COMMISSIONE
EUROPEA

Bruxelles, 13.9.2017
COM(2017) 474 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

che valuta in che misura gli Stati membri hanno adottato le misure necessarie per conformarsi alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio

Indice

1. Introduzione

Secondo la valutazione della minaccia della criminalità organizzata su internet (IOCTA) 2016 svolta dall'Europol, la criminalità informatica sta diventando più aggressiva e sfrontata. Questo fenomeno si può osservare in varie forme di criminalità informatica, tra cui gli attacchi ai sistemi di informazione[1]. Tra le gravi forme di attacchi menzionate dall'Europol figurano l'uso di software maligni e dell'ingegneria sociale per infiltrarsi in un sistema di informazione e acquisirne il controllo o per intercettare le comunicazioni e il lancio di attacchi alla rete su vasta scala, anche ai danni di infrastrutture critiche. Tali attacchi sono individuati come importanti minacce per la nostra società.

Data la quantità sempre maggiore di dati archiviati nelle nubi informatiche e considerata l'elevata mobilità delle informazioni e dei criminali, la cooperazione transfrontaliera fra le autorità di contrasto è diventata indispensabile per molte indagini sulla criminalità informatica.

Per contrastare tali reati in maniera efficace, gli Stati membri devono definire insieme quali atti debbano essere considerati attacchi ai danni dei sistemi di informazione. Devono anche avere livelli di sanzioni ravvicinati e disporre dei mezzi operativi per la comunicazione dei reati e lo scambio di informazioni fra le autorità. Di conseguenza, il 12 agosto 2013 il Parlamento europeo e il Consiglio hanno adottato la direttiva 2013/40/UE ("la direttiva") relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio[2].

1.1. Obiettivi e ambito di applicazione della direttiva

Gli obiettivi della direttiva sono ravvicinare il diritto penale degli Stati membri[3] nel settore degli attacchi contro i sistemi di informazione e migliorare la cooperazione fra le autorità competenti. A tal fine la direttiva stabilisce norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione e prescrive la predisposizione di punti di contatto operativi disponibili ventiquattr'ore su ventiquattro e sette giorni su sette.

Per quanto riguarda i termini pertinenti, la direttiva stabilisce le seguenti **definizioni**:

- "sistema di informazione" all'articolo 2, lettera a)[4]. La definizione è simile a quella di "sistema informatico" di cui all'articolo 1, lettera a), della convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001 ("la convenzione di Budapest"), tranne per il fatto che la direttiva comprende anche i dati informatici;

[1] Europol, 2016 Internet Organised Crime Threat Assessment (IOCTA), disponibile all'indirizzo: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:pdf.

[3] Nel prosieguo, salvo diversa ed esplicita indicazione, per "Stati membri" o "tutti gli Stati membri" si intendono gli Stati membri vincolati dalla direttiva, cioè tutti gli Stati membri dell'UE tranne la Danimarca, che non ha partecipato all'adozione della direttiva conformemente agli articoli 1 e 2 del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea (TFUE). Ai sensi dell'articolo 3 del protocollo 21 sulla posizione del Regno Unito e dell'Irlanda, entrambi i paesi hanno preso parte all'adozione della direttiva e sono da essa vincolati.

[4] Salvo diversa indicazione, tutti gli articoli menzionati si riferiscono a quelli della direttiva.

- "dati informatici" all'articolo 2, lettera b). La definizione segue quella di cui all'articolo 1, lettera b), della convenzione di Budapest, ma fa riferimento a un sistema di informazione invece che a un sistema computerizzato;
- "persona giuridica" all'articolo 2, lettera c). La definizione mira ad assicurare la responsabilità delle persone fisiche e giuridiche, escludendo gli Stati, gli organismi pubblici e le organizzazioni pubbliche internazionali;
- "senza diritto" all'articolo 2, lettera d). La definizione riguarda un principio generale di diritto penale e mira a escludere la responsabilità penale di una persona che agisce secondo quanto consentito a norma del diritto nazionale o con l'autorizzazione del proprietario o di un altro titolare di diritti sul sistema di informazione o su una sua parte.

Sono definiti alcuni **reati penali specifici**, ovvero:

- accesso illecito a sistemi di informazione (articolo 3);
- interferenza illecita relativamente ai sistemi (articolo 4), che comprende qualsiasi accesso illecito a un sistema di informazione che ne ostacoli gravemente o interrompa il funzionamento;
- interferenza illecita relativamente ai dati (articolo 5), cioè qualsiasi interferenza illegittima con dati informatici che ne comprometta l'integrità o la disponibilità;
- intercettazione illecita (articolo 6) di trasmissioni non pubbliche di dati informatici ed emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici;
- fornitura illecita di strumenti utilizzati per commettere i suddetti reati (articolo 7). In questo contesto, tali strumenti possono essere un programma per computer, una password di un computer o qualsiasi altro dato che permetta di accedere a un sistema di informazione.

Inoltre la direttiva **estende la responsabilità penale** all'istigazione, al favoreggiamento e al concorso, da parte di persone fisiche e/o giuridiche, nella commissione e nel tentativo di commettere i suddetti reati (articolo 8). L'istigazione, il favoreggiamento e il concorso riguardano tutti i reati di cui agli articoli da 3 a 7, mentre il tentativo riguarda soltanto gli articoli 4 e 5.

Il livello minimo delle **sanzioni** massime da infliggere per i reati previsti dalla direttiva è stabilito all'articolo 9:

- come base di partenza, è prevista una pena detentiva massima non inferiore a due anni per tutti i reati, tranne quelli di cui all'articolo 8 (articolo 9, paragrafo 2);
- una pena detentiva massima non inferiore a tre anni è inflitta per i reati di cui agli articoli 4 e 5, se un numero significativo di sistemi di informazione è stato colpito (in genere definiti reati "botnet"; articolo 9, paragrafo 3);
- una pena detentiva massima non inferiore a cinque anni è prevista per i reati di cui agli articoli 4 e 5 commessi da un'organizzazione criminale (articolo 9, paragrafo 4, lettera a)), che causano danni gravi (articolo 9, paragrafo 4, lettera b)) o commessi ai danni di un sistema di informazione di un'infrastruttura critica (articolo 9, paragrafo 4, lettera c));
- qualora un reato di cui agli articoli 4 e 5 sia commesso nel contesto di un abuso dei dati personali di un'altra persona, gli Stati membri assicurano che ciò possa essere

considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato (articolo 9, paragrafo 5).

Gli articoli successivi stabiliscono condizioni minime relative alla **responsabilità delle persone giuridiche** (articolo 10) e forniscono esempi di sanzioni che possono essere applicate nei loro confronti (articolo 11).

Riconoscendo che i reati di cui sopra possono essere commessi (nel senso di "messi in atto") in un luogo in cui l'autore del reato agisce concretamente, ma che i loro effetti sul sistema di informazione preso di mira possono manifestarsi altrove, l'articolo 12 prevede l'obbligo di stabilire la **competenza giurisdizionale** operando una distinzione fra:

- il luogo in cui l'autore del reato è fisicamente presente quando commette il reato,
- l'ubicazione del sistema di informazione preso di mira,
- la cittadinanza dell'autore del reato,
- il luogo in cui risiede abitualmente e
- il luogo in cui ha sede una persona giuridica a vantaggio della quale è commesso il reato.

Per quanto riguarda lo scambio di informazioni, l'articolo 13, paragrafo 1, impone agli Stati membri di predisporre **punti di contatto** operativi nazionali disponibili ventiquattr'ore su ventiquattro e sette giorni su sette, che possano rispondere a qualsiasi richiesta urgente proveniente dall'estero entro otto ore.

Gli Stati membri devono inoltre adottare le misure necessarie per **agevolare le comunicazioni** alle autorità nazionali competenti sui reati di cui sopra (articolo 13, paragrafo 3) e per raccogliere e condividere un minimo di **dati statistici** su tali reati (articolo 14).

1.2 Scopo e metodologia della relazione

L'articolo 16 della direttiva impone agli Stati membri di mettere in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttiva entro il 4 settembre 2015 e di comunicarne il testo alla Commissione.

La presente relazione risponde all'obbligo di cui all'articolo 17 della direttiva, che impone alla Commissione di presentare al Parlamento europeo e al Consiglio una relazione che valuta in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla direttiva. Scopo della relazione è dunque presentare un quadro generale, conciso ma informativo, delle principali misure di recepimento adottate dagli Stati membri.

Il recepimento negli Stati membri ha comportato la raccolta di informazioni sulle disposizioni legislative e amministrative pertinenti, la relativa analisi, l'elaborazione di nuovi atti legislativi o – nella maggior parte dei casi – la modifica di atti esistenti, fino all'adozione e infine alla comunicazione alla Commissione.

Entro il termine stabilito per il recepimento, 22 Stati membri avevano comunicato alla Commissione di aver portato a termine il recepimento della direttiva. Nel novembre 2015 la Commissione ha avviato procedimenti di infrazione per mancata comunicazione delle misure

nazionali di recepimento nei confronti degli altri Stati membri: BE, BG, EL, IE e SI[5]. Al 31 maggio 2017 i procedimenti di infrazione per mancata comunicazione delle misure nazionali di recepimento avviati nei confronti di BE, BG e IE erano ancora in corso[6].

Nella presente relazione, la descrizione e l'analisi si basano sulle informazioni fornite dagli Stati membri entro il 31 maggio 2017[7]. Le comunicazioni ricevute dopo tale data non sono state prese in considerazione. Sono state prese in considerazione tutte le misure comunicate riguardanti la legislazione nazionale, nonché le decisioni giudiziarie e, ove opportuno, le teorie giuridiche comuni. Nel corso dell'analisi, inoltre, la Commissione ha contattato direttamente gli Stati membri nei casi in cui era necessario e opportuno richiedere informazioni o chiarimenti supplementari. Tutte le informazioni raccolte sono state prese in considerazione ai fini dell'analisi.

Oltre alle problematiche individuate nella presente relazione, è possibile che vi siano altre difficoltà nel recepimento e altre disposizioni non comunicate alla Commissione o futuri sviluppi legislativi e non legislativi. Pertanto, la presente relazione non impedisce alla Commissione di valutare ulteriormente alcune disposizioni e di continuare a sostenere gli Stati membri nel recepimento e nell'attuazione della direttiva.

2. Misure di recepimento

2.1 Definizioni giuridiche (articolo 2 della direttiva)

L'articolo 2 della direttiva stabilisce le definizioni giuridiche di "sistema di informazione" (lettera a)), "dati informatici" (lettera b)), "persona giuridica" (lettera c)) e "senza diritto" (lettera d)). Soltanto CY e UK (Gibilterra) hanno introdotto una legislazione che copre tutti gli aspetti di tali definizioni. In particolare, ciò significa quanto segue.

a) Sistema di informazione

La definizione fornita nella direttiva si basa sulla definizione di "sistema informatico" di cui all'articolo 1, lettera a), della convenzione di Budapest, con l'aggiunta dei dati informatici quale elemento del sistema di informazione. CY, EL, IE, FI, HR, MT, PT e UK (Gibilterra) hanno adottato disposizioni legislative contenenti la definizione di un sistema di informazione, mentre DE, ES, FR, LU, LV, PL, SE e SK non hanno fornito informazioni definitive. Per quanto riguarda gli altri Stati membri, cioè AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI e UK (tranne Gibilterra), le rispettive definizioni giuridiche non menzionano specificamente i "dati informatici". Ciò implica un riferimento all'articolo 1, lettera a), della convenzione di Budapest con un ambito di applicazione identico a quello della definizione di "sistema informatico".

b) Dati informatici

L'espressione "dati informatici" è prevista dalla legislazione di AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO e UK (Gibilterra), mentre le informazioni comunicate da ES, FR, IT, LU, LV, PL, SE, SK e UK (tranne Gibilterra) non erano definitive. Tuttavia, nel

[5] Nel presente documento, gli Stati membri sono indicati secondo i seguenti codici: http://publications.europa.eu/code/it/it-5000600.htm.

[6] Per informazioni sulle decisioni della Commissione relative ai procedimenti di infrazione consultare il seguente indirizzo: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

[7] IE ha comunicato il pieno recepimento della direttiva il 31 maggio 2017.

caso della SE, la struttura specifica degli articoli di riferimento rende superflua questa definizione. Per quanto riguarda i restanti Stati membri, in HU la definizione di "dati informatici" si riferisce soltanto ai reati di cui agli articoli 4 e 5 della direttiva, mentre BE e SI non hanno incluso nella definizione di dati informatici "un programma atto a far svolgere una funzione a un sistema di informazione".

c) Persona giuridica
Ad eccezione del LU, che non ha fornito informazioni definitive sul recepimento dell'articolo 2, lettera c), il recepimento della definizione di "persona giuridica" non ha creato problemi. In generale, ciò è dovuto al fatto che è già presente in molte disposizioni di diritto civile o commerciale degli Stati membri. Soltanto CY ha previsto una disposizione specifica nelle misure adottate per il recepimento della direttiva.

d) Senza diritto
Riguardo alla definizione dell'espressione "senza diritto" di cui all'articolo 2, lettera d), soltanto CY, IE, RO e UK (Gibilterra) hanno comunicato il recepimento, mentre gli altri 23 Stati membri non hanno adottato misure per il recepimento di questa definizione. Va tuttavia osservato che in tutti gli Stati membri vige il principio generale dell'assenza di responsabilità penale per qualsiasi atto compiuto con la relativa autorizzazione.

2.2 Reati penali specifici (articoli da 3 a 7 della direttiva)

a) Accesso illecito a sistemi di informazione
Per quanto riguarda l'accesso illecito a un sistema di informazione, l'articolo 3 della direttiva è compreso nella legislazione nazionale di AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE e SK.

In tutti gli altri Stati membri, cioè BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI e UK, la rispettiva descrizione nazionale del reato penale non distingue fra ottenere l'accesso all'intero sistema di informazione o solo a una parte di esso, anche se tale distinzione è espressamente prevista dalla direttiva. Inoltre il recepimento non contempla il semplice accesso alle apparecchiature informatiche (hardware) in DE e prevede disposizioni supplementari riguardanti una particolare intenzione (intenzione di ottenere informazioni, infliggere uno svantaggio o intenzione fraudolenta) in AT e LU e il fatto di causare un danno rilevante in LV. Nel caso di BE, BG, FR, HR, LU, MT, PT, RO, SI e UK, l'ambito di applicazione delle disposizioni nazionali è più ampio di quello della direttiva, in quanto non è prevista l'elusione di alcuna misura di sicurezza per stabilire la responsabilità penale. Gli altri Stati membri prevedono letteralmente che il reato sia commesso in violazione di una misura di sicurezza (CY, EL e SK) o usano una terminologia analoga per descrivere questo aspetto (AT, CZ, DE, EE, ES, FI, HU, IT; LT, LV, NL, PL e SE).

b) Interferenza illecita relativamente ai sistemi
L'articolo 4 della direttiva riguarda l'interferenza illecita relativamente ai sistemi. La direttiva elenca otto possibili azioni (l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendere tali dati inaccessibili) e due possibili risultati della rispettiva azione (ostacolare gravemente o interrompere il funzionamento di un sistema di informazione). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE e UK (tranne Gibilterra) hanno introdotto disposizioni legislative corrispondenti. BG fa riferimento soltanto all'immissione di un virus, mentre gli altri Stati membri (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK e UK) non menzionano espressamente da una a quattro possibili azioni. In questo contesto, si può osservare che i

problemi sono emersi soprattutto riguardo ai termini "deterioramento" (mancante in otto casi) e "rendere inaccessibili" (mancante in nove casi).

c) Interferenza illecita relativamente ai dati
L'articolo 5 della direttiva riguarda l'interferenza illecita relativamente ai dati ed elenca i sei possibili atti seguenti: cancellare, danneggiare, deteriorare, alterare, sopprimere dati informatici o renderli inaccessibili. CY, EL, IE e MT hanno recepito la disposizione letteralmente; BE, CZ, LT, PT e SE hanno usato termini più generici per comprendere tutti i possibili atti. Le misure di recepimento di tutti gli altri Stati membri non comprendono ciascuna possibilità, ma indicano soltanto cinque alternative (FI e SK) o meno (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI e UK). La maggior parte dei problemi è emersa riguardo ai termini "danneggiare" (mancante in otto casi), "deteriorare" (13 casi), "sopprimere dati" (11 casi) e "rendere i dati inaccessibili" (13 casi). Oltre alla formulazione prevista dalla direttiva, FI prevede "l'intenzione di arrecare danni o perdite finanziarie" per la responsabilità penale mentre LT e LV prevedono "l'atto di causare un danno grave o rilevante".

d) Intercettazione illecita
L'articolo 6 riguarda l'intercettazione illecita e si riferisce alla trasmissione non pubblica di dati informatici ed emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK e UK (Gibilterra) hanno introdotto una legislazione che copre integralmente l'articolo 6. Per quanto riguarda l'intercettazione di dati informatici, l'ambito di applicazione generale della direttiva è limitato ai messaggi (AT e BG), all'osservazione di una persona (EE) o alla corrispondenza (FR e HU). Le misure di recepimento dei seguenti Stati membri peraltro non comprendono l'intercettazione di emissioni elettromagnetiche: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI e UK (tranne Gibilterra). Inoltre alcuni Stati membri prevedono una particolare intenzione (per esempio ottenere informazioni o un vantaggio economico, o provocare uno svantaggio – si vedano AT, EL, HU) o atti supplementari specifici (per esempio registrare o venire a conoscenza dei contenuti intercettati – si vedano BG e HU).

e) Strumenti utilizzati per commettere i reati
L'articolo 7 penalizza alcuni atti riguardanti gli strumenti, quali i programmi per computer o i codici di accesso, utilizzati al fine di commettere i reati di cui agli articoli da 3 a 6: la fabbricazione di tali strumenti, la loro vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo. AT, BE, CY, DE, EL, IE e SK hanno introdotto disposizioni nazionali corrispondenti. Alcuni Stati membri non coprono tutti i reati menzionati (EE, IT, MT, PL e SI). Alcuni non indicano l'autore degli atti di cui all'articolo 7 come una persona diversa dall'autore dei reati di cui agli articoli da 3 a 6 (CZ e SI). Alcuni prevedono una particolare intenzione (infliggere un danno o agire in modo fraudolento – si vedano FI, IT e LU), un risultato specifico, per esempio una violazione della segretezza (BG) o almeno un certo livello di preparazione dei reati menzionati (SE). Infine le discrepanze tra l'articolo 7 e le disposizioni nazionali riguardano il mancato recepimento di tutti i possibili atti elencati. Il problema interessa BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI e UK. Fra questi, la legislazione del LU menziona specificamente cinque dei sei possibili atti elencati nella direttiva, mentre gli altri Stati membri ne indicano espressamente solo quattro o meno.

Soltanto la ES ha recepito l'atto di approvvigionamento per l'uso.

2.3 Norme generali relative ai reati (articoli da 8 a 12 della direttiva)

a) Istigazione, favoreggiamento e concorso

L'articolo 8, paragrafo 1, impone agli Stati membri di garantire che l'istigazione o il favoreggiamento e il concorso nella commissione di un reato di cui agli articoli da 3 a 7 siano punibili come reato. Tutti gli Stati membri hanno recepito questa disposizione.

b) Tentativo

Secondo l'articolo 8, paragrafo 2, il tentativo di commettere i reati di cui agli articoli 4 e 5 deve essere punibile come reato. Il PT non comprende tutti i tipi di tentativi di commettere i reati di cui all'articolo 4 e la SE non prevede la responsabilità penale per il tentato reato di "violazione della segretezza delle comunicazioni", ma tutti gli altri Stati membri si avvalgono di una legislazione che recepisce questa disposizione.

c) Sanzioni

aa) Disposizione generale

L'articolo 9, paragrafo 1, impone agli Stati membri, in generale, di prevedere sanzioni effettive, proporzionate e dissuasive per i reati rientranti nell'ambito di applicazione della direttiva. La disposizione si considera recepita in quasi tutti gli Stati membri, ma AT, BE, BG, IT, PT, SE e SI non rispettano i livelli minimi delle sanzioni massime previsti all'articolo 9, paragrafo 2, (si veda il punto 1.1 *supra*) in tutti i casi. Ciò incide sul recepimento dell'articolo 9, paragrafo 1, in quanto si può concludere che le prescrizioni minime di cui all'articolo 9, paragrafo 2, siano il minimo necessario per considerare una sanzione effettiva, proporzionata e dissuasiva.

bb) Livello minimo generale della sanzione massima

Secondo l'articolo 9, paragrafo 2, il livello minimo della sanzione massima per i reati ordinari di cui agli articoli da 3 a 7 è una pena detentiva non inferiore a due anni. La maggior parte degli Stati membri si è conformata a questa disposizione. Soltanto sei Stati membri presentano alcune discrepanze: AT (pena detentiva massima di sei mesi), BG (pena detentiva massima di un anno per tutti i reati, tranne l'intercettazione illecita,), IT (pena detentiva massima di un anno per il reato di cui all'articolo 7, lettera b)), PT (pena detentiva massima di un anno per il reato di cui all'articolo 3), SE (pena detentiva massima di un anno per il reato di "infliggere un danno") e SI (pena detentiva massima di un anno per i reati di cui agli articoli 3, 6 e 7). Nel caso del BE, il livello minimo della sanzione massima per i reati di cui agli articoli 3, 6 e 7 si raggiunge soltanto se i reati sono commessi con un'intenzione fraudolenta.

cc) Un numero significativo di sistemi di informazione colpiti

L'articolo 9, paragrafo 3, eleva il livello minimo delle sanzioni massime a tre anni di detenzione quando un numero significativo di sistemi di informazione è stato colpito commettendo un reato di cui agli articoli 4 e 5. In generale, gli Stati membri hanno introdotto una disposizione corrispondente; DE menziona soltanto i sistemi di informazione "che rivestono importanza considerevole per altri", FI prevede la valutazione del reato "nel suo insieme" per applicare la pena detentiva più elevata e LV non fa riferimento a un numero significativo di sistemi di informazione (o formulazione analoga), ma solo al fatto di causare un "danno rilevante". Le informazioni fornite da BG e SI non erano definitive.

dd) Organizzazioni criminali

A norma dell'articolo 9, paragrafo 4, lettera a), per i reati di cui agli articoli 4 e 5 si applica una pena detentiva massima non inferiore a cinque anni, qualora siano commessi da un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI.

Anche in questo caso, la maggior parte degli Stati membri si è conformata alla disposizione di cui all'articolo 9, paragrafo 4, lettera a). Ai sensi del diritto penale di LU e SI, i reati informatici non rientrano nell'ambito di applicazione delle disposizioni relative ai reati commessi da un'organizzazione criminale. La legislazione del BE prevede una pena detentiva massima di soli tre anni per i reati di cui all'articolo 5, la legislazione della DE non contempla le persone fisiche quali vittime dei reati, la legislazione della FI prevede una valutazione supplementare del reato "nel suo insieme" e la legislazione della SE prevede una pena detentiva massima di quattro anni qualora sia "inflitto un danno rilevante".

ee) Danni gravi

L'articolo 9, paragrafo 4, lettera b), stabilisce un pena detentiva massima non inferiore a cinque anni per i reati di cui agli articoli 4 e 5 qualora causino danni gravi. Sebbene non sia fornita una definizione di cosa debba essere considerato danno grave, tutti gli Stati membri tranne BG, DE, FI, HU, LU e SE hanno introdotto una legislazione corrispondente alla direttiva. Le informazioni fornite dalla HU non erano definitive. La BG non raggiunge il livello minimo di cinque anni per la sanzione massima, mentre il LU fa riferimento a una clausola generale sulle sanzioni applicate qualora siano causati danni gravi che non si applica ai reati informatici. Sono presenti piccole discrepanze in DE (le persone fisiche non sono contemplate quali vittime dei reati), FI (la sanzione più elevata richiede una valutazione supplementare del reato "nel suo insieme") e SE (pena detentiva massima di quattro anni qualora sia "inflitto un danno rilevante").

ff) Sistemi di informazione di infrastrutture critiche

Anche nel caso in cui i reati di cui agli articoli 4 e 5 riguardino i sistemi di informazione di infrastrutture critiche si applica una sanzione massima non inferiore a cinque anni, come indicato all'articolo 9, paragrafo 4, lettera c).

La maggior parte degli Stati membri si è conformata a questa disposizione, mentre la BG non ha fornito informazioni specifiche sul recepimento. Il BE ha fissato una pena detentiva massima di tre anni per i reati di cui all'articolo 5. La DE non contempla le persone fisiche come vittime. La FI prevede una valutazione supplementare del reato "nel suo insieme", l'IT prevede che sia causata l'effettiva "distruzione", il PT prevede un attacco "grave con effetti duraturi" e non menziona l'articolo 5 e la SE soddisfa le prescrizioni della direttiva soltanto per il reato di "sabotaggio rilevante".

gg) Furto d'identità e altri reati connessi all'identità

L'articolo 9, paragrafo 5, impone agli Stati membri di assicurare che, qualora i reati di cui agli articoli 4 e 5 siano commessi abusando dei dati personali di un’altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo proprietario dell’identità, ciò possa essere considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato. Gli ampi margini di discrezionalità hanno determinato una grande varietà di misure di recepimento negli Stati membri. BE ed EL non hanno comunicato misure di recepimento e in CZ la legislazione penale non contiene una disposizione specifica al riguardo. L'approccio della circostanza aggravante è stato scelto da AT, CY, ES, IE, MT, PT e SE (quest'ultima fa riferimento alla circostanza della "particolare pianificazione"), mentre tutti gli altri Stati membri rimandano ad altre disposizioni relative al reato specifico. Fra i paesi che rimandano a disposizioni specifiche, si possono osservare i seguenti problemi di recepimento: BG e NL prevedono una particolare intenzione ("procurare un vantaggio" e "intento di contraffazione o abuso di identità"), la DE fa riferimento soltanto a "dati personali generalmente non accessibili", la FR menziona solo il nome di una persona e

nessun altro dato personale, la LV prevede che sia causato "un danno rilevante", la RO menziona soltanto l'uso di "un documento" e prevede che sia commesso un inganno.

d) Responsabilità delle persone giuridiche

aa) In generale

L'articolo 10, paragrafo 1, impone di considerare una persona giuridica responsabile dei reati di cui agli articoli da 3 a 8, qualora l'autore del reato abbia il potere di rappresentanza della persona giuridica (lettera a), il potere di prendere decisioni per conto della persona giuridica (lettera b) o il potere di esercitare il controllo in seno alla persona giuridica (lettera c). Tutti gli Stati membri hanno introdotto disposizioni legislative corrispondenti a questo articolo e sono emersi soltanto problemi di minore entità: la BG non ha incluso il reato di cui all'articolo 6 e la HR non menziona un autore del reato che abbia il potere di esercitare il controllo in seno alla persona giuridica (articolo 10, paragrafo 1, lettera c)).

bb) Per mancata sorveglianza o mancato controllo

L'articolo 10, paragrafo 2, impone agli Stati membri di prevedere che le persone giuridiche siano ritenute responsabili qualora sia stata permessa la commissione di un reato di cui agli articoli da 3 a 8 a causa della mancata sorveglianza o del mancato controllo da parte di una persona di cui all'articolo 10, paragrafo 1. Quasi tutti gli Stati membri si sono conformati alla disposizione, mentre il LU non ha fornito informazioni definitive e la BG non menziona la commissione di un reato rientrante nell'ambito di applicazione dell'articolo 6.

e) Sanzioni applicabili alle persone giuridiche

aa) Sanzioni obbligatorie

L'articolo 11, paragrafo 1, della direttiva impone agli Stati membri di prevedere sanzioni pecuniarie penali o non penali quali sanzioni effettive, proporzionate e dissuasive da infliggere alle persone giuridiche. Tutti gli Stati membri hanno comunicato misure nazionali di recepimento, tranne IE e UK. In questi due paesi, l'importo massimo delle sanzioni pecuniarie non è stato determinato a causa della mancanza di disposizioni legislative concrete. Non è quindi possibile valutare se le rispettive sanzioni pecuniarie siano effettive, proporzionate e dissuasive.

bb) Sanzioni facoltative

L'articolo 11, paragrafo 1, contiene anche un elenco di possibili sanzioni supplementari da infliggere alle persone giuridiche. Tali sanzioni sono: l'esclusione dal godimento di un beneficio o aiuto pubblico (adottata da CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT e SK), l'interdizione temporanea o permanente dall'esercizio di attività commerciali (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI e SK), l'assoggettamento a sorveglianza giudiziaria (CY, ES, FR, MT, PT e RO), provvedimenti giudiziari di scioglimento (CY, CZ, EL, ES, FR, HR, HU,LT, LU, LV, MT, PT, RO, SI e SK) e la chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato (BE, CY, WS, FR, LT, MT, PT e RO). BG, DE, EE, IE, FI, NL e UK invece non hanno scelto alcuna alternativa.

cc) Sanzioni in caso di omissione

Secondo l'articolo 11, paragrafo 2, gli Stati membri devono garantire che siano inflitte sanzioni effettive, proporzionate e dissuasive alle persone giuridiche responsabili dei reati di omissione di cui all'articolo 10, paragrafo 2. Le informazioni fornite dal LU non erano definitive. Tutti gli altri Stati membri, tranne IE e UK, hanno previsto disposizioni legislative corrispondenti. Nel caso di IE e UK, lo stesso problema emerge per l'articolo 11, paragrafo 1: (si veda il punto aa) *supra*).

f) Competenza giurisdizionale

aa) Criteri di competenza prescritti

L'articolo 12, paragrafi 2 e 3, della direttiva impone agli Stati membri di stabilire la propria competenza giurisdizionale per i reati di cui agli articoli da 3 a 8 quando il reato sia stato commesso in tutto o in parte sul loro territorio – sia che l'autore vi fosse fisicamente presente mentre commetteva il reato sia che il sistema di informazione colpito fosse ubicato nel rispettivo territorio – o quando il reato sia stato commesso all'estero da un loro cittadino. La maggior parte degli Stati membri ha introdotto disposizioni nazionali corrispondenti; la legislazione dell'IT non stabilisce la competenza giurisdizionale per i propri cittadini all'estero in caso di reati di base, la legislazione di LV e SI fa riferimento a disposizioni poco chiare in materia di competenza, la competenza giurisdizionale di MT per la commissione parziale sul proprio territorio non è chiara e UK fa riferimento a un computer invece che a un sistema di informazione.

bb) Altri criteri di competenza

L'articolo 12, paragrafo 3, prevede che ogni Stato membro, ove stabilisca la propria competenza giurisdizionale nei casi in cui l'autore del reato risieda abitualmente nel suo territorio (scelto da AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE e SK) o nei casi in cui il reato sia stato commesso a vantaggio di una persona giuridica che ha sede nel suo territorio (CY, CZ, LV, PT, RO e SK), lo comunichi alla Commissione.

2.4 Aspetti operativi (articoli 13 e 14 della direttiva)

a) Disposizione relativa ai punti di contatto operativi nazionali

L'articolo 13, paragrafo 1, prevede che gli Stati membri istituiscano punti di contatto operativi nazionali per lo scambio di informazioni relative ai reati di cui agli articoli da 3 a 8. A norma di detta disposizione, gli Stati membri devono garantire di predisporre procedure tali da consentire all'autorità competente di rispondere a ogni richiesta di assistenza urgente entro otto ore dalla richiesta stessa. Secondo le informazioni comunicate, la maggior parte degli Stati membri ha istituito l'infrastruttura necessaria. IE e RO hanno comunicato che i rispettivi punti di contatto sono disponibili soltanto alcune ore al giorno, il che non consente alle autorità di fornire in ogni possibile caso una risposta entro otto ore dalla richiesta. Vari Stati membri hanno indicato di utilizzare le reti esistenti di punti di contatto operativi istituiti tramite la rete G7 o nel quadro della convenzione del Consiglio d'Europa sulla criminalità informatica.

b) Informazioni in merito ai punti di contatto operativi nazionali

A norma dell'articolo 13, paragrafo 2, gli Stati membri sono tenuti a fornire alla Commissione informazioni in merito al rispettivo punto di contatto ed essa le trasmette agli altri Stati membri. Tutti gli Stati membri hanno fornito le informazioni necessarie.

c) Canali di comunicazione

L'articolo 13, paragrafo 3, impone agli Stati membri di assicurare che siano disponibili idonei canali di comunicazione per agevolare le comunicazioni alle autorità nazionali competenti sui reati di cui agli articoli da 3 a 6. Le informazioni fornite da HR, IT, IE e PT non erano definitive. Negli altri Stati membri sembrano essere stati adottati diversi approcci per la predisposizione dei canali di comunicazione. La maggior parte degli Stati membri (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK e UK) ha comunicato misure che prevedono canali atti a facilitare le comunicazioni da parte della persona o dell'organizzazione che denuncia inizialmente un reato, per esempio la vittima di un attacco informatico (con i canali di comunicazione effettivi non precisati da LV). Altri Stati

membri (AT, ES e LU) hanno invece fornito informazioni identiche sull'attuazione dell'articolo 13, paragrafi 1 e 2, dalle quali risulta che le rispettive misure faciliteranno soprattutto le comunicazioni fra le autorità competenti.

d) Raccolta di dati statistici
Secondo l'articolo 14, paragrafi 1 e 2, gli Stati membri devono predisporre un sistema di registrazione, produzione e fornitura di dati statistici, come minimo sul numero dei reati di cui agli articoli da 3 a 7 registrati dagli Stati membri e sul numero di persone che sono state oggetto di un procedimento giudiziario e che sono state condannate per tali reati. Stando alle comunicazioni ricevute, la maggior parte degli Stati membri sembra avere adottato le misure legislative e amministrative per garantire la raccolta delle informazioni, di solito sulla base di un sistema elettronico nazionale generale. Le informazioni fornite da alcuni Stati membri non erano definitive (EL, IE, UK (Gibilterra, Irlanda del Nord e Scozia)), in quanto le informazioni sui reati specifici di cui alla direttiva potrebbero non essere raccolte separatamente (BE, DE e SE) o le informazioni raccolte potrebbero non comprendere tutti i reati di cui alla direttiva (RO).

e) Trasmissione dei dati statistici alla Commissione
L'articolo 14, paragrafo 3, prevede che gli Stati membri trasmettano alla Commissione i rispettivi dati statistici. Tutti gli Stati membri che hanno comunicato misure, tranne UK (Gibilterra, Irlanda del Nord e Scozia) e HU, hanno confermato di avere adottato misure giuridiche o amministrative o entrambe per assicurare il rispetto di questo obbligo. Per quanto riguarda EL, ES, LU e SI, le informazioni fornite non erano definitive.

3. Conclusione e iniziative future

La direttiva ha determinato progressi sostanziali in termini di penalizzazione degli attacchi informatici a un livello analogo in tutti gli Stati membri, facilitando la cooperazione transfrontaliera fra le autorità di contrasto che indagano su questo tipo di reati. Gli Stati membri hanno modificato i codici penali e altre normative pertinenti, semplificato le procedure e avviato o migliorato programmi di cooperazione. La Commissione riconosce i grandi sforzi compiuti dagli Stati membri per dare attuazione alla direttiva.

Tuttavia, esistono ancora ampi margini d’azione perché la direttiva possa raggiungere le sue piene potenzialità, se gli Stati membri garantiranno l'attuazione completa di tutte le sue disposizioni. In base all'analisi condotta finora, alcuni principali miglioramenti che gli Stati membri devono realizzare riguardano l'uso delle definizioni (articolo 2), che incide sull'entità dei reati definiti nel diritto nazionale sulla base della direttiva. Inoltre, gli Stati membri sembrano avere avuto problemi a includere tutte le possibilità nel definire le azioni che costituiscono reati (articoli da 3 a 7) e a prevedere norme comuni in materia di sanzioni per gli attacchi informatici (articolo 9). Altre problematiche sembrano riguardare l'attuazione delle disposizioni amministrative riguardanti i canali di comunicazione idonei (articolo 13, paragrafo 3) e il monitoraggio e le statistiche sui reati contemplati dalla direttiva (articolo 14).

La Commissione continuerà a fornire sostegno agli Stati membri ai fini dell'attuazione della direttiva. In vista del potenziale contributo alla cooperazione transfrontaliera, tale sostegno riguarderà, in particolare, le disposizioni operative della direttiva sullo scambio di informazioni (articolo 13, paragrafi 1 e 2), i canali di comunicazione (articolo 13, paragrafo 3) e il monitoraggio e le statistiche (articolo 14). A tal fine, la Commissione offrirà agli Stati membri nuove opportunità di individuazione e scambio di migliori pratiche nella seconda metà del 2017.

La Commissione al momento non ritiene necessario proporre modifiche della direttiva. Sta invece studiando, anche a sostegno delle indagini penali relative agli attacchi ai sistemi di informazione, alla criminalità informatica e ad altri tipi di reati, misure volte a migliorare l'accesso transfrontaliero alle prove elettroniche per le indagini penali, compresa la proposta di misure legislative entro l'inizio del 2018[8]. La Commissione sta anche esaminando il ruolo della crittografia nelle indagini penali e presenterà una relazione sulle proprie conclusioni entro ottobre 2017[9].

La Commissione si impegna a garantire che il recepimento sia completato in tutta l'UE e che le disposizioni siano attuate correttamente, anche controllando che le misure nazionali siano conformi alle disposizioni corrispondenti della direttiva. Ove necessario, la Commissione si avvarrà dei poteri di esecuzione di cui dispone in forza dei trattati e li eserciterà mediante l'avvio di procedure di infrazione.

[8] Valutazione d'impatto iniziale sul miglioramento dell'accesso transfrontaliero alle prove elettroniche, del 4 agosto 2017, reperibile su ec.europa.eu.

[9] Comunicazione sull'ottava relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza, COM(2017) 354 final.