

ICT Security: Panorama Internazionale

SMAU 2002

Milano - 28 ottobre 2002

Diritto penale e Internet: analisi del contesto europeo

La Convenzione del Consiglio d'Europa sui cybercrime

MARA MIGNONE

TRANSCRIME – Università di Trento

mmignone@gelso.unitn.it

web site: <http://www.transcrime.unitn.it>

IL DIFFICILE ITER DI APPROVAZIONE DELLA CONVENZIONE

Il Consiglio d'Europa ha lavorato al testo della Convenzione dal **1997** fino al **2001**. Il testo finale è stato adottato l'8 novembre 2001
(Council of Europe – ETS 185 – Convention on Cybercrime.
<http://www.coe.int>);

Dal **23 novembre 2001**, è stata aperta la procedura per la **firma** del testo finale da parte degli Stati Membri del Consiglio d'Europa e di quelli che hanno collaborato alla elaborazione della Convenzione;

Condizioni per l'entrata in vigore: **5 ratifiche** e, di queste, almeno 3 da parte di Stati Membri del Consiglio d'Europa;

status al 24/10/2002:

Stati Membri: 30 firme (su 44) + 2 ratifiche (Albania – Rep. Ceca)

Stati non-Membri: 4 firme (Canada, Giappone, Sudafrica, USA) – nessuna ratifica

I PRINCIPALI OBIETTIVI DELLA CONVENZIONE

(Council of Europe, Explanatory Report to the Convention on Cybercrime – ETS 185)

1. Armonizzazione del **diritto penale sostanziale** nazionale in materia di cybercrime e dei reati collegati;
2. Conferire alle **procedure nazionali** il potere e gli strumenti necessari per l'investigazione e la repressione dei cybercrime, dei reati collegati commessi per mezzo di un sistema informatico e di quei reati per i quali vi siano prove in formato elettronico;
3. Organizzare un **sistema internazionale di cooperazione** veloce ed efficace.

PRINCIPALI CRITICHE AI VARI **DRAFT** DELLA CONVENZIONE

- ✓ violazione dei **diritti umani**, relativamente al pericolo di continue ingerenze nella sfera privata, nel diritto alla riservatezza e alla libertà di pensiero;
- ✓ ostacolo alla **libera circolazione** delle informazioni e delle idee;
- ✓ strumento per estendere i poteri delle agenzie di **law enforcement**;
- ✓ **rischio di criminalizzazione** per tecniche o prodotti pensati e realizzati per propositi assolutamente non illeciti;
- ✓ contrarietà rispetto a **leggi esistenti**, quali ad esempio la normativa in materia di privacy e di protezione/trattamento dei dati;
- ✓ poca partecipazione del **settore privato** (anche NGO). Quindi, eccessive soluzioni a favore del settore pubblico, poche orientate alle esigenze delle imprese;
- ✓ limitazione allo **sviluppo economico** di alcune attività legate alla rete (esempio: ISPs);

GLI ARTICOLI SOTTO ACCUSA

Global Internet Campaign “SI OPPONE” a:

- ✓ Art. 17, 18, 24, 25: norme che richiedono agli ISPs di conservare le registrazioni relative alle attività dei loro clienti
- ✓ Art. 6 e, in specifico, il concetto di “dispositivi illegali”
- ✓ Art. 10: protezione del diritto d'autore

(Global Internet Campaign, LETTERA SULLA FUTURA CONVENZIONE INTERNAZIONALE SUI REATI INFORMATICI, inviata alla Commissione Europea - 18 ottobre 2000)

PRINCIPALI CRITICHE AL **TESTO FINALE** DELLA CONVENZIONE

le critiche alla Convenzione possono essere raggruppate in tre ordini di motivi:

- 1.critiche contro la richiesta alle imprese che operano in Internet di fornire, in tempo reale, **dati e informazioni** alle agenzie di law enforcement (costi troppo alti). Perplessità anche da parte dei Garanti europei relativamente alla tutela della privacy (anche segretezza conversazioni) e al trattamento dei dati nell'ambito delle attività di investigazione e cooperazione internazionale;
- 2.critiche contro l'eccessivo potere che i governi finirebbero per avere nella **raccolta di informazioni** e nel **controllo dei cittadini**;
- 3.critiche contro le possibili restrizioni alle attività di **hacking** poste in essere dalle aziende per testare i propri sistemi di sicurezza.

DIRITTO PENALE SOSTANZIALE/1

9 TIPOLOGIE DI “OFFENCES”, RAGGRUPPATE IN 4 CATEGORIE

1. crimini contro confidentiality, integrity, and availability (CIA) dei dati e dei sistemi informatici:

Illegal access

Illegal interception

Data interference

System interference

Misuse of devices

2. computer-related offences

Computer-related forgery

Computer-related fraud

DIRITTO PENALE SOSTANZIALE/2

3. content-related offences:

Offences related to child pornography

(produzione per diffusione, offerta o messa a disposizione, distribuzione o trasmissione, il procurare e il possesso di pornografia infantile, attraverso un sistema informatico)

4. offences related to infringements of copyright and related rights

Reati contro la proprietà intellettuale e diritti connessi

(puniti se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico)

Protocollo aggiuntivo facoltativo per reati di propaganda anti-razziale e/o xenofoba attraverso un sistema informatico

DIRITTO PENALE SOSTANZIALE: ALCUNI ASPETTI PROBLEMATICI

- ✓ le Parti possono decidere di escludere le condotte definite come “**petty**” e/o “**insignificant**” ...
- ✓ le condotte previste dalla Convenzione devono essere commesse tutte “**without right**”;
- ✓ le condotte previste dalla Convenzione devono essere commesse tutte “**intentionally**”. In alcuni casi, la condotta deve anche prevedere esplicitamente il **beneficio economico** quale finalità del fatto perché possa essere prevista la responsabilità penale (es: computer-related fraud);

APPROFONDIMENTO:

Art. 6 – Misuse of device/1

1. Adozione di misure legislative e di altra natura necessarie per definire come reato, in base alla legge nazionale, se commessi intenzionalmente e senza autorizzazione:

a) fabbricazione, vendita, approvvigionamento per l'uso, importazione, distribuzione o l'utilizzabilità in altro modo di:

1. un'apparecchiatura, **incluso un programma per computer**, destinato o utilizzato principalmente al fine di commettere un qualsiasi reato in base agli artt. da 2 a 5 di cui sopra;
2. una **password** di un computer, un **codice di accesso** o **informazioni simili** con le quali l'intero sistema informatico o una sua parte sono accessibili, con l'intento di commettere un qualsiasi reato in base agli artt. da 2 a 5 di cui sopra;

Art. 6 – Misuse of device/2

- b) il possesso di uno degli elementi di cui ai sopra citati paragrafi a) 1. e 2., con l'intento di utilizzarlo allo scopo di commettere qualche reato in base agli artt. da 2 a 5. **Una Parte può richiedere per legge che vi sia il possesso di un certo numero di tali elementi perché vi sia una responsabilità penale.**
2. Questo articolo non va interpretato nel senso di prevedere una responsabilità penale laddove la produzione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzazione in altro modo o il possesso di cui al paragrafo 1 di questo articolo, non avvenga allo scopo di commettere un reato in base agli artt. da 2 a 5 di questa Convenzione, come anche per il collaudo autorizzato o la protezione di un sistema informatico.
3. Ogni Parte può riservarsi il diritto di non applicare il paragrafo 1. di questo articolo, purché tale riserva non concerna la vendita, la distribuzione o l'utilizzazione in altro modo degli elementi riferiti al paragrafo 1 a 2 di questo articolo

Commenti all'Art. 6 – Misuse of device

“the tools used by cyber-criminals to interrupt Internet services are the same tools those responsible for the Internet security use to protect the Internet and its users. The draft regulations appear to deny these tools even for crucial legitimate use”

(Tom Evslin, GIP Principal member e CEO of ITXC Corp.)

“crediamo che tale concetto (ndr dispositivi illegali) **manchi della specificità sufficiente** ad assicurare che non diverrà uno **strumento multifunzionale** per porre sotto **indagine** gli individui impegnati in attività completamente legali che implicano l'utilizzo del computer.

Come messo in evidenza da esperti del settore, questa norma scoraggerà anche lo sviluppo di nuovi strumenti di sicurezza e darà al **governo** un **ruolo improprio nella regolamentazione delle innovazioni scientifiche**”

(Global Internet Liberty Campaign)

LA SPIEGAZIONE UFFICIALE ...

“The offence requires that it be committed **intentionally** and **without right**.

In order to avoid the danger of over-criminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, **further elements are added to restrict the offence.**

Apart from the **general intent requirement**, there must be the **specific** (i.e. direct) **intent that the device is used for the purpose of committing any of the offences** established in Articles 2-5 of the Convention”

(Council of Europe, Explanatory Report to the Convention on Cybercrime – ETS 185)

DIRITTO PROCEDURALE/1

PREVISIONI DI MAGGIORE INTERESSE:

1. **Conservazione rapida di dati informatici immagazzinati in un sistema informatico – art. 16**

(ordine di conservazione da parte delle autorità + obbligo *ex lege* di protezione per almeno 90 giorni – rinnovabili!)

2. **Ingiunzioni di produrre – art. 18** (a carico di “soggetti” e ISPs) (... il problema sono le informazioni che possono essere richiestelle!)

3. **Perquisizioni e sequestri – art. 19**

(Sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici + possibilità di “rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato”)

4. **Raccolta in tempo reale di dati informatici – artt. 20 – 21**

Raccolta e registrazione da parte delle autorità competenti/ordine agli ISPS + obbligo per gli ISPs di cooperare ed assistere le autorità competenti

DIRITTO PROCEDURALE/2

5. **Informazioni spontanee – art. 26**

(possibilità di trasmissione, anche in assenza di richiesta preventiva, di informazioni ottenute nell'ambito delle proprie indagini ... se di aiuto per la Parte ricevente nell'avvio o nello svolgimento di indagini o procedimenti riguardanti i reati previsti dalla Convenzione)

6. **Mutua assistenza e poteri di indagine– artt. 31 - 34**

(possibilità di accesso **SENZA AUTORIZZAZIONE** a dati informatici immagazzinati in un sistema informatico con il consenso o quando pubblicamente disponibili)

ICT Security: Panorama Internazionale

SMAU 2002

Milano - 28 ottobre 2002

Diritto penale e Internet: analisi del contesto europeo

La Convenzione del Consiglio d'Europa sui cybercrime

MARA MIGNONE

TRANSCRIME – Università di Trento

mmignone@gelso.unitn.it

web site: <http://www.transcrime.unitn.it>