Collegio Ghislieri – Convegno "PRESI NELLA RETE"

23 novembre 2012

Abstract

Normativa internazionale in tema di cybercrime

Fin dall'inizio degli anni 80 lo sviluppo delle nuove tecnologie nel campo dell'informatica e l'utilizzo sempre più diffuso di impianti di elaborazione e trasmissione elettronica dei dati, hanno determinato la nascita di nuove tipologie di illeciti. Tali condotte hanno convenzionalmente assunto la denominazione di "*computer crimes*".

La necessità di un intervento volto a regolare comportamenti socialmente dannosi o pericolosi legati alle nuove tecnologie era stata avvertita fin dai primi anni ottanta a tal punto da indurre numerosi Stati, sia europei (ad esempio, Danimarca, Norvegia, Austria, Francia) che extraeuropei (ad esempio, Stati Uniti, Australia, Canada, Giappone) a dotarsi di una specifica legislazione penale specifica.

Il 13 Settembre 1989, il Consiglio d'Europa emanò una "*Raccomandazione sulla Criminalità Informatica"* dove venivano discusse le condotte informatiche abusive e si pensò per la prima volta ad alcune fattispecie di reato da introdurre negli ordinamenti degli Stati membri. I reati vennero divisi in due liste: facevano parte della prima lista detta 'lista minima' quelle condotte che gli Stati erano invitati a perseguire penalmente quali ad esempio: la frode informatica; il falso in documenti; il danneggiamento dei dati e programmi; facevano invece parte della seconda lista detta "lista facoltativa" condotte come: l'alterazione dei dati e programmi e lo spionaggio informatico la cui repressione veniva lasciata alla valutazione discrezionale dei singoli stati.

Successivamente, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale (AIDP) - Bruxelles 1990 -, emerse la necessità di incriminare non solo i reati previsti dalla lista minima, ma anche le condotte descritte nella lista facoltativa. Le varie delegazioni 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 e la diffusione di *malware*. L'Italia aveva già recepito tempo prima, con la legge n.547 del 1993, anche quest'ultimi delitti ed è stato uno dei primi Paesi ad avere una legislazione soddisfacente.

Nell'ultimo decennio, nel mondo della telematica e di *internet* si è avuta una radicale trasformazione culturale, la straordinaria velocità con la quale le tecnologie dell'informazione si sono evolute e l'uso sempre più frequente e capillare dei sistemi e delle reti informatiche da parte dei cittadini, delle aziende e dei paesi nazionali li hanno resi anche più vulnerabili.

Il Consiglio d'Europa ha adottato, il 23 novembre 2001 la Convenzione di Budapest in tema di lotta contro la criminalità informatica al fine di introdurre norme internazionali comuni ed efficaci basate su linee guida e procedure adottate a livello internazionale per lo svolgimento delle indagini informatiche, ma soprattutto, al fine di migliorare il coordinamento e la cooperazione tra le Autorità Giudiziarie e tra le Forze dell'ordine dei Paesi firmatari (oggi, 23 novembre 2012, qui al Ghisleri, tra l'altro, ricorre proprio il suo undicesimo compleanno).

Una delle principali novità introdotte dalla Convenzione è, infatti, la sua applicabilità rispetto alle nuove norme sulle investigazioni informatiche anche a tutti i delitti commessi mediante un sistema informatico, o comunque in tutti i casi in cui si possono raccogliere elementi di prova in forma elettronica. Importante è anche l'introduzione di quasi tutte le fattispecie relative ai reati informatici tra i reati presupposto della legge n. 231 del 2001 sulla responsabilità "penale" delle persone giuridiche.

La tabella che si allega è aggiornata alla fine di ottobre scorso con l'indicazione di tutti gli Stati membri che hanno partecipato alla stesura della Convenzione del 2001, quelli che l'hanno firmata e quelli che ancora non l'hanno fatto. Il tutto corredato di date e riferimenti.

Su 47 Stati :

- 4 Stati non hanno firmato la Convenzione
- 7 Stati hanno firmato ma non hanno ratificato (quindi la legge non è in vigore)
- 36 Stati hanno firmato, ratificato e la Convenzione per loro è entrata in vigore

Altri 12 Stati non membri del Consiglio d'Europa si sono seduti nel 2001 al tavolo della Convenzione : ma solo 4 hanno firmato (Usa, Giappone, sud Africa e Canada) e di questi ad oggi solo 2 (Usa, Giappone) hanno ratificato la Convenzione con conseguente entrata in vigore.

Un po' poco di fronte ad una sfida globale e planetaria.

In Italia la convenzione è stata ratificata con la legge n. 48 del 2008 che ha novellato il codice di procedura penale e inserito nel codice penale altre fattispecie delittuose rispetto a quelle già previste fin dal 1993 (sono state introdotte tre ulteriori norme in tema di danneggiamento informatico oltre all'art. 635 bis c.p. già previsto e con questa ulteriormente modificato ed è stato definito meglio il reato di falso documento informatico, art. 491 bis cp).

Un'altra normativa internazionale molto importante è quella sulla *data retention* ovvero sulla conservazione dei dati di traffico telefonico e telematico per motivi di indagine nei procedimenti penali. Fino a quando avremo un sufficiente periodo di conservazione dei dati telefonici/telematici con indizi utilissimi alle indagini ? E' davvero utile ? Quando cominceremo a considerarli indizi e non elementi di prova ? Quando l'eccessivo ricorso a tali indizi provocherà le ire del legislatore europeo con conseguente giro di vite e limitazione del tempo di conservazione dei dati telematici (e telefonici) ? L'ingresso (prossimo futuro ?) dell'IPV6 sulla scena dei dati telematici faciliterà le indagini ? Quando ci si accorgerà che il rischio di intrusioni nella privacy dei cittadini da parte delle forze dell'ordine è più basso del rischio di intrusioni nella privacy dei cittadini per motivi commerciali e di business ?[1] Perché non si nota e non si denuncia anche quando i processi su dossieraggi e intrusioni sistematiche in Italia e nel mondo finiscono in giganteschi buchi neri..che tutto inghiottono e nulla chiariscono e puniscono ?

Si potrebbe avere una legislazione efficace a livello internazionale e pene molto più severe per gli eventuali abusi. Troppi però fanno finta di non capire e il problema si rimanda……..fino alla prossima emergenza….[2]

Ma questi sforzi legislativi limitati ad un numero ristretto di nazioni non sono purtroppo sufficienti.

---

[1] Sono un avvocato che da 12 anni si occupa di processi per reati informatici anche relativi a casi di spionaggio/dossieraggio come avvocato sia di indagati e imputati sia di parti lese.

[2] Non abbiamo il tempo necessario per parlare qui di un altro esempio di schizzofrenia legislativa ovvero del problema del "captatore informatico". Uno strumento che risolverebbe molti problemi a livello di indagini ma che per funzionare giuridicamente bene avrebbe bisogno di regole che però nessuno vuole scrivere: è un po' come una macchina da corsa che potrebbe vincere tutte le gare aiutando le persone offese ad ottenere buoni risultati anche in indagini che toccano i punti opposti del globo ma che per essere legittimata avrebbe bisogno di un libretto di regole per uscire "dal garage e andare sulle strade e negli autodromi". Nessuno le vuole scrivere perché si preferisce fare come le tre scimmiette (non vedo, non sento, non parlo). Intanto però da alcune parti si usa l'auto da corsa per farsi un giretto del palazzo dietro l'angolo di casa... accontentandosi "di poco" e rinunciando a disciplinare utili strumenti investigativi.

Il fenomeno degli attacchi informatici, delle minacce alla sicurezza informatica di un Paese o delle minacce ai più semplici beni giuridici dei cittadini è molto più complesso e "globale" di come appare a chi vi si avvicina per semplice curiosità.

Gli attacchi, anche i meno pericolosi o dannosi, avvengono sempre più spesso attraverso una serie complessa di sistemi informatici situati nei Paesi più remoti e spesso meno collaborativi del mondo.

La normativa europea che vincola gli Stati membri, gli Stati firmatari e qualche altro firmatario virtuoso non basta.

Gli sforzi della comunità internazionale sono sufficienti ? Vi è una percezione corretta dei rischi ? si può fare di meglio ? Come ? Qual è l'istituzione internazionale, o forse meglio dire mondiale, che dovrebbe occuparsi del problema o almeno di una parte di esso ?

Il raggiungimento degli obiettivi di uniformità globale degli ordinamenti penali e della cooperazione giudiziaria internazionale non è solo la condizione necessaria per fronteggiare la criminalità elettronica, ma anche lo strumento per evitare che vi siano Stati individuabili come "paradisi del *cybercrime*".

C'è però ancora molto da fare e di paradisi del *cyber crime* ne rimangono ancora molti. Sono ancora troppi gli Stati che non prestano collaborazione e non si curano molto delle Convenzioni internazionali. Sono ancora troppi gli Stati che vogliono collaborazione internazionale per colpire le opposizioni interne su reati di opinione. Sono troppe le forze di polizia di molti Stati che soffrono di gelosia e non forniscono molta collaborazione.

Non si intende qui ritenere che il conflitto cibernetico tra guardie e ladri si possa risolvere a favore delle guardie visto il maggiore livello di conoscenza e capacità tecnologica dei ladri.

forse però è venuto il momento di diminuire l'enorme divario esistente tra le forze in campo (anche se troppe voci tendono a sminuire perché fa comodo tranquillizzare....) e si potrebbe **pensare a qualcosa, un'istituzione sovranazionale** per esempio, che **vincoli <u>tutti</u> gli stati -nazione** a prestare la collaborazione richiesta di volta in volta dallo Stato che ne fa richiesta.

Fino a quando esisteranno molti Stati disposti ad ospitare *server* e sistemi telematici che sfuggono alle indagini delle Autorità Giudiziarie di mezzo mondo avremo un serio problema presente sulle autostrade della Rete. Basta esserne coscienti del rischio e come si dice : infrastruttura avvisata mezza salvata.

Un certo tipo di criminalità informatica è come il ghiaccio sporco sulle strade: non lo vedi subito e quando te ne accorgi….. è troppo tardi.

Pavia, 23 novembre 2012

Avv. Stefano Aterno

Avvocato
Docente diritto penale dell'informatica
Università LUMSA di Roma
www. studioaterno.it