

$$\frac{A_{12}}{360}$$



Francesca Santoro

COOPERAZIONE  
INTERNAZIONALE  
IN MATERIA  
DI CRIMINALITÀ INFORMATICA



Copyright © MMXI  
ARACNE editrice S.r.l.

[www.aracneeditrice.it](http://www.aracneeditrice.it)  
[info@aracneeditrice.it](mailto:info@aracneeditrice.it)

via Raffaele Garofalo, 133/A-B  
00173 Roma  
(06) 93781065

isbn 978-88-548-4214-4

*I diritti di traduzione, di memorizzazione elettronica,  
di riproduzione e di adattamento anche parziale,  
con qualsiasi mezzo, sono riservati per tutti i Paesi.*

*Non sono assolutamente consentite le fotocopie  
senza il permesso scritto dell'Editore.*

I edizione: luglio 2011

A Massimiliano



## 9 Introduzione

### 13 Capitolo I

#### La criminalità informatica come *species* del *genus* criminalità transnazionale

1.1. Globalizzazione e criminalità transnazionale – 1.2. Il ruolo dell'ONU nel contrasto del fenomeno dei crimini transnazionali – 1.2.1. La nozione di crimine transnazionale – 1.2.2. Distinzione tra criminalità transnazionale e criminalità internazionale – 1.3. I crimini informatici nel “villaggio globale” – 1.4. Cyberspazio: il carattere transnazionale dei reati informatici – 1.5. L'erosione del monopolio statale relativo alla regolamentazione dell'assetto giuridico dei privati e all'esercizio dell'attività coercitiva dopo l'avvento di Internet – 1.6. La strategia della cooperazione internazionale nel contrasto alla criminalità transfrontaliera – 1.7. Lotta al crimine transnazionale: interesse astratto della comunità internazionale o aggregazione di interessi nazionali?

### 59 Capitolo II

#### La definizione della fattispecie reato informatico

2.1. Diffusione della tecnologia e proliferazione dei crimini informatici – 2.1.1. Le tre fasi evolutive dei reati digitali nella società dell'IT – 2.2. Offensività dell'azione criminosa: pluralità di beni giuridici da tutelare – 2.3. *Computer crime*: il problema definitorio – 2.4. Inquadramento comune della fattispecie di reato informatico in ambito sovranazionale: la Convenzione di Budapest – 2.5. I tipi più comuni di *computer crime* – 2.5.1. Accesso abusivo – 2.5.2. Intercettazione abusiva – 2.5.3. Danneggiamento informatico e attacchi all'integrità dei sistemi – 2.5.4. Falso e frode informatica – 2.5.5. Pornopedofilia informatica – 2.5.6. Reati informatici e proprietà intellettuale – 2.6. L'armonizzazione dei sistemi penali e gli obblighi imposti ai singoli Stati dalla Convenzione di Budapest in ambito di diritto sostanziale – 2.7. Le nuove frontiere del *computer crime*: *cyberwarfare* e cyberterrorismo

## 115 Capitolo III

### La cooperazione internazionale nella repressione dei reati informatici alla luce della Convenzione di Budapest

3.1. La natura delocalizzata di Internet e la crisi del principio *locus commissi delicti* – 3.1.1. Quale giurisdizione è competente a conoscere dei fatti che si verificano in rete? – 3.1.2. I criteri di determinazione della competenza giurisdizionale contenuti nell'art. 22 della Convenzione di Budapest – 3.2. La strategia della cooperazione internazionale in materia di criminalità informatica – 3.3. Lo strumento dell'extradizione – 3.4. Principi generali in materia di assistenza giudiziaria e scambio di informazioni – 3.5. L'esperienza di cooperazione europea-americana: brevi cenni – 3.6. Prospettive evolutive della Convenzione

## 161 Capitolo IV

### Il coordinamento investigativo internazionale

4.1. L'oggetto dell'indagine transnazionale in materia di criminalità informatica – 4.2. Il principio del coordinamento investigativo nella prassi e nelle fonti sovranazionali – 4.3. La nozione giuridica di coordinamento – 4.4. L'Organizzazione Internazionale di Polizia Criminale – 4.5. La Centrale operativa europea nella lotta al *cyber crime*

## 179 Conclusioni

### 181 *Tavola delle ratifiche*

### 185 *Bibliografia*

### 193 *Webgrafia*



## Introduzione

Attraverso la penetrazione tecnologica degli ultimi decenni, la moderna società risulta profondamente trasformata nei costumi e nelle aspettative.

In particolare, con l'avvento della tecnologia informatica emerge attualmente un rilevante sviluppo delle relazioni tra le diverse aree del globo. L'aspetto interessante è che la maggior parte di queste relazioni si instaurano con modalità e tempi tali da far sì che ciò che avviene in un'area si ripercuota anche in tempo reale sulle altre aree, pure le più lontane, con esiti che i tradizionali modelli interpretativi dell'economia e della società non sono più in grado di valutare correntemente, soprattutto per la simultaneità tra l'azione ed il cambiamento che si produce.

La transnazionalità di alcuni fenomeni criminosi da anni rappresenta un'enorme sfida per l'evoluzione e l'innovazione delle politiche criminali e genera l'esigenza di dare impulso ad un nuovo approccio ideologico e metodologico di portata globale. Tale esigenza è avvertita in modo ancora più forte quando si tratta dei reati informatici in quanto lo spostamento da un ambiente tangibile e corporeo verso un ambiente elettronico ed intangibile, comporta che i reati commessi e gli strumenti e i metodi utilizzati per investigarli non siano più soggetti alle regole tradizionali e precostituite. Soprattutto le norme che disciplinano i mezzi di comunicazione tradizionali (radio, stampa, televisione, editoria) risultano oggi, a fronte della nuova dimensione virtuale (c.d. cyberspazio), profondamente inadeguate perché sono state tutte elaborate pensando ad uno spazio

territoriale. Ed è chiaro che diventa molto difficile estenderle fino a ricomprendervi le azioni esercitate attraverso internet, poiché la rete ha una natura delocalizzata.

Sul fronte delle strategie di contrasto, pertanto, le nuove politiche criminali dovranno prima di tutto prospettare la costituzione di un sistema che incentivi in particolar modo forme di cooperazione internazionale, attraverso il potenziamento delle relazioni tra gli Stati e l'armonizzazione degli strumenti di contrasto. Inoltre, un'efficace strategia di politica criminale dovrà seguire un percorso che, sebbene sia stato già intrapreso a livello nazionale o internazionale, venga costantemente modificato da continui e rapidi aggiustamenti che tengano conto del costante progresso della tecnologia, essendo l'elemento tecnologico l'elemento specializzante tali fattispecie di reato.

Un notevole passo in avanti è stato fatto, sul fronte delle strategie di contrasto, con la recente Convenzione di Budapest del 2001 che attualmente rappresenta il maggior sforzo sinora effettuato, a livello sovranazionale, per tentare di combattere in modo efficace questo particolare tipo di criminalità, i cui sviluppi minacciano seriamente oltre che il settore dell'economia e della finanza internazionale, lo stesso equilibrio politico dei Paesi industrializzati.

Essa chiude un complesso percorso normativo internazionale avviato in sede OCSE, nel cui ambito fu elaborata una prima "lista comune" di reati informatici già sin dal 1983.

Ma è chiaro che, a causa dell'incessante progresso tecnologico, la materia in esame risulta un terreno ideale per lo sviluppo di norme che in primo luogo dovranno essere inquadrate in un regime che andrà necessariamente aggiornato di continuo alla luce delle nuove tendenze e della peculiarità del mezzo tecnico utilizzato e in secondo luogo dovranno rappresentare fonti di soluzioni a carattere globale.

Certo è che il percorso d'integrazione e di adattamento delle normative nazionali si presenta complesso. L'esigenza di assicurare la cooperazione internazionale si affianca, infatti, a quella di realizzare metodi operativi efficaci, che le istituzioni dovranno applicare tenendo presenti le diverse implicazioni offerte dall'evolversi delle tecnologie e, al tempo stesso, le problematiche del rispetto dei diritti

fondamentali, rispetto alle quali occorre prestare particolare attenzione. Fondamentale è la stabilità e la continuità della cooperazione internazionale, e quindi la definizione di procedure uniformi, nonché la certezza delle competenze dei soggetti abilitati a dialogare istituzionalmente: questi ultimi dovranno non soltanto essere in grado di effettuare lo scambio di dati e di suggerimenti operativi ed esperienze concrete d'indagine, ma dovranno anche essere aperti ad una prospettiva di regolazione spontanea del cyberspazio, esattamente come è accaduto per gli atti di pirateria aerea o per il terrorismo internazionale.