



**CONSIGLIO
DELL'UNIONE EUROPEA**

**Bruxelles, 8 aprile 2011
(OR. en)**

8795/11

**Fascicolo interistituzionale:
2010/0273(COD)**

**DROIPEN 27
TELECOM 43
CODEC 609**

NOTA

della:	presidenza
al:	Consiglio
n. doc. prec.:	8508/11 DROIPEN 24 TELECOM 39 CODEC 561
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 - dibattito orientativo e situazione dei lavori

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 ha 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 Gruppo per le questioni generali, valutazione compresa (GENVAL), il 13 ottobre 2010, e al Consiglio nella sessione dell'8-9 novembre 2010. Il Consiglio ha preso atto dello stato dei lavori in data 25 febbraio 2011.

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, sono state affrontate alcune questioni di ordine generale. 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 riguardanti i casi di minore gravità, la portata dell'incriminazione prevista 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 e del 2-3 e 29 marzo 2011: in quest'ultima occasione il gruppo DROIPEN ha portato a termine la terza lettura del testo ed ha esaminato le proposte redazionali suggerite dalla presidenza per far avanzare i lavori.

Il 4 aprile 2011 la proposta è stata ulteriormente esaminata dai Consiglieri GAI.

II. PUNTI RELATIVAMENTE AI QUALI I MINISTRI SONO INVITATI A FORNIRE UN ORIENTAMENTO POLITICO

Nel corso delle varie discussioni sono state apportate varie modifiche alla proposta iniziale della Commissione per tener conto il più possibile delle preoccupazioni espresse dalle delegazioni. La presidenza ha inoltre preso atto delle posizioni delle delegazioni favorevoli a mantenere un certo livello di ambizione nel testo. Secondo la presidenza è emersa la possibilità di un compromesso e a tal fine la proposta è stata presentata al COREPER il 7 aprile 2011 (allegato I).

Le discussioni in seno al COREPER hanno tuttavia messo in evidenza che esistono alcune questioni politiche che richiederebbero ulteriori orientamenti da parte del Consiglio onde poter definire il quadro politico nel quale il gruppo proseguirà le sue deliberazioni. Al riguardo la presidenza desidera sottoporre all'attenzione del Consiglio i punti seguenti :

1. Livello delle sanzioni (articolo 9, paragrafo 2) in relazione alla portata dell'incriminazione (articoli da 3 a 7)

Rispetto alla proposta iniziale della Commissione sono stati introdotti, in seguito ai lavori del gruppo, alcuni importanti compromessi che incidono sulla portata dell'incriminazione. Le seguenti modifiche sono intese a venire incontro a preoccupazioni specifiche di alcuni Stati membri:

- 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.
- 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 gli attacchi informatici è stato escluso dal campo di applicazione dell'articolo 7.

Secondo la presidenza, questa portata limitata dell'incriminazione giustifica il mantenimento della proposta iniziale della Commissione in relazione al livello delle sanzioni per i reati di base (cfr. articolo 9, paragrafo 2), cioè pene detentive non inferiori nel massimo a due anni. Va inoltre rilevato che 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.

Vi è tuttavia un gruppo di Stati membri che continua ad opporsi a questa soluzione, sostenendo che il livello della sanzione dovrebbe essere ridotto a un anno. In alternativa alla sanzione di un anno, questo obiettivo potrebbe anche essere conseguito mantenendo la soluzione prevista nella decisione quadro 2005/222/GAI che prevede pene detentive della durata massima compresa almeno tra uno e tre anni, in quanto essa comporta in pratica l'obbligo per gli Stati membri di prevedere almeno un anno quale pena massima.

La presidenza desidera sottolineare che la soluzione relativa al livello delle sanzioni è connessa al campo d'applicazione della proposta e pertanto in quest'ultimo caso alcuni elementi del pacchetto di compromesso presentato al COREPER il 7 aprile dovranno essere riveduti.

In considerazione della portata limitata dell'incriminazione, si chiede ai ministri di indicare

- *se accettano due anni come livello della sanzione per i reati di base all'articolo 9, paragrafo 2, come previsto nella proposta della Commissione,*
- *o se sostengono la posizione espressa da alcune delegazioni di ridurre il livello della sanzione alla reclusione non inferiore nel massimo a un anno.*

2. Circostanze aggravanti (articolo 9, paragrafi 3, 4 e 5)

La proposta della Commissione mirava ad affrontare due minacce emergenti nel mondo dell'informatica, introducendo due circostanze aggravanti per i reati di base. Le due nuove circostanze aggravanti cui si fa riferimento sono le seguenti:

- attacchi informatici su larga scala, perpetrati mediante le cosiddette botnet (attualmente incluse nell'articolo 9, paragrafo 3) e
- abuso dei dati personali altrui al fine di ottenere la fiducia di terzi, che facilita nella pratica l'esecuzione dell'attacco informatico (attualmente incluso nell'articolo 9, paragrafo 5)

Nel corso delle varie discussioni queste disposizioni, benché rappresentassero elementi centrali delle ambizioni espresse dalla Commissione, sono state notevolmente modificate per tenere conto delle preoccupazioni delle delegazioni, preservando nel contempo il contenuto della proposta della Commissione su queste questioni.

Per quanto riguarda il livello delle sanzioni per le circostanze aggravanti, il testo offre attualmente più flessibilità rispetto alla proposta originaria della Commissione. Sono previste due diverse soglie: una pena detentiva massima non inferiore ad anni tre e ad anni cinque, a seconda della gravità del reato, oltre all'introduzione di nuove circostanze in cui si applicherebbe la pena più elevata. Così, quando l'attacco ha provocato danni gravi o quando ha colpito un sistema di informazione relativo a infrastrutture critiche, il livello proposto di pena detentiva massima è di almeno anni cinque.

L'abuso dei dati anagrafici di una terza persona rientra nell'articolo 9, paragrafo 5 come mera circostanza aggravante senza che sia previsto un livello di sanzione specifico, mentre viene lasciata agli Stati membri la facoltà di decidere il metodo con cui raggiungere tale risultato. Nel corso delle discussioni, si è evidenziato più volte che occorre distinguere questo elemento da un'usurpazione d'identità, che è un fenomeno complesso di natura parzialmente diversa. Nel contempo, per quanto concerne gli attacchi informatici, il modus operandi è spesso utilizzato per perpetrare gravi reati informatici.

Alcune delegazioni mantengono la loro preferenza per l'esclusione di questo elemento dalla direttiva, poiché dovrebbe essere affrontato in uno strumento separato, incentrato sull'usurpazione d'identità in generale. Per quanto concerne l'altro elemento nuovo della proposta della Commissione, relativo all'utilizzo di uno strumento per il lancio di attacchi su larga scala (articolo 9, paragrafo 3), la questione ha incontrato una certa resistenza da parte delle delegazioni.

Si chiede ai ministri di indicare se il concetto di un reato commesso dalle botnet debba essere mantenuto come circostanza aggravante o se vada soppresso nel progetto.

Si chiede ai ministri di indicare se il concetto dell'abuso di dati di identità debba essere mantenuto come circostanza aggravante o se vada soppresso nel progetto.

In caso di risposta affermativa, la formulazione sarà ulteriormente adattata a livello di esperti.

3. Competenza giurisdizionale (articolo 13)

La questione della competenza giurisdizionale è stata oggetto di discussioni approfondite nei lavori del gruppo. Il testo di compromesso che figura nell'articolo 13 differisce dalla proposta iniziale della Commissione e sviluppa l'approccio presentato a tale riguardo nella direttiva concernente la tratta degli esseri umani. Introduce inoltre come norma minima il requisito di un positivo controllo della doppia punibilità, in particolare in relazione alla cittadinanza qualora il reato sia stato commesso al di fuori del territorio dello Stato membro interessato (articolo 13, paragrafo 1, lettera b)). Le condizioni di esercizio della competenza nazionale non sono soggette alle disposizioni della direttiva stabilite nel considerando 10 bis di nuova introduzione.

Si chiede ai ministri di confermare che la competenza giurisdizionale in relazione alla cittadinanza deve essere mantenuta nel campo di applicazione della proposta.

4. Strumenti utilizzati per commettere i reati - incriminazione del dispositivo (Articolo 7)

Il Gruppo ha confermato l'interpretazione della portata dell'articolo 7 del progetto di proposta conformemente all'articolo 6 della convenzione di Budapest sulla criminalità informatica.

L'articolo 6, paragrafo 3 della convenzione, tuttavia, prevede la possibilità per ciascuna parte contraente della convenzione di non applicare tale disposizione in alcune parti, ivi compreso quando si tratta di un dispositivo destinato o utilizzato principalmente al fine di commettere attacchi informatici. Una delegazione ha manifestato perplessità relativamente all'impossibilità di una simile eccezione nella proposta della Commissione.

A tale proposito la presidenza suggerisce la seguente formulazione di compromesso:

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.

2. Gli Stati membri possono inoltre adottare 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 di qualunque altro dispositivo destinato o utilizzato principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6.

Si invitano i ministri a confermare la proposta di compromesso della presidenza concernente l'articolo 7.

III. SITUAZIONE DEI LAVORI

La presidenza ritiene che vi sia un certo numero di disposizioni su cui è stato raggiunto un accordo provvisorio. Tali disposizioni sono: dall'articolo 1 all'articolo 6 e dall'articolo 11 all'articolo 19.

In considerazione di quanto sopra, si invita il Consiglio a prendere atto che il testo dall'articolo 1 all'articolo 6 e dall'articolo 11 all'articolo 19 quale figura nell'allegato II è oggetto di un accordo provvisorio, restando inteso che ulteriori discussioni potrebbero evidenziare la necessità di riesaminare una o più di dette disposizioni.

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 europea¹,

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 (...) competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge.

¹ GU C [...] del [...], pag. [...].

- (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 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 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.
- (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 l'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 organizzata², quando l'attacco è condotto su larga scala, o ha causato un danno grave o quando il reato è commesso (...) abusando dei dati personali concernenti una persona diversa dall'autore del reato al fine di ottenere la fiducia di terzi³.
- (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.

² GU L 300 dell'11.11.2008, pag. 42.

³ Il testo è stato adattato all'attuale formulazione della proposta.

- (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 informatici⁴.
- (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 avviare un'azione penale relativa a uno dei reati di cui agli articoli da 3 a 8 se commessi al di fuori del territorio dello Stato membro interessato, 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 qualora sia d'applicazione il principio *ne bis in idem*.
- (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.

⁴ LT ha espresso una riserva d'esame in attesa di un accordo sull'articolo 9.

- (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 Europa⁵.
- (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.

⁵ NL ha espresso una riserva d'esame in attesa di un accordo sull'articolo 15.

- (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 penale⁶, 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 dati⁷.
- (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 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, il Regno Unito e l'Irlanda hanno notificato che desiderano partecipare all'adozione ed applicazione della presente direttiva.

⁶ GU L 350 del 30.12.2008, pag. 60.

⁷ GU L 8 del 12.1.2001, pag. 1.

- (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"⁸, 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 attuazione⁹.

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 competenti¹⁰.

⁸ GU C 321 del 31.12.2003, pag. 1.

⁹ DE ha formulato una riserva d'esame.

¹⁰ ES mantiene una riserva d'esame.

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 informazione¹¹

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.

¹¹ Riserva d'esame di UK.

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 reati¹²

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 dispositivo, incluso¹³ 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.

(...)

¹² UK mantiene la sua riserva d'esame.

¹³ DE suggerisce di sopprimere i termini: "un dispositivo, incluso".

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 siano punibili con pene detentive non inferiori nel massimo ad anni tre, se commessi intenzionalmente con strumenti concepiti principalmente per lanciare attacchi contro un gran numero di sistemi di informazione o attacchi che causano danni gravi.

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 qualora¹⁴:
- 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, o
 - c) siano commessi ai danni di un sistema di informazione relativo a infrastrutture critiche.
5. Gli Stati membri adottano le misure necessarie affinché, qualora i reati siano stati commessi abusando dei dati personali di una persona diversa dall'autore allo scopo di guadagnare la fiducia di terzi, tali circostanze, purché non siano già elementi costitutivi dei reati di cui agli articoli da 3 a 5, possano essere considerate circostanze aggravanti (...).
- (...)

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.

¹⁴ RO ha formulato una riserva d'esame sull'articolo 9, paragrafo 4, lettere b) e c).

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 giurisdizionale¹⁵

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:

¹⁵ UK e ES mantengono una riserva d'esame su questo articolo.

- 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.

(...)¹⁶

- 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.

¹⁶ Su richiesta di varie delegazioni, l'articolo 13, paragrafo 1 bis è stato trasferito nel preambolo, come nuovo considerando 10 bis.

Articolo 14

Scambio di informazioni¹⁷

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 statistiche¹⁸

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.

¹⁷ Riserva d'esame di ES.

¹⁸ Riserva d'esame di ES.

Articolo 16

Sostituzione della decisione quadro 2005/222/GAI¹⁹

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.

¹⁹ UK mantiene una riserva d'esame.

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.
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 direttiva²⁰.

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

Il Presidente

Per il Consiglio

Il Presidente

²⁰ ES ha formulato riserve sul paragrafo 2 in quanto non si tratta di un elemento della direttiva concernente la tratta degli esseri umani.

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

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) per "sistema di informazione" s'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 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 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) 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 giurisdizionale²¹

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:

²¹ Il seguente considerando di accompagnamento è inserito nell'orientamento generale parziale: "La presente direttiva non regola le condizioni da soddisfare per avviare un'azione penale relativa a uno dei reati di cui agli articoli da 3 a 8 se commessi al di fuori del territorio dello Stato membro interessato, 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".

- 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.

Articolo 14

Scambio di informazioni

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

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.

Articolo 16

Sostituzione della decisione quadro 2005/222/GAI

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.
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 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,
