COMMISSIONE EUROPEA

Bruxelles, 30.9.2010
COM(2010) 517 definitivo

2010/0273 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

RELAZIONE

1. MOTIVAZIONI E OBIETTIVI DELLA PROPOSTA

La presente proposta è volta a sostituire la decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione[1]. Come specificato nei suoi considerando, la decisione quadro rispondeva all'obiettivo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione. La decisione quadro ha così creato una legislazione europea per trattare reati quali l'accesso illecito a sistemi di informazione, l'interferenza illecita per quanto riguarda i sistemi e l'interferenza illecita per quanto riguarda i dati, così come specifiche norme sulla responsabilità delle persone giuridiche, sulla competenza giurisdizionale e sullo scambio di informazioni. Gli Stati membri erano tenuti ad adottare le misure necessarie per conformarsi alle disposizioni della decisione quadro entro il 16 marzo 2007.

Il 14 luglio 2008 la Commissione ha pubblicato una relazione sull'attuazione della decisione quadro[2]. Nelle conclusioni della relazione si osservava che erano stati fatti progressi significativi nella maggior parte degli Stati membri e che il grado di attuazione era relativamente buono, ma che alcuni Stati membri non avevano ancora portato a termine tale processo. La relazione indicava in seguito: "I recenti attacchi perpetrati in Europa dall'adozione della decisione quadro hanno evidenziato l'emergere di varie minacce, in particolare gli attacchi massicci simultanei contro i sistemi di informazione e l'uso crescente delle botnet a fini criminali. Questi attacchi non erano al centro dell'attenzione al momento dell'adozione della decisione quadro. Per far fronte alle nuove evoluzioni, la Commissione prenderà in considerazione l'adozione di misure per reagire più prontamente alle minacce" (per la spiegazione del termine "botnet" si veda la prossima sezione).

L'importanza di prendere nuove misure per intensificare la lotta contro la criminalità informatica è stata sottolineata nel programma dell'Aia del 2004 inteso a rafforzare la libertà, la sicurezza e la giustizia dell'Unione europea, così come nel programma di Stoccolma del 2009 e il relativo piano d'azione[3]. Inoltre, la recentemente adottata agenda digitale europea[4], prima iniziativa faro lanciata nell'ambito della strategia Europa 2020, ha riconosciuto la necessità di affrontare l'emergere di nuove forme di criminalità, in particolare la criminalità informatica, a livello europeo. Nell'area d'azione incentrata sulla fiducia e sulla sicurezza, la Commissione si è impegnata a presentare misure per combattere gli attacchi informatici contro i sistemi d'informazione.

A livello internazionale, la Convenzione del Consiglio d'Europa sulla criminalità informatica ("Convenzione sulla criminalità informatica"), firmata il 23 novembre 2001, è considerata come la norma internazionale finora più completa, poiché fornisce un quadro esaustivo e coerente di tutti i vari aspetti della criminalità informatica[5]. La Convenzione è stata firmata,

---

1 GU L 69 del 16.3.2005, pag. 68.

2 Relazione della Commissione al Consiglio ai sensi dell'articolo 12 della decisione quadro del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione (COM (2008) 448).

3 GU C 198 del 12.8.2005; GU C 115 del 4.5.2010; (COM (2010) 171) del 20.4.2010.

4 Comunicazione della Commissione (COM (2010) 245) del 19.5.2010.

5 Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 23.11.2001, STCE n. 185.

finora, da tutti e 27 gli Stati membri, ma solo 15 l'hanno ratificata[6]. È entrata in vigore il 1° luglio 2004. L'UE non ne è firmataria. Data l'importanza dello strumento, la Commissione incoraggia attivamente gli altri Stati membri dell'UE a ratificarlo al più presto.

- **Contesto generale**

La causa principale del fenomeno della criminalità informatica è la vulnerabilità, che a sua volta dipende da numerosi fattori. La risposta insufficiente dei meccanismi di contrasto contribuisce alla diffusione del fenomeno e la situazione si fa più complessa perché alcuni tipi di reato trascendono i confini nazionali. La segnalazione di questo tipo di reati è spesso insufficiente, in parte perché non tutte le violazioni vengono notate, in parte perché le vittime (operatori economici e imprese) non le segnalano per timore che, rendendo pubbliche le loro vulnerabilità, la loro reputazione e le loro future prospettive commerciali possano risultarne compromesse.

Inoltre, le differenze a livello di diritto e procedura penale nazionali danno luogo a indagini e procedimenti giudiziari diversi, portando a divergenze nel modo di trattare questi reati. Gli sviluppi delle tecnologie informatiche hanno esacerbato questi problemi perché hanno reso più semplice produrre e diffondere strumenti (malware e botnet), garantendo nel contempo l'anonimato agli autori del reato e creando confusione a livello di giurisdizione. Data la difficoltà nel promuovere l'azione penale contro questi reati, la criminalità organizzata può ottenere profitti consistenti con rischi minimi.

La presente proposta tiene conto dei nuovi metodi utilizzati per commettere reati informatici, specialmente l'uso delle botnet. Il termine "botnet" indica una rete di computer infettati da software maligni (virus informatici). Una tale rete di computer compromessi ("zombie") può essere attivata per eseguire azioni specifiche, ad esempio attacchi ai sistemi d'informazione (attacchi informatici). Questi "zombie" possono essere controllati – spesso ad insaputa dei loro utilizzatori – da un altro computer, noto anche come "centro di comando e di controllo". Le persone che controllano questo centro sono da annoverarsi fra gli autori del reato, poiché usano i computer compromessi per lanciare attacchi contro i sistemi di informazione. Rintracciare tali persone è molto difficile, poiché i computer che fanno parte della botnet e che effettuano gli attacchi possono trovarsi in un luogo diverso da quello in cui è localizzato l'autore del reato.

Gli attacchi lanciati da una botnet sono spesso eseguiti su larga scala: sono cioè effettuati con strumenti che colpiscono un gran numero di sistemi d'informazione (computer), oppure sono attacchi che causano danni ingenti, in termini ed esempio di perturbazione dei servizi di sistema, costi finanziari, perdita di dati personali, ecc. Il danno causato dagli attacchi su larga scala ha un impatto notevole sul funzionamento del bersaglio e/o colpisce anche il suo ambiente di lavoro. In tale contesto, si intende con "big botnet" una rete in grado di provocare danni gravi. È difficile definire le botnet in termini di dimensioni, ma si stima che le più grosse di cui si abbia testimonianza contino fra 40 000 e 100 000 connessioni (cioè computer infettati) per periodo di 24 ore[7].

---

6 Per un quadro generale delle ratifiche della Convenzione (STCE n. 185) si veda: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

7 Il numero di connessioni su 24 ore è l'unità di misura comunemente usata per stimare la dimensione delle botnet.

- **Disposizioni vigenti nel settore della proposta**

A livello UE, la decisione quadro introduce un livello minimo di ravvicinamento fra le legislazioni degli Stati membri per quanto riguarda la punibilità di una serie di atti di criminalità informatica, fra cui l'accesso illecito a sistemi di informazione, l'interferenza illecita per quanto riguarda i sistemi, l'interferenza illecita per quanto riguarda i dati, l'istigazione, il favoreggiamento, la complicità e il tentativo.

Benché le disposizioni della decisione quadro siano state, in generale, attuate dagli Stati membri, si riscontrano una serie di carenze dovute all'evoluzione, in dimensione e numero, dei reati (attacchi informatici). La decisione quadro ravvicina in effetti le legislazioni solo per quanto riguarda un numero limitato di reati, ma non affronta pienamente la potenziale minaccia rappresentata per la società dagli attacchi su larga scala, né la questione della gravità dei reati e delle sanzioni applicabili.

Altre iniziative e programmi dell'UE, esistenti o previsti, contribuiscono ad affrontare i problemi legati agli attacchi informatici o a questioni informatiche, quali la sicurezza delle reti e degli utilizzatori di Internet. Fra di essi si annoverano le azioni sostenute dai programmi "Prevenzione e lotta contro la criminalità"[8], "Giustizia penale"[9], "Internet più sicuro"[10] e dall'iniziativa relativa alle infrastrutture critiche informatizzate[11]. Oltre alla decisione quadro, un altro strumento giuridico rilevante in vigore è la decisione quadro 2004/68/GAI relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile.

A livello amministrativo, la pratica di infettare i computer per trasformarli in botnet è già vietata dalle norme UE in materia di privacy e protezione dei dati[12]. Organismi amministrativi nazionali, in particolare, stanno già collaborando nell'ambito della rete europea di contatto delle autorità antispam. In base a tali norme, gli Stati membri devono vietare l'intercettazione delle comunicazioni sulle reti pubbliche di comunicazione e i servizi di comunicazione elettronica di pubblico accesso senza il consenso degli utenti interessati o un'autorizzazione legale.

La presente proposta è conforme a tali norme. Occorre che gli Stati membri provvedano a migliorare la cooperazione fra le autorità amministrative e di contrasto per i casi passibili di sanzioni sia amministrative che penali.

- **Coerenza con gli altri obiettivi e politiche dell'Unione**

Gli obiettivi sono in linea con le politiche dell'UE volte a combattere la criminalità organizzata, ad aumentare la resilienza delle reti informatiche, a proteggere le infrastrutture di informazione critiche e a garantire la tutela dei dati. Sono inoltre coerenti con il programma "Internet più sicuro", creato per promuovere un uso senza rischi di Internet e delle nuove tecnologie on-line, e per combatterne i contenuti illegali.

---

8 Cfr.: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Cfr.: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Cfr.: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Cfr.: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Direttiva relativa alla vita privata e alle comunicazioni elettroniche (GU L 201 del 31.7.2002), modificata dalla direttiva 2009/136/CE (GU L 337 del 18.12.2009).

La presente proposta è stata oggetto di un esame approfondito per garantirne la piena compatibilità con i diritti fondamentali, specialmente la protezione dei dati personali, la libertà di espressione e d'informazione, il diritto a un giudice imparziale, la presunzione di innocenza e i diritti della difesa così come i principi della legalità e della proporzionalità dei reati e delle pene.

2. CONSULTAZIONE DELLE PARTI INTERESSATE E VALUTAZIONE D'IMPATTO

- **Consultazione delle parti interessate**

È stata consultata un'ampia gamma di esperti in una serie di diverse riunioni incentrate sui vari aspetti della lotta contro la criminalità informatica, compreso il seguito giudiziario (procedimenti). Si è trattato, in particolare, di rappresentanti dei governi degli Stati membri e del settore privato, di giudici e pubblici ministeri specializzati, organizzazioni internazionali, agenzie europee e organismi specializzati. Successivamente molti esperti ed organizzazioni hanno inviato contributi e fornito informazioni.

Gli elementi chiave scaturiti dalla consultazione sono:

– la necessità che l'UE intervenga in tale settore;

– la necessità di considerare reato certe forme di illecito non contemplate nella decisione quadro vigente, in particolare le nuove forme di attacchi informatici (botnet);

– la necessità di eliminare gli ostacoli allo svolgimento delle indagini e dei procedimenti giudiziari nei casi transfrontalieri.

Nella valutazione d'impatto si è tenuto conto dei contributi raccolti durante la consultazione.

Ricorso al parere di esperti

Conoscenze specializzate esterne sono state ottenute durante le varie riunioni con le parti interessate.

Valutazione d'impatto

Per raggiungere l'obiettivo sono state esaminate varie opzioni.

- Opzione (1): Status quo / Nessuna nuova azione dell'UE

Questa opzione implica che l'UE non prenda alcuna iniziativa supplementare per contrastare questo particolare tipo di criminalità informatica, cioè gli attacchi contro i sistemi d'informazione. Saranno portate avanti le azioni in corso, in particolare i programmi per il rafforzamento della protezione delle infrastrutture di informazione critiche e per il miglioramento della cooperazione fra il settore pubblico e quello privato contro la criminalità informatica.

- Opzione (2): Elaborazione di un programma per intensificare l'impegno a contrastare gli attacchi contro i sistemi di informazione per mezzo di misure non legislative

Parallelamente al programma di protezione delle infrastrutture di informazione critiche, le misure non legislative si concentrerebbero sulle attività di contrasto transfrontaliere e sulla cooperazione pubblico-privato. Questi strumenti non vincolanti sarebbero destinati a sostenere l'azione coordinata a livello UE, e comprenderebbero il rafforzamento dell'esistente rete 24/7 dei punti di contatto degli organi di contrasto, la creazione di una rete UE di punti di contatto pubblico-privati che riunisca esperti in materia di criminalità informatica e organi di contrasto, l'elaborazione di un accordo standard UE sul livello dei servizi per la cooperazione nelle attività di contrasto con gli operatori del settore privato, e il sostegno all'organizzazione di programmi di formazione per gli organi di contrasto sulle indagini sui reati informatici.

- Opzione (3): Aggiornamento mirato delle disposizioni della decisione quadro (nuova direttiva che la sostituisce) per affrontare la minaccia degli attacchi su larga scala contro i sistemi di informazione (botnet) e, quando perpetrati celando la reale identità dell'autore e arrecando pregiudizio al legittimo proprietario dell'identità, per rafforzare l'efficienza dei punti di contatto degli organi di contrasto nazionali, e per rimediare alla mancanza di dati statistici sugli attacchi informatici.

Questa opzione prevede l'introduzione di specifiche norme mirate (ossia circoscritte) per prevenire attacchi su larga scala contro i sistemi d'informazione. La normativa verrebbe affiancata da misure non legislative per rafforzare la cooperazione operativa transfrontaliera contro tali attacchi, cosa che faciliterebbe l'applicazione delle misure legislative. Scopo di queste misure sarebbe rafforzare la preparazione, la sicurezza e la resilienza delle infrastrutture di informazione critiche e lo scambio delle migliori prassi.

- Opzione (4): Introduzione di una legislazione UE generale contro la criminalità informatica

Questa opzione comporterebbe una nuova legislazione UE generale. Oltre all'adozione delle misure non vincolanti dell'opzione 2 e all'aggiornamento di cui all'opzione 3, questa soluzione affronterebbe altri problemi giuridici legati all'utilizzo di Internet. Tali misure riguarderebbero non solo gli attacchi contro i sistemi di informazione, ma anche questioni come la criminalità informatica finanziaria, i contenuti illegali di Internet, la raccolta/la conservazione/il trasferimento di prove elettroniche, e norme più dettagliate sulla competenza giurisdizionale. Tale legislazione funzionerebbe in parallelo con la Convenzione del Consiglio d'Europa sulla criminalità informatica, e includerebbe le misure di accompagnamento non legislative sopra menzionate.

- Opzione (5): Aggiornamento della Convenzione del Consiglio d'Europa sulla criminalità informatica

Questa opzione richiederebbe una sostanziale rinegoziazione dell'attuale Convenzione, processo lungo e incompatibile con la tabella di marcia proposta nella valutazione d'impatto. Non vi sembra essere del resto alcuna volontà internazionale di rinegoziare la Convenzione. L'aggiornamento della Convenzione non può quindi essere considerato un'opzione percorribile, poiché andrebbe oltre il termine d'azione previsto.

Opzione privilegiata: Combinazione di misure non legislative (opzione 2) con un aggiornamento mirato della decisione quadro (opzione 3)

Dall'analisi dell'incidenza economica e sociale e delle ripercussioni sui diritti fondamentali risulta che le opzioni 2 e 3 rappresentano il migliore approccio per affrontare il problema e realizzare gli obiettivi della proposta.

Nell'elaborare la presente proposta la Commissione ha effettuato una valutazione d'impatto.

3. ELEMENTI GIURIDICI DELLA PROPOSTA

- **Sintesi dell'azione proposta**

Pur abrogando la decisione quadro 2005/222/GAI, la direttiva ne manterrà le attuali disposizioni e includerà i nuovi elementi esposti in appresso.

– Per quanto riguarda, in generale, il diritto penale sostanziale, essa:

A. definisce come reato la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo di dispositivi/strumenti usati con l'intento di commettere i reati;

B. prevede circostanze aggravanti:

- il carattere su larga scala degli attacchi. Le botnet o strumenti simili sarebbero combattuti introducendo una nuova circostanza aggravante: il fatto di creare una botnet o uno strumento simile verrebbe a costituire un fattore aggravante nell'ambito della commissione dei reati elencati nell'attuale decisione quadro;

- il fatto di perpetrare tali attacchi celando la reale identità dell'autore e arrecando pregiudizio al legittimo proprietario dell'identità. Tutte queste disposizioni devono rispettare i principi della legalità e della proporzionalità dei reati e delle pene ed essere conformi alla legislazione esistente in materia di protezione dei dati personali[13];

C. introduce la fattispecie di reato di "intercettazione illecita";

D. introduce misure per migliorare la cooperazione giudiziaria in materia penale a livello europeo rafforzando l'esistente struttura dei punti di contatto 24/7[14]:

- è proposto l'obbligo, per i punti di contatto operativi (di cui all'articolo 14 della direttiva), di rispondere a una richiesta di assistenza entro un determinato limite di tempo. La Convenzione sulla criminalità informatica non prevede alcuna disposizione vincolante di questo tipo. Scopo di tale misura è garantire che i punti

---

[13] Come la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37) (attualmente in fase di revisione), e come la direttiva generale sulla protezione dei dati 95/46/CE.

[14] Introdotta dalla Convenzione, cfr. anche la decisione quadro 2005/222/GAI relativa agli attacchi contro i sistemi di informazione.

di contatto indichino entro un determinato lasso di tempo se sono in grado o meno di fornire una soluzione alla richiesta di assistenza, ed entro quando ritengono di poter trovare tale soluzione. L'effettivo contenuto della soluzione non è specificato;

E. risponde alla necessità di disporre di statistiche sulla criminalità informatica facendo obbligo agli Stati membri di predisporre un sistema adeguato di registrazione, produzione e fornitura di dati statistici sui reati contemplati dall'attuale decisione quadro e sul nuovo reato di "intercettazione illecita".

Nelle definizioni dei reati di cui agli articoli 3, 4 e 5 (accesso illecito a sistemi di informazione, interferenza illecita per quanto riguarda i sistemi e intercettazione illecita), la direttiva contiene una disposizione che permette, col recepimento della direttiva nel diritto nazionale, di perseguire penalmente solo i "casi gravi". Questo elemento di flessibilità è volto a consentire agli Stati membri di non includere casi che rientrerebbero *in abstracto* nella definizione di base, ma che si ritiene non pregiudichino l'interesse giuridico protetto, ad esempio atti commessi da giovani che cercano di dimostrare la loro abilità nelle tecnologie dell'informazione. Questa possibilità di limitare la portata dell'incriminazione non deve tuttavia condurre all'introduzione di altri elementi costitutivi dei reati oltre a quelli già previsti dalla direttiva, poiché ne conseguirebbe che sarebbero contemplati solo i reati commessi in circostanze aggravanti. Nel recepire la direttiva, gli Stati membri dovrebbero in particolare evitare di aggiungere altri elementi costitutivi ai reati di base, come ad esempio la particolare intenzione di ottenere proventi illeciti dal reato o l'esistenza di uno specifico effetto, ad esempio un danno considerevole.

- **Base giuridica**

Articolo 83, paragrafo 1, del trattato sul funzionamento dell'Unione europea[15].

- **Principio di sussidiarietà**

Alle azioni dell'Unione europea si applica il principio di sussidiarietà. Gli obiettivi della proposta non possono essere realizzati in misura sufficiente dagli Stati membri per i motivi di seguito indicati.

La criminalità informatica e, più specificamente, gli attacchi contro i sistemi di informazione, hanno una dimensione transfrontaliera considerevole, che appare tanto più chiara in caso di attacchi su larga scala, poiché gli elementi di connessione di un attacco si trovano spesso in luoghi ed in paesi diversi. È di conseguenza necessario un intervento a livello dell'UE, soprattutto per non farsi sopraffare dall'attuale tendenza a lanciare attacchi massicci in Europa e nel mondo. Un'azione a livello UE e un aggiornamento della decisione quadro 2005/222/GAI sono anche stati invocati nelle conclusioni del Consiglio del novembre 2008[16], poiché l'obiettivo di proteggere efficacemente i cittadini contro gli atti di criminalità informatica non può essere realizzato in misura sufficiente dagli Stati membri da soli.

Gli obiettivi della proposta possono essere realizzati più efficacemente a livello dell'Unione europea per i motivi di seguito esposti.

---

15 GU C 83 del 30.3.2010, pag. 49.

16 "Strategia di lavoro concertata e misure pratiche di lotta alla criminalità informatica", 2987° sessione del Consiglio "Giustizia e affari interni", Bruxelles, 27-28 novembre 2008.

La proposta ravvicinerà ulteriormente il diritto penale sostanziale degli Stati membri e le norme procedurali, con conseguente impatto positivo sulla lotta contro questi reati. Essa permetterà anzitutto di impedire agli autori dei reati di spostarsi in Stati membri in cui la legislazione contro gli attacchi informatici è più indulgente. In secondo luogo, avere definizioni comuni permette di scambiarsi informazioni e di raccogliere e raffrontare dati pertinenti. Ne risulterà poi rafforzata, in terzo luogo, l'efficacia delle misure di prevenzione in tutta Europa e la cooperazione internazionale.

La proposta è quindi conforme al principio di sussidiarietà.

- **Principio di proporzionalità**

La proposta è conforme al principio di proporzionalità per il motivo di seguito esposto.

La direttiva si limita a emanare le disposizioni minime per il conseguimento dei suoi obiettivi a livello europeo e non va al di là di quanto è necessario a tale scopo, tenendo conto dell'esigenza di accuratezza del diritto penale.

- **Scelta degli strumenti**

Strumento proposto: direttiva.

Altri mezzi non sarebbero adatti per il motivo esposto in appresso.

La base giuridica richiede una direttiva.

Le misure non legislative e l'autoregolamentazione migliorerebbero la situazione in alcuni settori in cui è fondamentale l'attuazione, ma i vantaggi sarebbero scarsi nei settori in cui è essenziale una nuova normativa.

4. INCIDENZA SUL BILANCIO

L'incidenza della proposta sul bilancio dell'Unione è lieve. Più del 90% del costo stimato di 5 913 000 euro verrebbe sostenuto dagli Stati membri, e vi è la possibilità di chiedere un finanziamento dell'UE ai fini della riduzione di tali spese.

5. INFORMAZIONI SUPPLEMENTARI

- **Abrogazione della normativa vigente**

L'adozione della proposta comporterà l'abrogazione della normativa vigente.

- **Applicazione territoriale**

Gli Stati membri sono destinatari della presente direttiva conformemente ai trattati.

2010/0273 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare

l'articolo 83, paragrafo 1,

vista la proposta della Commissione europea[17],

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo,

visto il parere del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) L'obiettivo della presente direttiva è ravvicinare le legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione e migliorare la cooperazione fra le autorità giudiziarie le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge.

(2) Gli attacchi ai danni dei sistemi di informazione, in particolare ad opera della criminalità organizzata, sono una minaccia crescente, e la preoccupazione per la possibilità di attacchi terroristici o di matrice politica contro sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri e dell'Unione è in aumento. Ciò costituisce una minaccia per la creazione di una società dell'informazione sicura e di uno spazio di libertà, sicurezza e giustizia, e richiede pertanto una risposta a livello di Unione europea.

(3) Si registra chiaramente una tendenza a perpetrare attacchi su larga scala sempre più pericolosi e ricorrenti contro sistemi di informazione critici per lo Stato o per particolari funzioni del settore pubblico o privato. Questa tendenza va di pari passo con lo sviluppo di strumenti sempre più sofisticati che possono essere usati dai criminali per lanciare attacchi informatici di vario tipo.

[17] GU C […] del […], pag. […].

(4) Per garantire un approccio coerente degli Stati membri nell'applicazione della presente direttiva è importante avere, in questo settore, definizioni comuni, in particolare quelle inerenti ai sistemi di informazione e ai dati informatici.

(5) È necessario giungere ad un approccio comune nei confronti degli elementi costitutivi dei reati mediante l'introduzione dei reati comuni di accesso illecito a sistemi di informazione, di interferenza illecita per quanto riguarda i sistemi, di interferenza illecita per quanto riguarda i dati, e di intercettazione illecita.

(6) È necessario che gli Stati membri prevedano sanzioni per gli attacchi ai danni di sistemi di informazione, e che le sanzioni previste siano efficaci, proporzionate e dissuasive.

(7) È opportuno prevedere sanzioni più severe quando un attacco contro un sistema di informazione è perpetrato da un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI del Consiglio, del 24 ottobre 2008, relativa alla lotta contro la criminalità organizzata[18], quando l'attacco è condotto su larga scala, o quando il reato è commesso celando la reale identità dell'autore e arrecando pregiudizio al legittimo proprietario dell'identità. È inoltre opportuno prevedere sanzioni più severe quando tale attacco ha provocato danni gravi o ha colpito interessi essenziali.

(8) Nelle sue conclusioni del 27-28 novembre 2008, il Consiglio ha invocato l'elaborazione di una nuova strategia con gli Stati membri e la Commissione, tenendo conto del contenuto della Convenzione del 2001 del Consiglio d'Europa sulla criminalità informatica. Tale Convenzione è il quadro giuridico di riferimento per la lotta contro la criminalità informatica, compresi gli attacchi contro i sistemi di informazione, e su di essa si basa la presente direttiva.

(9) Tenuto conto delle varie modalità con cui possono essere effettuati gli attacchi e della rapida evoluzione degli hardware e dei software, la presente direttiva fa riferimento a "strumenti" che possono essere utilizzati per commettere i reati in essa contemplati. Con "strumenti" si intendono ad esempio software maligni, fra cui le botnet, usati per perpetrare attacchi informatici.

(10) La presente direttiva non intende prevedere la responsabilità penale qualora gli atti ivi contemplati siano compiuti senza dolo, ad esempio per effettuare un collaudo autorizzato o proteggere un sistema informatico.

(11) La presente direttiva rafforza l'importanza delle reti, come la rete di punti di contatto del G8 o quella del Consiglio d'Europa, disponibili 24 ore su 24 e 7 giorni su 7 per lo scambio di informazioni allo scopo di assicurare un'assistenza immediata per le indagini o i procedimenti relativi a reati connessi a sistemi e dati informatici, o per la raccolta di prove in formato elettronico di un reato. Data la rapidità con cui possono essere lanciati gli attacchi su larga scala, occorre che gli Stati membri siano in grado di rispondere prontamente alle richieste urgenti provenienti da questa rete di punti di contatto. Tale assistenza deve consistere nel facilitare o nell'applicare direttamente misure come l'apporto di consigli tecnici, la conservazione dei dati, la raccolta di

[18] GU L 300 dell'11.11.2008, pag. 42.

prove, la trasmissione di informazioni di carattere giuridico e la localizzazione dei sospetti.

(12) È necessario raccogliere dati sui reati contemplati dalla presente direttiva per ottenere un quadro più completo del problema a livello dell'Unione e contribuire così alla formulazione di risposte più efficaci. Grazie ai dati raccolti, inoltre, agenzie specializzate come Europol e l'Agenzia europea per la sicurezza delle reti e dell'informazione potranno valutare meglio la portata della criminalità informatica e lo stato della sicurezza delle reti e dell'informazione in Europa.

(13) Le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri nel campo degli attacchi contro i sistemi di informazione possono ostacolare la lotta contro la criminalità organizzata ed il terrorismo e complicare un'efficace cooperazione di polizia e giudiziaria in questo settore. Il carattere transnazionale e senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi abbiano una dimensione transnazionale, e rende evidente la necessità di adottare urgentemente azioni ulteriori per il ravvicinamento delle legislazioni penali in questo settore. L'adozione della decisione quadro 2009/948/GAI del Consiglio sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali dovrebbe inoltre agevolare il coordinamento dell'azione penale nei casi di attacchi contro i sistemi di informazione.

(14) Poiché gli obiettivi della presente direttiva, vale a dire fare sì che gli attacchi ai danni di sistemi di informazione siano puniti in tutti gli Stati membri con sanzioni penali efficaci, proporzionate e dissuasive, e migliorare ed incoraggiare la cooperazione giudiziaria mediante la rimozione delle difficoltà potenziali, non possono essere conseguiti in misura sufficiente dagli Stati membri, in quanto le norme devono essere comuni e compatibili, e possono dunque essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi.

(15) Il trattamento di dati personali effettuato nel contesto dell'attuazione della presente direttiva deve essere conforme alle disposizioni della decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[19], per le attività di trattamento che rientrano nel suo campo d'applicazione, e del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati[20].

(16) La presente direttiva rispetta i diritti fondamentali ed osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea, inclusi la protezione dei dati personali, la libertà di espressione e d'informazione, il diritto a un giudice imparziale, la presunzione di innocenza e i diritti della difesa così come i principi della legalità e della proporzionalità dei reati e delle pene. In particolare, la

---

19 GU L 350 del 30.12.2008, pag. 60.

20 GU L 8 del 12.1.2001, pag. 1.

presente direttiva è volta a garantire il pieno rispetto di tali diritti e principi e deve essere attuata di conseguenza.

(17) [A norma degli articoli 1, 2, 3 e 4 del protocollo sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sul funzionamento dell'Unione europea, detti Stati membri hanno notificato che desiderano partecipare all'adozione e all'applicazione della presente direttiva] OPPURE [Fatto salvo l'articolo 4 del protocollo sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, il Regno Unito e l'Irlanda non partecipano all'adozione della presente direttiva, non sono da essa vincolati, né sono soggetti alla sua applicazione].

(18) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca, allegato al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione della presente direttiva, non è da essa vincolata, né è soggetta alla sua applicazione,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1
Oggetto

La presente direttiva introduce fattispecie di reato nel settore degli attacchi contro i sistemi di informazione e stabilisce norme minime per le relative sanzioni. Essa mira altresì a introdurre disposizioni comuni per impedire tali attacchi e migliorare la cooperazione giudiziaria penale europea in questo campo.

Articolo 2
Definizioni

Ai fini della presente direttiva si applicano le seguenti definizioni:

(a) per "sistema di informazione" si intende qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione;

(b) per "dati informatici" s’intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata da un sistema di informazione, compreso un programma atto a far svolgere una funzione ad un sistema di informazione;

(c) per "persona giuridica" s’intende qualsiasi entità che sia tale in forza del diritto applicabile, ad eccezione degli Stati o di altre istituzioni pubbliche nell’esercizio dei pubblici poteri e delle organizzazioni internazionali pubbliche;

(d) l’espressione "senza diritto" significa l’accesso o l’interferenza non autorizzati da parte di chi ha il diritto di proprietà o altro diritto sul sistema o una sua parte, ovvero non consentiti ai sensi della legislazione nazionale.

Articolo 3

Accesso illecito a sistemi di informazione

Gli Stati membri adottano le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato, almeno per i casi gravi.

Articolo 4

Interferenza illecita per quanto riguarda i sistemi

Gli Stati membri adottano le misure necessarie affinché l'atto intenzionale di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili sia punito come reato se compiuto senza diritto, almeno per i casi gravi.

Articolo 5

Interferenza illecita per quanto riguarda i dati

Gli Stati membri adottano le misure necessarie affinché l'atto intenzionale di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione sia punito come reato se compiuto senza diritto, almeno per i casi gravi.

Articolo 6

Intercettazione illecita

Gli Stati membri adottano le misure necessarie affinché l'intercettazione intenzionale, tramite strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che ha tali dati informatici, sia punita come reato se compiuta senza diritto.

Articolo 7

Strumenti utilizzati per commettere i reati

Gli Stati membri adottano le misure necessarie affinché siano puniti come reato, se compiuti intenzionalmente e senza diritto con l'intento di perpetrare uno dei reati di cui agli articoli da 3 a 6, la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, il possesso, la distribuzione o la messa a disposizione in altro modo dei seguenti strumenti:

a) un dispositivo, incluso un programma per computer, destinato o utilizzato principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6;

b) una password di un computer, un codice d'accesso, o informazioni simili che permettono di accedere in tutto o in parte a un sistema di informazione.

Articolo 8

Istigazione, favoreggiamento, complicità e tentativo

1. Gli Stati membri provvedono a che l'istigazione, il favoreggiamento e la complicità in ordine alla commissione dei reati di cui agli articoli da 3 a 7 siano punibili come reati.

2. Gli Stati membri provvedono a che il tentativo di commettere i reati di cui agli articoli da 3 a 6 sia punibile come reato.

Articolo 9

Sanzioni

1. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 8 siano punibili con sanzioni efficaci, proporzionate e dissuasive.

2. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 7 siano punibili con pene detentive non inferiori nel massimo ad anni due.

Articolo 10

Circostanze aggravanti

1. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 7 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora siano stati commessi nell'ambito di un'organizzazione criminale come definita nella decisione quadro 2008/841/GAI.

2. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 6 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora siano stati commessi con strumenti concepiti per lanciare attacchi contro un gran numero di sistemi d'informazione o attacchi che causano danni ingenti, come perturbazioni dei servizi di sistema, costi finanziari o perdita di dati personali.

3. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 6 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora siano stati commessi celando la reale identità dell'autore e arrecando pregiudizio al legittimo proprietario dell'identità.

Articolo 11

Responsabilità delle persone giuridiche

1. Gli Stati membri adottano le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli da 3 a 8 commessi a loro beneficio da qualsiasi soggetto, che agisca a titolo individuale o in quanto membro di un organo della persona giuridica, e che detenga una posizione preminente in seno alla persona giuridica stessa, basata:

(a) sul potere di rappresentanza di detta persona giuridica;

(b) sul potere di prendere decisioni per conto della persona giuridica;

(c) sull'esercizio di poteri di controllo in seno a tale persona giuridica.

2. Gli Stati membri adottano le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di uno dei soggetti di cui al paragrafo 1 abbia reso possibile la commissione, a vantaggio della persona giuridica, di uno dei reati di cui agli articoli da 3 a 8 da parte di una persona sottoposta all'autorità di tale soggetto.

3. La responsabilità delle persone giuridiche ai sensi dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori o complici di uno dei reati di cui agli articoli da 3 a 8.

Articolo 12
Sanzioni applicabili alle persone giuridiche

1. Gli Stati membri adottano le misure necessarie affinché alla persona giuridica ritenuta responsabile ai sensi dell'articolo 11, paragrafo 1, siano applicabili sanzioni efficaci, proporzionate e dissuasive, che comprendano sanzioni pecuniarie penali o non penali e che possano comprendere anche altre sanzioni quali:

   (a) misure di esclusione dal godimento di un beneficio o aiuto pubblico;

   (b) misure di divieto temporaneo o permanente di esercitare attività commerciali;

   (c) assoggettamento a sorveglianza giudiziaria;

   (d) provvedimenti giudiziari di scioglimento;

   (e) chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato.

2. Gli Stati membri adottano le misure necessarie affinché alla persona giuridica ritenuta responsabile ai sensi dell'articolo 11, paragrafo 2, siano applicabili sanzioni o provvedimenti efficaci, proporzionati e dissuasivi.

Articolo 13
Competenza giurisdizionale

1. Gli Stati membri stabiliscono la propria competenza giurisdizionale in ordine ai reati di cui agli articoli da 3 a 8 laddove i reati siano stati commessi:

   (a) interamente o in parte sul territorio dello Stato membro interessato, oppure

   (b) da un loro cittadino o da una persona che risiede abitualmente nel territorio dello Stato membro interessato, oppure

   (c) a beneficio di una persona giuridica che ha la sede legale nel territorio dello Stato membro interessato.

2. Nello stabilire la propria competenza giurisdizionale ai sensi del paragrafo 1, lettera a), gli Stati membri provvedono a che tale giurisdizione abbracci i casi in cui:

(a) l'autore abbia commesso il reato mentre era fisicamente presente nel territorio dello Stato membro interessato, indipendentemente dal fatto che il sistema di informazione contro il quale è stato commesso il reato si trovi o meno nel suo territorio, oppure

(b) il reato sia stato commesso ai danni di un sistema di informazione che si trova nel territorio dello Stato membro interessato, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.

Articolo 14
Scambio di informazioni

1. Per lo scambio delle informazioni relative ai reati di cui agli articoli da 3 a 8, fatte salve le disposizioni sulla protezione dei dati, gli Stati membri si servono della rete esistente di punti di contatto operativi 24 ore su 24 e 7 giorni su 7. Gli Stati membri provvedono inoltre a predisporre procedure per rispondere entro un massimo di otto ore alle richieste urgenti. La risposta deve almeno indicare se, in che forma e quando sarà soddisfatta la richiesta di aiuto.

2. Gli Stati membri informano la Commissione in merito al proprio punto di contatto operativo stabilito per lo scambio d'informazioni sui reati di cui agli articoli da 3 a 8. La Commissione trasmette tali informazioni agli altri Stati membri.

Articolo 15
Monitoraggio e statistiche

1. Gli Stati membri provvedono a predisporre un sistema di registrazione, produzione e fornitura di dati statistici sui reati di cui agli articoli da 3 a 8.

2. I dati statistici di cui al paragrafo 1 riguardano come minimo il numero dei reati di cui agli articoli da 3 a 8 segnalati agli Stati membri e il seguito dato a tali segnalazioni, e indicano, su base annuale, il numero dei casi segnalati che sono stati oggetto di indagine, il numero di persone che sono state oggetto di un procedimento giudiziario, e il numero di persone condannate per i reati contemplati dagli articoli da 3 a 8.

3. Gli Stati membri trasmettono alla Commissione i dati raccolti ai sensi del presente articolo. Provvedono inoltre alla pubblicazione di una revisione consolidata di queste relazioni statistiche.

Articolo 16
Abrogazione della decisione quadro 2005/222/GAI

La decisione quadro 2005/222/GAI è abrogata, fatti salvi gli obblighi degli Stati membri relativi ai termini per il recepimento nel diritto nazionale.

I riferimenti alla decisione quadro abrogata si intendono fatti alla presente direttiva.

Articolo 17
Recepimento

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro [due anni dall'adozione]. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni nonché una tavola di concordanza tra queste ultime e la presente direttiva. Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni essenziali di diritto interno adottate nella materia disciplinata dalla presente direttiva.

Articolo 18
Relazioni

1. Entro [QUATTRO ANNI DALL'ADOZIONE], e successivamente ogni tre anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione della presente direttiva negli Stati membri, corredata delle opportune proposte.

2. Gli Stati membri trasmettono alla Commissione ogni informazione utile ai fini della relazione di cui al paragrafo 1. Tali informazioni comprendono una descrizione dettagliata delle misure legislative e non legislative adottate per l'attuazione della presente direttiva.

Articolo 19
Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 20
Destinatari

Gli Stati membri sono destinatari della presente direttiva conformemente ai trattati.

Fatto a Bruxelles,

Per il Parlamento europeo
Il Presidente

Per il Consiglio
Il Presidente