CAMERA DEI DEPUTATI N. **2318**

PROPOSTA DI LEGGE

d'iniziativa del deputato MAURI

Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione

Presentata il 24 marzo 2025

Onorevoli Colleghi ! – Negli ultimi anni l'Italia ha registrato un preoccupante aumento degli attacchi informatici a scopo di estorsione (*ransomware)*, ossia di quei programmi informatici dannosi *(malware)* che, crittografando tutti i dati, bloccano i sistemi informatici di imprese e pubbliche amministrazioni, chiedendo un riscatto per ripristinarli.

Un fenomeno, quello dell'attacco informatico a scopo di estorsione, che negli ultimi anni si è affermato come una delle minacce informatiche più rilevanti a livello nazionale, dimostrando non solo di avere un impatto diretto sull'economia delle nostre imprese e sull'erogazione dei servizi ai cittadini da parte delle pubbliche amministrazioni, ma caratterizzandosi sempre più spesso come una minaccia capace di impattare anche sulla sicurezza nazionale.

Nonostante sia particolarmente complesso stimare il numero esatto di questi attacchi informatici a causa delle ancora troppo numerose omesse segnalazioni e denunce da parte delle vittime, secondo i dati forniti a dicembre 2024 dall'Agenzia per la cybersicurezza nazionale (ACN), gli attacchi informatici a scopo di estorsione gestiti dal Gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia) sono in costante ascesa. Secondo gli ulteriori dati riferiti a luglio 2024, l'Italia si colloca al primo posto tra i Paesi dell'Unione europea maggiormente colpiti dalla minaccia di attacchi informatici a scopo di estorsione, seguita soltanto dalla Germania e dalla Spagna; invece, a livello mondiale, il nostro Paese è la terza nazione più colpita.

Sempre i dati ufficiali dell'ACN segnalano come le vittime appartengano prevalentemente al settore privato e si collochino nei grandi distretti industriali del Nord Italia, con le piccole imprese che, spesso per una limitata attitudine a una cultura della cybersicurezza, risultano essere la tipologia di vittima principale da parte degli

autori di questi attacchi. Peraltro, analizzando la loro distribuzione in base all'attività economica di appartenenza, il settore manifatturiero emerge come quello maggiormente colpito, seguito da altre tipologie di società private che fanno parte del comparto della vendita al dettaglio e dell'industria tecnologica.

Al contempo, la Relazione sulla politica dell'informazione per la sicurezza per l'anno 2024 (Doc. XXXIII, n. 3), trasmessa dal Governo alle Camere il 28 febbraio 2025, descrive un quadro ancora più preoccupante, evidenziando come gli attacchi informatici a scopo di estorsione si prestino oggi a un uso duale: da un lato, quello del mero profitto economico delle organizzazioni criminali e, dall'altro lato, in misura crescente, il perseguimento di finalità di spionaggio, di influenza, di disturbo e di sabotaggio digitale da parte di attori di matrice statuale.

Tra i mesi di gennaio e febbraio del 2025, ben due società sono state vittime di un attacco informatico a scopo di estorsione, che ha comportato il blocco delle attività produttive e commerciali, costringendole a richiedere all'Istituto nazionale della previdenza sociale di aderire alla cassa integrazione ordinaria per i propri dipendenti. Ciò, ovviamente, senza contare il numero, di difficile quantificazione, di soggetti privati che, pur di riprendere la normale operatività, sono stati costretti a cedere alla richiesta estorsiva pagando il riscatto richiesto.

La presente proposta di legge, quindi, si pone l'obiettivo di fornire ai cittadini, alle imprese che compongono il nostro tessuto produttivo e alle pubbliche amministrazioni una risposta concreta per arginare il fenomeno degli attacchi informatici a scopo di estorsione, migliorando la postura di contrasto di questo fenomeno tenuta finora dall'Italia e aumentando le capacità di resilienza di tutti gli attori coinvolti.

Pertanto, l'articolo 1, comma 1, della presente proposta di legge prevede una disposizione di delega al Governo, da esercitare entro sei mesi dalla data di entrata in vigore della legge, sulla base di dettagliati princìpi e criteri direttivi, indicati alle lettere da *a)* a *i)*.

In particolare, la lettera *a)* prevede il divieto di pagamento di un riscatto a seguito di una « estorsione informatica » per quei soggetti pubblici e privati compresi nell'applicazione delle disposizioni in materia di perimetro di sicurezza nazionale cibernetica di cui al decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, del decreto legislativo 4 settembre 2024, n. 138, e della legge 28 giugno 2024, n. 90. La violazione di tale divieto comporta l'applicazione di una sanzione amministrativa commisurata alla violazione medesima. Tale divieto può essere derogato solo attraverso una specifica determinazione del Presidente del Consiglio dei ministri in presenza di un rischio grave ed imminente per la sicurezza nazionale connesso all'attacco informatico a scopo di estorsione.

La lettera *b)* prevede che l'attacco informatico a scopo di estorsione condotto contro i soggetti pubblici e privati compresi nell'applicazione delle disposizioni in materia di perimetro di sicurezza nazionale cibernetica, del decreto legislativo 4 settembre 2024, n. 138, e della legge 28 giugno 2024, n. 90, possa essere qualificato dal Presidente del Consiglio dei ministri, discrezionalmente e non obbligatoriamente, come un incidente o una compromissione che comporti un pregiudizio per la sicurezza nazionale.

La lettera *c)* prevede che, nel caso di un attacco informatico a scopo di estorsione eventualmente qualificato come pregiudizievole per la sicurezza nazionale, il Presidente del Consiglio dei ministri possa decidere di applicare, discrezionalmente e non obbligatoriamente, le misure di *intelligence* di contrasto in ambito cibernetico, anche quando ci si trovi in situazioni di crisi o emergenza che siano fronteggiabili anche soltanto con azioni di resilienza.

La lettera *d)* estende le garanzie legate alle attività sotto copertura in favore degli ufficiali di polizia giudiziaria delle Forze dell'ordine impegnati in indagini su reati informatici anche su reti, sistemi informa-

tivi e servizi informatici posti al di fuori dei confini nazionali.

La lettera *e)* prevede l'introduzione di un obbligo di notifica al CSIRT Italia nei confronti di qualsivoglia soggetto pubblico e privato che subisca un attacco informatico a scopo di estorsione e i cui effetti non siano bloccati dalle misure di sicurezza prima dell'esecuzione dell'attacco informatico stesso. La notifica deve avvenire entro sei ore dal momento in cui il soggetto pubblico o privato ne ha avuto conoscenza, pena una sanzione amministrativa commisurata alla violazione. Il CSIRT Italia provvede tempestivamente a informare della notifica ricevuta la Polizia postale nonché, se pertinente e secondo le rispettive attribuzioni di vigilanza, le autorità competenti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, cosiddetto « regolamento DORA », previste dall'articolo 3 del decreto legislativo 10 marzo 2025, n. 23, ossia la Banca d'Italia, la Commissione nazionale per le società e la borsa, l'Istituto per la vigilanza sulle assicurazioni e la Commissione di vigilanza sui fondi pensione. Il CSIRT Italia, inoltre, provvede tempestivamente a informare della notifica ricevuta anche gli organismi di informazione per le loro finalità istituzionali nonché, ove rilevante per la difesa dello Stato, il Ministero della difesa nella sua qualità di Autorità nazionale di gestione delle crisi informatiche. Si prevede, infine, che l'adempimento dell'obbligo di notifica dell'attacco informatico a scopo di estorsione lasci impregiudicati eventuali ulteriori obblighi di notifica di incidenti informatici già previsti da altre normative.

La lettera *f)* prevede che l'ACN predisponga un piano di azione a concreto sostegno dei soggetti pubblici e privati colpiti da un attacco informatico a scopo di estorsione, che abbracci sia la fase preliminare volta a prevenire tale genere di attacchi sia quella di gestione e mitigazione dei suoi effetti.

La lettera *g)* prevede che sia istituito un nucleo d'intervento nazionale per il contrasto degli attacchi informatici a scopo di estorsione, incardinato nel CSIRT Italia, che funga da organo per l'attuazione di quanto previsto alla lettera *f)* e da punto unico di contatto per la resilienza a tale genere di attacchi informatici sia a livello nazionale che internazionale. Il nucleo d'intervento deve operare integrando tutti gli attori istituzionali che hanno ricevuto la notifica dell'attacco informatico a scopo di estorsione, i quali operano ciascuno per le proprie finalità a supporto della vittima.

La lettera *h)* prevede che siano introdotti degli incentivi sul piano economico a favore dell'ACN per la realizzazione delle attività di cui alle lettere *f)* e *g)*.

Infine, la lettera *i)* prevede che venga istituito il Fondo nazionale di risposta agli attacchi informatici a scopo di estorsione per supportare i soggetti pubblici e privati nel ristoro, anche solo parziale, delle perdite economiche subite a seguito di un attacco informatico a scopo di estorsione. Questo purché tali soggetti dimostrino di aver adempiuto all'obbligo di notifica di cui alla lettera *e)* e di aver applicato quanto previsto nel piano di azione di cui alla lettera *f)*.

Il comma 2 disciplina la procedura per l'esercizio della delega di cui al comma 1 e il comma 3 reca la disposizione di delega per l'adozione di disposizioni correttive e integrative dei decreti legislativi adottati.

Il comma 4, infine, prevede la copertura finanziaria.

PROPOSTA DI LEGGE

—

Art. 1.

1. Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione, sulla base dei seguenti princìpi e criteri direttivi:

a) previsione del divieto di pagamento di un riscatto a seguito delle condotte di cui all'articolo 629, terzo comma, del codice penale per i soggetti pubblici e privati di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, per i soggetti pubblici e privati inseriti nell'elenco dei soggetti essenziali e dei soggetti importanti ai sensi dell'articolo 7, comma 2, del decreto legislativo 4 settembre 2024, n. 138, nonché per i soggetti pubblici e privati di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90. La violazione di tale divieto comporta una sanzione amministrativa commisurata alla violazione. Tale divieto può essere derogato con atto del Presidente del Consiglio dei ministri in presenza di un rischio grave e imminente per la sicurezza nazionale connesso all'attacco informatico a scopo di estorsione;

b) introduzione di una disposizione che specifichi che l'attacco informatico a scopo di estorsione condotto contro e che generi effetti sui soggetti pubblici e privati di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sui soggetti pubblici e privati inseriti nell'elenco dei soggetti essenziali e dei soggetti importanti ai sensi dell'articolo 7, comma 2, del decreto legislativo 4 settembre 2024, n. 138, nonché sui soggetti pubblici e privati di cui all'articolo 1, comma 1, della legge 28 giu-

gno 2024, n. 90, possa essere qualificato, indipendentemente dal soggetto che lo ha realizzato, come un incidente o una compromissione che comporta un pregiudizio per la sicurezza nazionale, come definiti rispettivamente dalle lettere *h)*, *g)* e *f)* del comma 1 dell'articolo 1 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131. Tale qualificazione è effettuata dal Presidente del Consiglio dei ministri, ai sensi dell'articolo 2, comma 2, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) nel caso di cui alla lettera *b)*, attribuzione al Presidente del Consiglio dei ministri del potere di decidere l'eventuale applicazione delle misure di *intelligence* di contrasto in ambito cibernetico di cui all'articolo 7-*ter* del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, anche quando ci si trovi in situazioni di crisi o emergenza che siano fronteggiabili solo con azioni di resilienza;

d) introduzione di una disposizione che preveda che gli ufficiali di polizia giudiziaria delle Forze dell'ordine possano svolgere le attività sotto copertura di cui all'articolo 9, comma 1, lettera *b-ter)*, della legge 16 marzo 2006, n. 146, anche su reti, sistemi informativi e servizi informatici utilizzati per compiere reati informatici posti al di fuori dei confini nazionali;

e) previsione di un obbligo di notifica a carico di qualsivoglia soggetto pubblico e privato che subisca un attacco informatico a scopo di estorsione, ad esclusione dei casi in cui gli effetti dell'attacco siano neutralizzati dalle misure di sicurezza della vittima prima dell'esecuzione dell'attacco informatico stesso. Tale notifica è effettuata al Gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia) entro sei ore dal momento in cui il soggetto ne sia venuto a conoscenza, pena una sanzione amministrativa commisurata alla violazione. Il CSIRT Italia trasmette tempestivamente tale notifica all'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomuni-

cazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché, se pertinente e secondo le rispettive attribuzioni di vigilanza, alle autorità competenti ai sensi del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, previste dall'articolo 3, comma 1, del decreto legislativo 10 marzo 2025, n. 23. Il CSIRT Italia provvede, altresì, a trasmettere tempestivamente tale notifica agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, per le loro finalità istituzionali e, ove rilevanti per la difesa dello Stato, al Ministero della difesa, in qualità di Autorità nazionale di gestione delle crisi informatiche ai sensi dell'articolo 13 del decreto legislativo 4 settembre 2024, n. 138. L'adempimento dell'obbligo di notifica dell'attacco informatico a scopo di estorsione lascia impregiudicati eventuali ulteriori obblighi di notifica di incidenti informatici già previsti della normativa vigente;

f) introduzione di una disposizione che preveda che l'Agenzia per la cybersicurezza nazionale predisponga un piano di azione a sostegno dei soggetti pubblici e privati colpiti da un attacco informatico a scopo di estorsione con particolare riguardo anche per le pubbliche amministrazioni locali e le piccole e medie imprese, che preveda almeno il supporto operativo nelle fasi di gestione degli attacchi informatici a scopo di estorsione, di contenimento dei loro effetti, di recupero dell'operatività delle reti, dei sistemi informativi e dei servizi informatici colpiti, e di valutazione delle alternative all'eventuale pagamento del riscatto. Il piano di azione deve indicare anche le buone prassi e le misure di sicurezza informatica preventive a cui i soggetti pubblici e privati possono fare riferimento per mitigare il rischio di essere colpiti da un attacco informatico a scopo di estorsione;

g) istituzione di un nucleo d'intervento nazionale per il contrasto degli attacchi informatici a scopo di estorsione,

incardinato nel CSIRT Italia, che svolga il ruolo di:

1) coordinamento delle attività di cui alla lettera *f)*;

2) attuazione di quanto previsto dalla lettera *f)*;

3) punto di riferimento e contatto unico per i soggetti pubblici e privati colpiti da un attacco informatico a scopo di estorsione durante la gestione dell'emergenza;

4) punto di riferimento unico per la raccolta, analisi e condivisione delle informazioni per la resilienza agli attacchi informatici a scopo di estorsione, sia a livello nazionale che internazionale. Il nucleo di intervento del CSIRT Italia, nell'attuazione di quanto previsto alla lettera *f)*, è integrato con i soggetti di cui alla lettera *e)* destinatari della notifica dell'attacco informatico a scopo di estorsione dal CSIRT Italia;

h) introduzione di incentivi economici in favore dell'Agenzia per la cybersicurezza nazionale per la realizzazione delle attività di cui alle lettere *f)* e *g)*;

i) istituzione del Fondo nazionale di risposta agli attacchi informatici a scopo di estorsione per supportare i soggetti pubblici e privati nel ristoro, anche solo parziale, delle perdite economiche subite a seguito di un attacco informatico a scopo di estorsione, anche al fine di disincentivare il pagamento del riscatto. Prevedere, inoltre, che possano fare richiesta di ristoro economico al Fondo solo i soggetti pubblici e privati che dimostrino di avere effettuato la notifica di cui alla lettera *e)* nei termini e secondo le modalità ivi previste e di aver applicato quanto previsto nel piano di azione di cui alla lettera *f)*.

2. Gli schemi dei decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro dell'interno, sentita l'Agenzia per la cybersicurezza nazionale, e sono successivamente trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti per materia e per i profili finanziari. Decorsi sessanta giorni

dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine scada nei trenta giorni antecedenti la scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni. Entro i trenta giorni successivi all'espressione dei pareri, il Governo, ove non intenda conformarsi ai pareri parlamentari, ritrasmette i testi alle Camere, corredati dei necessari elementi integrativi di informazione, per l'espressione dei pareri definitivi da parte delle Commissioni parlamentari competenti, che sono espressi entro trenta giorni dalla data di trasmissione. Decorso tale termine, i decreti possono essere comunque emanati.

3. Entro un anno dalla data di entrata in vigore di ciascuno dei decreti legislativi adottati nell'esercizio della delega di cui al comma 1, il Governo può adottare uno o più decreti legislativi contenenti disposizioni correttive e integrative dei decreti legislativi medesimi, nel rispetto dei princìpi e criteri direttivi di cui al comma 1 e secondo la procedura di cui al comma 2.

4. Qualora uno o più decreti legislativi di cui al comma 1 determinino nuovi o maggiori oneri che non trovino compensazione al proprio interno, gli stessi decreti legislativi sono adottati solo successivamente o contestualmente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie, in conformità all'articolo 17, comma 2, della legge 31 dicembre 2009, n. 196.