CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 30 maggio 2011 (06.06)
(OR. en)

10751/11

Fascicolo interistituzionale: 2010/0273(COD)

DROIPEN 47
TELECOM 82
CODEC 915

NOTA

della:	presidenza
al:	COREPER/Consiglio
n. doc. prec.:	10357/11 DROIPEN 42 TELECOM 74 CODEC 851
Oggetto:	Proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI del Consiglio - Impostazione generale

I. INFORMAZIONI GENERALI

Il 30 settembre 2010 la Commissione ha presentato al Parlamento europeo e al Consiglio una 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.

In conformità dell'articolo 3, paragrafo 1 del protocollo (n. 21) dei trattati, sia il Regno Unito che l'Irlanda hanno notificato al Consiglio che desiderano partecipare all'adozione ed applicazione della direttiva. La Danimarca non partecipa all'adozione del suddetto strumento in conformità del protocollo (n. 22) dei trattati.

UK e FR hanno formulato una riserva d'esame parlamentare. DE, SI, FR e SE hanno espresso una riserva generale di esame sulla proposta.

La proposta è stata presentata al Consiglio nella sessione dell'8-9 novembre 2010.

In tre occasioni è stato chiesto al CATS di fornire orientamenti strategici per i lavori in sede di Gruppo "Diritto penale sostanziale" (di seguito DROIPEN). Il 13 dicembre 2010, all'inizio dei negoziati, il CATS ha fornito orientamenti generali per il futuro dibattito. L'11 febbraio 2011 il CATS ha preso in esame l'articolo 10, paragrafo 3 della proposta della Commissione, che introduce una nuova circostanza aggravante: gli attacchi informatici perpetrati abusando dei dati anagrafici del legittimo proprietario dell'identità. Il 22 marzo, infine, il CATS è stato consultato su quattro questioni in sospeso: la portata delle disposizioni, ad esclusione dei casi di minore gravità, gli elementi costitutivi del reato di cui all'articolo 3, l'entità delle sanzioni e la competenza giurisdizionale basata sulla cittadinanza.

Il gruppo DROIPEN ha discusso la proposta nelle riunioni del 13-14 e 28 gennaio 2011, nonché nelle riunioni del 2-3 e 29 marzo 2011. In quest'ultima riunione il gruppo DROIPEN ha portato a termine la terza lettura del testo.

Il Consiglio ha preso atto dello stato dei lavori in data 25 febbraio 2011. Il 12 aprile 2011 il Consiglio ha preso atto dell'accordo provvisorio raggiunto sugli articoli da 1 a 6 e sugli articoli da 11 a 19 del progetto di direttiva. Esso ha inoltre fornito orientamenti su varie questioni in sospeso, definendo in tal modo il quadro politico in cui sono stati portati avanti i lavori sulla proposta nell'ambito degli organi preparatori del Consiglio.

II. PROPOSTA DI PACCHETTO DI COMPROMESSO

Il testo di cui all'allegato costituisce una proposta di compromesso, come emerge dalla riunione dei consiglieri GAI del 13 maggio 2011 e dalla riunione del Gruppo degli Amici della Presidenza del 24 maggio 2011.

Nel corso delle varie discussioni la proposta iniziale della Commissione è stata modificata varie volte per tener conto il più possibile delle posizioni espresse dalle delegazioni. La presidenza ha inoltre pensato di mantenere un equilibrio con le ragioni intrinseche su cui si fonda la proposta della Commissione, segnatamente per dare, a livello dell'UE, una risposta più efficace in materia di diritto penale alle nuove minacce poste dalla cibercriminalità, quali gli attacchi informatici su larga scala.

A. A tale riguardo, la presidenza desidera rammentare gli elementi principali del pacchetto di compromesso, che erano stati provvisoriamente approvati dal Consiglio nella sua riunione del 12 aprile 2011.

1. Portata dell'incriminazione (articoli da 3 a 7)

- Il riferimento ai "casi di minore gravità" è stato esteso a tutti i reati contemplati dalla direttiva (articoli da 3 a 7). I casi di minore gravità sono pertanto totalmente esclusi dal campo di applicazione della direttiva. La definizione di ciò che costituisce un caso di minore gravità è determinata dal diritto interno e dalla prassi nazionale (cfr. considerando 6 bis); a tal fine sono altresì forniti degli esempi .
- Il campo di applicazione dell'articolo 3, "Accesso illecito a sistemi di informazione", è stato limitato ai casi in cui la violazione di una misura di sicurezza è un elemento costitutivo del reato. Tale possibilità è offerta, come opzione, dalla convenzione di Budapest ma non era stata inclusa nella proposta originaria della Commissione.
- Il possesso degli strumenti utilizzati per commettere attacchi informatici è stato escluso dal campo di applicazione dell'articolo 7.
- L'incriminazione del tentativo è stata limitata ai reati di cui agli articoli 4 e 5.

2. Sanzioni (articolo 9)

- La proposta della Commissione per quanto attiene al livello delle sanzioni per i reati di base (cfr. articolo 9, paragrafo 2), cioè pene detentive non inferiori nel massimo ad anni due, è stata mantenuta. Ciò è giustificato in particolare dalla portata limitata dell'incriminazione risultante dai lavori in seno agli organi preparatori del Consiglio. La portata della disposizione è stata ulteriormente limitata agli articoli da 3 a 6, escludendo così l'articolo 7 dall'obbligo di prevedere tale livello di sanzione specifico.
- La proposta di compromesso presenta più flessibilità per quanto concerne le sanzioni per le circostanze aggravanti: una pena detentiva massima non inferiore ad anni tre e ad anni cinque (articolo 9, paragrafi 3 e 4 rispettivamente) per tener conto della gravità dei reati, qualora l'applicazione delle disposizioni sia stata limitata a titolo di compromesso anche agli articoli 4 e 5.

3. Competenza giurisdizionale (articolo 13)

- Il fatto che sia istituita una competenza giurisdizionale in relazione alla cittadinanza si ricollega a un positivo controllo della doppia punibilità (articolo 13, paragrafo 1, lettera b)).
- Le condizioni di esercizio della competenza nazionale non sono soggette alle disposizioni della direttiva (cfr. preambolo, considerando 10 bis).

4. Scambio d'informazioni riguardo ai reati contemplati dal progetto di direttiva (articolo 14)

- È mantenuto il termine di 8 ore per rispondere a richieste urgenti, mentre il testo è stato modificato per precisare la natura dell'obbligo dello Stato richiesto, cioè che entro il limite di tempo previsto l'autorità competente risponde almeno circa la sua capacità di fornire riscontri e, in caso affermativo, specificare alcune modalità provvisorie della risposta prevista, quali la forma o l'orario presunto.

B. I lavori sulla proposta sono proseguiti alla luce dagli orientamenti politici forniti dal Consiglio in data 12 aprile 2011. Di conseguenza, il pacchetto di compromesso globale dovrebbe tenere conto anche dei seguenti nuovi elementi:

1. Strumenti utilizzati per commettere i reati - Articolo 7

- La portata dell'articolo 7 è stata ulteriormente limitata. Di conseguenza, sono state escluse dal campo di applicazione della proposta anche la fabbricazione o la messa a disposizione degli apparecchi che potrebbero essere usati per lanciare attacchi informatici.
- La direttiva si applica ad una nozione ristretta di "strumento", di cui all'articolo 7, contrariamente alla proposta della Commissione, basata su una più ampia interpretazione di tale nozione, che includeva ad esempio un hardware speciale come strumento per perpetrare attacchi informatici.

2. Circostanze aggravanti in relazione agli attacchi informatici su larga scala - Articolo 9

- L'elemento centrale della proposta della Commissione, riguardante gli attacchi informatici su larga scala in quanto circostanza aggravante, è stato mantenuto, anche se sostanzialmente modificato. Occorre sottolineare che vi sono due aspetti distintivi alternativi per gli attacchi informatici su larga scala, che sono o attacchi diretti a un gran numero di sistemi informatici, oppure attacchi che provocano danni gravi. Questi due aspetti sono trattati nell'articolo 9, paragrafo 3 e paragrafo 4, lettera b) rispettivamente.

- Per fugare i dubbi espressi da varie delegazioni sulla necessità di stabilire un nesso preciso con le attuali minacce poste da alcuni metodi usati dai criminali per lanciare attacchi informatici su larga scala, come la creazione e l'uso di "botnet" [1] , la relativa formulazione è stata inserita nei considerando della proposta (cfr. considerando 3 e 7). La presidenza ha scelto questo approccio, che consente, nella parte operativa della direttiva, di mantenere la flessibilità e la neutralità tecnica, nella misura in cui si tratta dei metodi usati per perpetrare attacchi informatici su larga scala. Tale approccio riveste una particolare rilevanza per le tecnologie in costante sviluppo e la natura in continua evoluzione di questo tipo di reato.

- A titolo di compromesso, è stato soppresso l'articolo 9, paragrafo 5 riguardante l'abuso dei dati personali altrui al fine di ottenere la fiducia di terzi per facilitare l'esecuzione dell'attacco informatico. Ciò è stato determinato dalle opinioni ripetutamente espresse da alcune delegazioni secondo le quali si tratta di un fenomeno che dovrebbe essere affrontato globalmente in uno specifico strumento inteso a lottare contro l'usurpazione d'identità.

[1] L'uso delle cosiddette "botnet" è caratterizzato da stadi susseguenti del reato, in cui ciascuno stadio singolarmente può mettere in grave pericolo i pubblici interessi. A tale riguardo, la direttiva mira, tra l'altro, a introdurre sanzioni penali per lo stadio in cui avviene la creazione della "botnet", ossia lo stadio in cui si stabilisce il controllo a distanza di un numero rilevante di computer infettandoli con software maligni per mezzo di attacchi informatici mirati. In una fase successiva, i computer infettati che costituiscono la "botnet" potrebbero essere attivati a insaputa degli utenti per lanciare attacchi informatici su larga scala, che, solitamente, sono in grado di causare danni gravi.

3. Competenza giurisdizionale (considerando 10 bis)

- La formulazione riveduta del considerando 10 bis ha introdotto una chiara distinzione tra le condizioni di fissazione della competenza giurisdizionale, definite all'articolo 13, e le condizioni per esercitarla.

Si invita il COREPER
a/ a considerare i nuovi elementi del compromesso come parte integrante di una proposta di pacchetto di compromesso globale e
b/ a confermare che il testo, riportato nell'allegato, dovrebbe essere sottoposto al Consiglio,in vista di un approccio globale sulla proposta, affinché il testo allegato costituisca la base dei futuri lavori con il Parlamento europeo conformemente all'articolo 294 del TFUE.

_____

ALLEGATO

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[2],
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, stabilendo norme minime relative alla definizione dei reati e delle sanzioni in tale settore, e migliorare la cooperazione fra le 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.

[2] GU C […] del […], pag. […].

(2 bis) Vi sono nell'Unione infrastrutture critiche la cui distruzione o il cui danneggiamento avrebbe un significativo impatto transfrontaliero. Dalla necessità di rafforzare la capacità di protezione delle infrastrutture critiche in Europa risulta evidente che la lotta agli attacchi contro i sistemi di informazione dovrebbe essere integrata con gravi sanzioni penali che rispecchino la gravità di tali attacchi. Per infrastruttura critica si può intendere un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni.

(3) Si registra chiaramente una tendenza a perpetrare attacchi su larga scala sempre più pericolosi e ricorrenti contro sistemi di informazione che possono essere spesso critici per lo Stato o per particolari funzioni del settore pubblico o privato. Questa tendenza va di pari passo con lo sviluppo di metodi sempre più sofisticati (…), quali la creazione e l'uso delle cosiddette "botnet". Essa è caratterizzato da stadi susseguenti del reato, in cui ciascuno stadio singolarmente può mettere in grave pericolo i pubblici interessi. A tale riguardo, la direttiva mira, tra l'altro, a introdurre sanzioni penali per lo stadio in cui avviene la creazione della "botnet", ossia lo stadio in cui si stabilisce il controllo a distanza di un numero rilevante di computer infettandoli con software maligni per mezzo di attacchi informatici mirati. In una fase successiva, la rete infettata di computer che costituiscono la "botnet" potrebbe essere attivata a insaputa degli utenti per lanciare attacchi informatici su larga scala, che, solitamente, sono in grado di causare danni gravi, ai sensi della presente direttiva. Gli Stati membri possono stabilire cosa costituisce danno grave ai sensi del loro diritto interno e della prassi nazionale, comprese eventualmente perturbazioni dei servizi di sistema di rilevante interesse pubblico, ovvero costi finanziari esorbitanti o perdita di dati personali.

(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, Le sanzioni dovrebbero essere efficaci, proporzionate e dissuasive.

(6 bis) La direttiva prevede sanzioni penali almeno nei casi gravi. Gli Stati membri possono stabilire cosa costituisce un caso di minore gravità ai sensi del loro diritto interno e della prassi nazionale. Un caso può essere considerato di minore gravità, ad esempio, quando il danno e/o il rischio che arreca a interessi pubblici o privati, quali l'integrità di un sistema informatico o di dati informatici o all'integrità di una persona, ai diritti o ad altri interessi è insignificante o di natura tale da non rendere necessario imporre una sanzione penale entro i limiti di legge né prevedere la responsabilità penale.

(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 [3] , o quando l'attacco è condotto su larga scala, colpendo così un gran numero di sistemi di informazione o causando danni gravi, anche quando l'attacco era inteso a creare una "botnet" o è stato perpetrato attraverso una "botnet", determinando in tal modo danni gravi (…).

(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 quelli capaci di creare botnet, usati per perpetrare attacchi informatici. Dal momento che la presente direttiva stabilisce norme minime, gli Stati membri possono prevedere sanzioni penali per altri tipi di reati in relazione agli strumenti usati per compiere reati, quali il possesso di siffatti strumenti oppure la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o

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

la messa a disposizione in altro modo di qualunque altro dispositivo, compreso il hardware destinato o utilizzato principalmente al fine di commettere uno dei reati di cui alla presente direttiva.

(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, o quando la persona in questione non sapeva che l'accesso non fosse autorizzato.

(10 bis) La presente direttiva non regola le condizioni da soddisfare per (…) esercitare la competenza giurisdizionale su uno dei reati di cui agli articoli da 3 a 8, quali una querela della vittima nel luogo in cui il reato è stato commesso o una segnalazione dello Stato in cui è stato commesso, o il fatto che l'autore non sia stato perseguito nel luogo in cui è stato commesso il reato.

(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 la comunicazione delle informazioni disponibili pertinenti per le indagini o i procedimenti relativi a reati connessi a sistemi e dati informatici che coinvolgono lo Stato membro richiedente.
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. In casi siffatti può essere opportuno che la richiesta di informazioni sia accompagnata da un contatto telefonico, per garantirne la rapida evasione da parte dello Stato richiesto, e che i riscontri siano forniti entro un termine di 8 ore, accusando ricevuta delle richieste e indicando se e quando la risposta sarà probabilmente fornita.

(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 non va al di là di quanto è necessario per il raggiungimento di tale obiettivo.

(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[4], 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[5].

---

[4] GU L 350 del 30.12.2008, pag. 60.
[5] GU L 8 del 12.1.2001, pag. 1.

(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 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 (…) 3 (…) 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, il Regno Unito e l'Irlanda hanno notificato che desiderano partecipare all'adozione ed applicazione della presente direttiva.

(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 e non è da essa vincolata, né è soggetta alla sua applicazione,

(19) La presente direttiva mira a modificare e ampliare le disposizioni della decisione quadro 2005/222/GAI. Poiché le modifiche da apportare sono numerose e sostanziali, è opportuno, per motivi di chiarezza, che la decisione quadro sia integralmente sostituita in relazione agli Stati membri che partecipano all'adozione della direttiva.

(20) Conformemente al punto 34 dell'accordo interistituzionale "Legiferare meglio"[6], gli Stati membri sono incoraggiati a redigere e rendere pubblici, nell'interesse proprio e dell'Unione, prospetti indicanti, per quanto possibile, la concordanza tra la presente direttiva e i provvedimenti di attuazione.

[6] GU C 321 del 31.12.2003, pag. 1.

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Oggetto

La presente direttiva stabilisce norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione. Mira inoltre a facilitare la prevenzione di tali reati e a migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti.

Articolo 2

Definizioni

Ai fini della presente direttiva s'intende per:

a) "sistema di informazione" 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) "dati informatici" 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) "persona giuridica" qualsiasi entità che abbia tale qualifica ai sensi della legislazione applicabile, eccetto gli Stati o altri organismi pubblici nell'esercizio dell'autorità statale e le organizzazioni internazionali;

d) l'espressione "senza diritto" significa l'accesso, l'interferenza, l'intercettazione o qualsiasi altro comportamento di cui alla presente direttiva 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 senza diritto ad un sistema di informazione o ad una parte dello stesso, se intenzionale, sia punito come reato, almeno quando si tratta di un reato commesso in violazione di una misura di sicurezza e 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, 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 intenzionalmente e senza diritto, almeno per i casi gravi.

Articolo 7

Strumenti utilizzati per commettere i reati

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

a) 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, complicità e tentativo

1. Gli Stati membri provvedono a che l'istigazione 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 un reato di cui agli articoli da 4 a 5 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 6 siano punibili con pene detentive non inferiori nel massimo ad anni due.

3. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli 4 e 5, se perpetrati intenzionalmente, siano punibili con pene detentive non inferiori nel massimo ad anni tre, (…) se un gran numero di sistemi di informazione (…) è stato colpito con uno degli strumenti di cui all'articolo 7, paragrafo 1, destinato o utilizzato principalmente a tal fine [7] .

4. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli 4 e 5 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora:

a) siano commessi nell'ambito di un'organizzazione criminale quale definita nella decisione quadro 2008/814/GAI indipendentemente dal livello delle sanzioni ivi previsto, o

b) causino danni gravi, [8] o

c) siano commessi ai danni di un sistema di informazione relativo a infrastrutture critiche.

(…)

[…]

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;

---

7 FR, ES e EE hanno formulato una riserva d'esame. LV non ha potuto appoggiare tale proposta.

8 RO ha formulato una riserva d'esame sull'articolo 9, paragrafo 4, lettera b).

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) interdizione temporanea o permanente di esercitare un'attività commerciale;
   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[9]

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, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso.

2. Nello stabilire la propria competenza giurisdizionale ai sensi del paragrafo 1, lettera a), ciascuno Stato membro provvede 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.

3. Ciascuno Stato membro informa la Commissione della decisione di stabilire la propria giurisdizione anche per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, per esempio nei seguenti casi:

   a) l'autore del reato risiede abitualmente nel suo territorio, oppure

   b) il reato è stato commesso a vantaggio di una persona giuridica che ha sede nel suo territorio.

---

9 UK mantiene una riserva d'esame su tale articolo.

Articolo 14

Scambio di informazioni[10]

1. Per lo scambio delle informazioni relative ai reati di cui agli articoli da 3 a 8, 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 tali da consentire loro di indicare entro un massimo di otto ore, in caso di richieste urgenti, se la richiesta di aiuto sarà soddisfatta, in che forma e prevedibilmente quando.

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 ne informa gli altri Stati membri.

Articolo 15

Monitoraggio e statistiche[11]

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 7.

2. I dati statistici di cui al paragrafo 1 riguardano come minimo i dati esistenti sul numero dei reati di cui agli articoli da 3 a 7 registrati dagli Stati membri e il numero di persone che sono state oggetto di un procedimento giudiziario e che sono state condannate per i reati contemplati dagli articoli da 3 a 7.

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

---

10 Riserva d'esame formulata da ES.

11 Riserva d'esame di ES.

Articolo 16

Sostituzione della decisione quadro 2005/222/GAI[12]

La decisione quadro 2005/222/GAI è sostituita dalla presente direttiva per gli Stati membri che partecipano all'adozione della direttiva stessa, fatti salvi gli obblighi degli Stati membri relativi al termine per il recepimento della decisione quadro nel diritto nazionale.

Per gli Stati membri che partecipano all'adozione della presente direttiva i riferimenti alla decisione 2005/222/GAI 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].

2. Gli Stati membri trasmettono alla Commissione il testo delle disposizioni inerenti al recepimento nella legislazione nazionale degli obblighi imposti dalla presente direttiva.

3. 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 di tale riferimento sono decise dagli Stati membri.

Articolo 18

Relazione

1. Entro [QUATTRO ANNI DALL'ADOZIONE], la Commissione presenta al Parlamento europeo e al Consiglio una relazione che valuti in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla presente direttiva, corredata, se del caso, di proposte legislative.

(…)

[12] UK mantiene riserve d'esame.

Articolo 19

Entrata in vigore

La presente direttiva entra in vigore il giorno della 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	*Per il Consiglio*
Il Presidente	*Il Presidente*