

I REATI INFORMATICI NELL'ORDINAMENTO ITALIANO

DANILO VIZZARRO
INFO@DANILOVIZZARRO.IT

16 MAGGIO 2006

Indice

1	Il Computer Crime	2
1.1	Il Panorama Europeo	2
1.2	Il Panorama Italiano	3
1.3	Opere Pirata e Diritto d'Autore	4
1.4	Identificazione dell'Autore di un Reato	5
2	L'accesso Abusivo	6
2.1	Il Panorama Italiano ed Europeo	6
2.2	La Lesione del Domicilio Informatico	6
2.3	I Sistemi Informatici Oggetto di Tutela	7
2.4	L'intrusione Abusiva	7
2.5	La Permanenza nel Sistema Altrui	8
2.6	Sanzioni e Circostanze Aggravanti	8
3	Diffusione Abusiva di Codici d'Accesso	9
3.1	Il Panorama Italiano	9
3.2	Identificazione dell'Oggetto del Reato	9
3.3	Le Condotte Punite	10
4	DoS e Intercettazione Abusiva	11
4.1	Le Condotte Punite	11
4.2	Sanzioni e Circostanze Aggravanti	12
4.3	Il Netstrike	12
5	Conclusione	14

Capitolo 1

Il Computer Crime

Il Computer Crime è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica.

Tutti i reati informatici sono accomunati da:

- L'utilizzo della tecnologia informatica per compiere l'abuso;
- L'utilizzo dell'elaboratore nella realizzazione del fatto.

1.1 Il Panorama Europeo

L'esigenza di punire i crimini informatici, emerse già alla fine degli anni '80, tanto che, il 13 Settembre 1989, il Consiglio d'Europa ha emanato una 'Raccomandazione sulla Criminalità Informatica' dove venivano discusse le condotte informatiche abusive. I reati vennero divisi in due liste: facevano parte della prima lista detta 'lista minima' quelle condotte che gli Stati sono invitati a perseguire penalmente quali:

- La frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- Il falso in documenti informatici;
- Il danneggiamento di dati e programmi;
- Il sabotaggio informatico;
- L'accesso abusivo associato alla violazione delle misure di sicurezza del sistema;

- L'intercettazione non autorizzata;
- La riproduzione non autorizzata di programmi protetti;
- La riproduzione non autorizzata di topografie.

Facevano invece parte della seconda lista detta 'lista facoltativa' condotte 'solo eventualmente' da incriminare, quali:

- L'alterazione di dati o programmi non autorizzata sempre che non costituisca un danneggiamento;
- Lo spionaggio informatico inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- L'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- L'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Successivamente, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale (AIDP) del 1990, emerse la necessità di incriminare non solo i reati previsti dalla lista minima ma anche le condotte descritte nella lista facoltativa. Le varie legislazioni informatiche che hanno seguito il XV Congresso dell'AIDP hanno tenuto conto delle indicazioni date dall'associazione e nel Settembre 1994 il Consiglio d'Europa ha aggiornato la precedente Raccomandazione ampliando le condotte perseguibili penalmente, inserendo:

- Il commercio di codici d'accesso ottenuti illegalmente;
- La diffusione di virus e malware.

1.2 Il Panorama Italiano

Il legislatore ha scelto di collocare i nuovi reati informatici accanto alle figure di reato già esistenti.

1. La Frode Informatica. Viene associata alla frode 'tradizionale' con la differenza che viene realizzata per mezzo di uno strumento informatico. La legge 547 del 1993 aggiunge al Codice Penale l'art 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Non viene identificato come frode informatica l'indebito utilizzo di carte di pagamento magnetiche che è invece disciplinato dall'art. 12 della legge 197 del 5 Luglio 1991.

2. La Falsificazione di Documenti Informatici. I documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali e l'art. 491-bis c.p. prevede l'applicabilità delle disposizioni sulla falsità in atti pubblici e privati. La falsificazione in comunicazioni informatiche ricalca invece il delitto di falsità in scrittura privata (art. 485 c.p.).
3. Le Aggressioni all'Integrità dei Dati. La legge 547 del 1993 amplia le precedenti disposizioni in materia e integra al Codice Penale l'art. 635-bis sul danneggiamento dei sistemi informatici e telematici, l'art. 615-quinquies sulla diffusione di virus e malware, l'art. 392 sulla violenza sulle cose (a tal proposito la legge 547 del 1993 precisa le situazioni dove le aggressioni riguardano beni informatici) ed infine l'art. 420 sul reato di attentato ad impianti di pubblica utilità.
4. Le Aggressioni alla Riservatezza dei Dati e delle Comunicazioni Informatiche. Riguardo le forme di intrusione nella sfera privata altrui si incriminano l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), la detenzione e diffusione abusiva di codici d'accesso (art. 615-quater c.p.) la rivelazione del contenuto di documenti segreti (art. 621 c.p.) includendo i documenti protetti contenuti su supporti informatici.

Circa le aggressioni alle comunicazioni informatiche viene ampliato il concetto di corrispondenza contenuto nel quarto comma dell'art. 616 c.p. che ingloba anche la corrispondenza informatica e telematica e punisce l'intercettazione e l'interruzione di comunicazioni informatiche (art. 617-quater c.p.) e l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni informatiche (art. 617-quinquies), qualora tali condotte non siano esplicitamente autorizzate.

1.3 Opere Pirata e Diritto d'Autore

Nei casi di pirateria, viene punita l'appropriazione indebita dell'idea originale. Gli oggetti che si intende tutelare sono di diversi tipi.

1. Le Topografie. Con qualche anno di ritardo rispetto ai termini previsti dalla direttiva europea, la legge 70 del 21 Febbraio 1989 tutela le topografie di prodotti a semiconduttori ovvero i tracciati incisi sulle piastrine di silicio. A tal proposito non sono previste sanzioni penali per le violazioni dei diritti nonostante la Raccomandazione del 13 Settembre 1989 del Consiglio d'Europa le preveda.

2. I Software. Con la modifica della legge 633 del 22 Aprile 1941 sul diritto d'autore, i programmi per elaboratore vengono inclusi tra le opere di ingegno. In seguito alla Direttiva CEE del 14 Maggio 1991 recepita dal Dlgs 518 del 29 Dicembre 1992, si vuole prevenire la duplicazione e la vendita dei programmi a fine di lucro (art. 171-bis 1.a.). La sanzione pecuniaria prevista viene successivamente aggravata dal Dlgs 205 del 15 Marzo 1996.
3. I Database. Il Dlgs 169 del 6 Maggio 1999 riconosce i diritti di esclusiva al creatore del database (artt 64-quinquies e sexies) e il diritto di tutela al 'costitutore' del database, ovvero a colui che effettua investimenti in termini di tempo e denaro per raccogliere e inserire materiale nel database, con il fine di salvaguardare il valore patrimoniale dell'investimento.
4. Le Opere Fonografiche e Videografiche. Gli abusi di duplicazione e distribuzione, vengono disciplinati dalla legge 406 del 29 Luglio 1981, mentre le opere cinematografiche destinate al circuito cinematografico e televisivo sono tutelate dalla legge 400 del 20 Luglio 1985.

1.4 Identificazione dell'Autore di un Reato

Le tipologie di reato in Internet sono di svariati tipi: si pensi al messaggio offensivo inviato per posta elettronica, alla diffusione di immagini diffamatorie o pedopornografiche, o al download di risorse protette dal diritto d'autore. L'identificazione dell'autore di un reato online è resa problematica da molteplici fattori: in un sistema, quale Internet, non controllato da alcuna autorità sovranazionale che consente agli utenti assoluto anonimato, dove i dati si diffondono con rapidità elevatissima oltre i confini nazionali, e dove cancellare le tracce è relativamente semplice, identificare il responsabile di un reato è un'operazione davvero complessa che difficilmente viene eseguita con successo.

Capitolo 2

L'accesso Abusivo

L'art. 615-ter c.p. punisce 'Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza'.

Ancora una volta il legislatore italiano ha voluto ricalcare una figura di reato già esistente quale la violazione del domicilio (art. 614 c.p.).

2.1 Il Panorama Italiano ed Europeo

A livello europeo tutte le norme che regolano l'accesso abusivo ad un sistema informatico presentano delle costanti:

- Si richiede che siano state violate delle misure di protezione;
- Si punisce l'accesso abusivo sia da remoto che da locale qualora chi commette il reato non sia autorizzato ad accedere a dei settori di memoria protetti;
- Deve essere minacciata la riservatezza dei dati o dei programmi. Che il sistema informatico attaccato custodisce.

2.2 La Lesione del Domicilio Informatico

Secondo una prima tesi in dottrina, il legislatore mira a introdurre la figura di domicilio informatico inteso come un'espansione ideale dell'area di rispetto pertinente al soggetto interessato. Ciò che si vuole tutelare è quindi quella che può definirsi 'privacy informatica' ancor prima di verificare se siano state attaccate l'integrità e la riservatezza dei dati.

Secondo una seconda tesi, il domicilio informatico non può assolutamente

essere comparato alla tradizionale figura di domicilio in quanto non c'è alcuna analogia tra i sistemi informatici e i luoghi privati menzionati dall'art. 614 c.p. A questo si aggiunge il fatto che se il domicilio tradizionale e quello informatico fossero messi sullo stesso piano non sarebbe comprensibile la scelta del legislatore di tutelare solo i sistemi informatici protetti da misure di sicurezza.

Considerata l'aggravante applicabile 'se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti' si può assumere che l'art. 615-ter c.p. mira a salvaguardare l'integrità dei dati prescindendo dalla collocazione dell'art. sull'accesso abusivo tra i reati di violazione del domicilio.

Considerando invece la decisione del legislatore di tutelare solo i sistemi protetti da misure di sicurezza pare plausibile l'intenzione di salvaguardare la riservatezza dei dati. Si assume infatti che il titolare debba manifestare il suo interesse a tutelare la riservatezza dei dati, adattando misure di sicurezza indipendentemente dalla loro complessità tecnica di implementazione.

2.3 I Sistemi Informatici Oggetto di Tutela

Resta estraneo all'art 615-ter c.p. l'accesso abusivo a sistemi informatici predisposti esclusivamente al controllo e alla gestione di altri apparecchi in quanto, non contenendo tali apparecchi dati rilevanti, non viene messa a rischio la loro riservatezza. In questi casi non vi è un danneggiamento logico del sistema anche se l'intrusione potrebbe essere finalizzata ad usufruire di servizi senza pagarne il corrispettivo dovuto.

2.4 L'intrusione Abusiva

L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema. L'art. 615-ter c.p. punisce la semplice intrusione ancor prima di valutare l'ipotesi di danneggiamento o furto dei dati.

Il reato può anche essere causato da soggetti legittimati all'uso del sistema, autorizzati ad accedere solo ad una parte dei dati contenuti in memoria. In tal caso il sistema protetto diviene quella parte di memoria a cui l'accesso non è autorizzato.

2.5 La Permanenza nel Sistema Altrui

Ha senso parlare di permanenza non autorizzata qualora il soggetto responsabile dell'intrusione si sia trovato casualmente in una zona protetta del sistema. Ad una introduzione nel sistema inizialmente autorizzata deve quindi far seguito una permanenza non autorizzata che si realizza allorquando il reo 'vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo'.

2.6 Sanzioni e Circostanze Aggravanti

La pena prevista per il reato di accesso abusivo è la reclusione fino a 3 anni. Qualora:

1. 'il fatto e' commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema';
2. 'il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se e' palesemente armato';
3. 'dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti';

la reclusione è da 1 a 5 anni con un incremento della pena da 3 a 8 anni se i fatti al punto 1 e 2 riguardano 'riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico'.

Capitolo 3

Diffusione Abusiva di Codici d'Accesso

L'art. 615-quater c.p. punisce 'Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo'.

3.1 Il Panorama Italiano

L'art. 615-quater delinea quello che può definirsi un reato di pericolo indiretto in quanto entrando in possesso abusivamente di codici d'accesso, si presenta il pericolo di commettere un accesso abusivo ad un sistema o si possano diffondere tali codici ad altre persone che a loro volta potrebbero accedere abusivamente ad un sistema. In nessuno degli ordinamenti vicini a quello italiano è stata introdotta una norma analoga. Solo negli USA tale condotta assume rilevanza penale (l'art. 502 [c][6] del codice penale californiano punisce chiunque consapevolmente e senza esserne autorizzato procura o aiuta altri a procurarsi un mezzo di accesso ad un computer o ad una rete informatica).

3.2 Identificazione dell'Oggetto del Reato

L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo. Può infatti trattarsi di una password, di un codice d'accesso o

semplicemente di informazioni che consentano di eludere le misure di protezione.

Non rientrano in quanto previsto dall'art 615-quater c.p. l'indebita acquisizione di carte di credito telefoniche in quanto l'illecito utilizzo permetterebbe solo di usufruire delle prestazioni telefoniche dell'apparecchio.

Diverso è il caso delle carte di debito magnetiche con le quali è possibile anche avere informazioni sul rispettivo conto corrente. In tal caso l'art. 615-quater c.p. completa quanto previsto dall'art 12 della legge 197 del 1991 a tutela di chi utilizza tali carte.

Rientrano nelle condotte descritte dall'art 615-quater c.p. anche le smart-card utilizzate per decodificare le trasmissioni televisive criptate.

3.3 Le Condotte Punite

Le condotte punite se realizzate abusivamente dall'art. 615-quater c.p. sono molteplici:

- l'utilizzo non autorizzato di codici d'accesso;
- la diffusione che si manifesta nel rendere disponibili tali codici ad un numero indeterminato di soggetti;
- la comunicazione che consiste nel rendere disponibili tali codici ad un numero limitato di soggetti;
- la consegna che riguarda cose materiali come può essere un token di accesso ad un servizio di home banking;
- la comunicazione o diffusione di istruzioni che permettono di eludere le protezioni di un sistema.

Resta irrilevante il fatto che i codici siano stati procurati abusivamente o mediante l'autonoma elaborazione.

Capitolo 4

DoS e Intercettazione Abusiva

L'art. 617-quater c.p. punisce 'Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe'.

L'art 617-quinquies c.p. punisce, invece, 'Chiunque fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi'.

Con gli articoli su citati, emerge ancora una volta l'intenzione del legislatore di ampliare alle comunicazioni informatiche la tutela che già esisteva per le comunicazioni telegrafiche e telefoniche.

4.1 Le Condotte Punite

Per comunicazione informatica si intende qualsiasi scambio di dati avviene tra due o più sistemi informatici: si pensi al semplice scambio di email, alle mailing list, ai forum, ai newsgroup o alle chat. Per poter parlare di intercettazione abusiva, è necessario poter determinare il numero di destinatari ai quali tale comunicazione è diretta, al fine di poter distinguere le comunicazioni a carattere riservato, con quelle a carattere pubblico, per la quale non è ipotizzabile alcuna riservatezza (si pensi per esempio ai siti web). Il reato di cui all'art. 617-quater, si verifica non appena si prende cognizione, in maniera fraudolenta, del contenuto di un messaggio in corso di trasmissione, mentre, il reato di cui all'art. 617-quinquies si verifica, non appena viene fatta cessare, in maniera fraudolenta, una comunicazione in corso.

Tali condotte sono punite se realizzate all'insaputa dei soggetti che partecipa-

no alla comunicazione. Il reato è invece escluso, se c'è stata un'autorizzazione esplicita preventiva, da parte di tali soggetti.

Qualora la comunicazione consista nello scambio di messaggi di posta elettronica, ha senso parlare di corrispondenza informatica intesa come ampliamento della tradizionale forma di 'corrispondenza', la cui libertà e segretezza sono ritenute 'inviolabili' dall'art. 15 della Costituzione. Ciò che si intende tutelare con gli articoli 617-quater e 617-quinquies, sono proprio la libertà e la riservatezza delle comunicazioni informatiche, al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

4.2 Sanzioni e Circostanze Aggravanti

La pena prevista per il reato di intercettazione o interruzione abusiva di comunicazioni informatiche è la reclusione da 6 mesi a 4 anni.

La reclusione è invece da 1 a 5 anni, se il fatto è commesso:

1. 'in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità';
2. 'da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema';
3. 'da chi esercita anche abusivamente la professione di investigatore privato';

Allo stesso modo si punisce chi 'rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni'. Per quanto riguarda il reato di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, esaminato dall'art. 617-quinquies, la pena prevista è la reclusione da 1 a 4 anni.

4.3 Il Netstrike

Il Netstrike è un modo utilizzato dalla comunità informatica per manifestare il proprio dissenso su questioni di rilevante importanza sociale. Per realizzarlo si invita ogni utente della rete a collegarsi attraverso il proprio browser ad un determinato sito web a un'ora precisa ed effettuare continue richieste

di aggiornamento della homepage. Il risultato è che possa essere generato un crash del server sulla quale il sito web risiede, il quale non riesce ad accontentare tutte le richieste che giungono.

Il Netstrike può essere paragonato a un attacco DDoS (Distributed Denial of Service) in quanto il risultato generato è lo stesso, ma ciò che li differenzia è che nel Netstrike ci si limita a puntare una pagina web tramite il proprio browser web, mentre nei DDoS si utilizzano particolari tool apposti al fine di migliorare l'efficacia dell'attacco. Questo permette a qualsiasi utente di Internet di partecipare alla manifestazione nella quale non viene ricercata alcuna forma di anonimità proprio in virtù del fatto che è del tutto lecito collegarsi ad una pagina web utilizzando un comune browser. Il Netstrike diventa illegittimo qualora vengano utilizzati script o altri programmi in grado di eseguire operazioni come automatizzare l'aggiornamento della pagina.

Capitolo 5

Conclusione

Nonostante la normativa italiana in materia sia una delle più recenti in materia, l'informatica avanza molto più velocemente di quanto possano fare le leggi. A complicare una situazione già complessa si aggiunge:

- la difficoltà che si riscontra nell'identificazione della persona che ha commesso il reato una volta identificato il sistema informatico utilizzato per commettere il reato
- la possibilità di essere vittime di criminali informatici che attaccano da stati con ordinamenti diversi dal nostro
- la possibilità di celare con facilità l'identità del criminale dietro quella di altre persone innocenti
- la carenza di sentenze a riguardo

Ci si trova pertanto molto spesso di a dei vuoti normativi a cui è davvero difficile porre rimedio.