delle attività di coordinamento con le amministrazioni e le parti interessate.

Il testo presenta aspetti che necessitano di essere definiti in maniera migliore in sede negoziale e che riguardano principalmente:

- l'opportunità di definire ruolo e interazioni dei SOC nazionali rispetto agli CSIRT nazionali;
- il rischio di duplicazione tra meccanismi di comunicazione e condivisione delle informazioni previste dalla direttiva NIS 2 e il CSoA;
- la reale possibilità di contare sui servizi della riserva cyber in presenza di incidenti cyber significativi e su ampia scala e la definizione della più opportuna modalità di impiego dei fornitori privati dei servizi connessi alla riserva cyber;
- le modalità di contrattualizzazione dei servizi della riserva cyber. Quest'ultimo aspetto assume particolare rilevanza anche in ragione dell'aleatorietà della formulazione dell'articolo 14, paragrafo 4, del CSoA, secondo il quale "*Gli accordi di cui al paragrafo 3 [stipulati tra il fornitore di servizi e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE per la cybersicurezza] possono essere basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri*".

C. Valutazione d'impatto

1. Impatto finanziario

Premesso che al momento non è possibile prevedere con precisione l'impatto finanziario della proposta, lo stesso potrà essere meglio quantificato agli esiti del relativo negoziato, poiché viene introdotto un quadro per l'attuazione dei finanziamenti dell'UE al fine di incrementare la resilienza in materia di cybersicurezza mediante azioni volte a migliorare le capacità di rilevamento, risposta e ripresa in caso di incidenti cyber significativi e su vasta scala.

I fondi per realizzare le iniziative di cui al CSoA proverranno dall'obiettivo strategico "cybersecurity" del "*Digital European Programme*" (DEP) e saranno gestiti attraverso l'ECCC, il Centro di Competenze Cyber dell'UE. Il bilancio totale comprende un aumento di 100 milioni di euro che il Regolamento propone di riassegnare da altri obiettivi strategici del DEP. Ciò porterà il nuovo importo totale disponibile per le azioni di cybersicurezza nell'ambito del DEP a 842,8 milioni di euro.

2. Effetti sull'ordinamento nazionale

La proposta di regolamento potrà richiedere adeguamenti nell'ordinamento nazionale per consentirne l'attuazione, anche se al momento non sembrerebbe presentare particolari elementi di criticità.

In particolare, a livello nazionale gli adeguamenti che saranno necessari serviranno per il raggiungimento degli obiettivi del progetto legislativo, ossia:

a) la realizzazione di un'infrastruttura paneuropea di centri operativi di sicurezza ("cyberscudo europeo");

b) la creazione di un "meccanismo per le emergenze di cybersicurezza";

c) l'istituzione del "meccanismo europeo di riesame degli incidenti cyber".

3. Effetti sulle competenze regionali e delle autonomie locali

La proposta così come formulata non incide sulle competenze regionali e delle autonomie locali ai

sensi di quanto previsto dalla Costituzione, pertanto, la relazione non dovrà essere inviata alle Regioni, per il tramite delle loro Conferenze (art. 24, comma 2, della legge n. 234/2012).

4. Effetti sull'organizzazione della pubblica amministrazione

Al momento non è possibile individuare effetti sull'organizzazione della pubblica amministrazione. Poiché anche le pubbliche amministrazioni, così come le imprese e i cittadini dell'Unione, sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero, la realizzazione delle misure contenute nella presente proposta di regolamento potrà avere effetti positivi in termini di rafforzamento delle capacità di difesa dalle minacce e dagli incidenti cyber, e di preparazione e risposta agli stessi anche sulla pubblica amministrazione stessa.

5. Effetti sulle attività dei cittadini e delle imprese

Il presente progetto di legge, come su evidenziato, potrà rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cybersicurezza nel mercato unico digitale; ciò potrà accrescere la resilienza dei cittadini, delle imprese e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce alla cybersicurezza.

Inoltre, in sede applicativa, il presente regolamento non dovrebbe comportare alcun impatto amministrativo o ambientale significativo oltre a quelli indicati nella valutazione d'impatto del regolamento sul programma Europa digitale.

Altro

Si precisa che la proposta nella sua versione originale è suscettibile di essere modificata nel corso del negoziato nell'ambito delle competenti sedi istituzionali europee e che la posizione della delegazione italiana potrà evolvere, agli esiti del coordinamento con le amministrazioni e le parti interessate

LOGO
Amministrazione
con competenza
prevalente

Tabella di corrispondenza
ai sensi dell'art. 6, comma 5, della legge n. 234/2012

(D.P.C.M. 17marzo 2015)

Oggetto dell'atto: Proposta di …
– **Codice della proposta:** COM(aaaa) 000 del gg/mm/aaaa – **Codice interistituzionale:** aaaa/0000(xxx) – **Amministrazione con competenza prevalente:** Ministero …

Disposizione del progetto di atto legislativo dell'Unione europea (articolo e paragrafo)	**Norma nazionale vigente** (norma primaria e secondaria)	**Commento** (natura primaria o secondaria della norma, competenza ai sensi dell'art. 117 della Costituzione, eventuali oneri finanziari, impatto sull'ordinamento nazionale, oneri amministrativi aggiuntivi, amministrazioni coinvolte, eventuale necessità di intervento normativo di natura primaria o secondaria)