Competenza del Legislatore, evoluzione della tecnologia, adeguamenti normativi e introduzione ai reati informatici

Davide Coppetti – 791110

Università degli Studi di Milano – Laurea Magistrale in Informatica per la Comunicazione

Corso di Cittadinanza Digitale e Tecnocivismo

Internet e le nuove tecnologie stanno influenzando la nostra società. Il costo dell'hardware è drasticamente calato e negli ultimi anni la nostra vita sempre di più ruota attorno ad Internet. Quasi ogni azione, grazie ai nuovi strumenti sociali può essere condivisa con gli amici abbattendo così le distanze fisiche e creando un continuum tra la vita vissuta on-line e off-line

Nel nostro stato la diffusione di massa dell'informatica ebbe inizio intorno agli anni '70. I computer erano visti come macchine assai ingombranti e dall'interfaccia non troppo amichevole nei confronti dei propri utilizzatori. L'unico modo per comunicare con essa era quello di ricordarsi a memoria una grande quantità di parole "magiche" per vedere alcune ore dopo il risultato della propria interrogazione o elaborazione. L'avvento dei primi sistemi operativi dotati di interfaccia grafica facilitarono questo rapporto comunicativo con la macchina. Ogni tanto ripenso al primo computer che mio padre comprò per lavoro negli anni '90: l' IBM PS/1 un personal computer dotato di 4 MB di memoria RAM, 170 Mb di disco rigido e con il sistema operativo Windows 3.1 questo fu il mio primo approccio al mondo dell'informatica.

L'evoluzione di questa disciplina ha introdotto dei nuovi comportamenti legati al concetto di "rete". Internet non deve essere considerato come un'immensa prateria dove ogni suo "cittadino" sia libero di fare ciò che vuole bensì questo spazio digitale deve essere correttamente regolamentato in modo adeguato e che l'utente possa percepire il peso e i possibili effetti dell'azione che sta compiendo. In certe situazioni anche un banale scherzo, una goliardata, sul web potrebbe ledere la reputazione di una persona provocando ad essa grandi situazioni di disagio.

La rete può essere vista come un'immensa memoria persistente nella quale qualsiasi contenuto che in essa viene caricato gode di una vita pressoché illimitata e l'operazione di retrieval può essere eseguita anche a molti anni dalla sua pubblicazione. Strumenti quali i motori di ricerca, altri tool svolgono operazioni automatiche di indexing e caching rendendo ancora più difficile la dimenticanza offerta dal passare degli anni e non garantendo sempre al diretto interessato di poter esercitare il diritto all'oblio.

La regolamentazione di questi nuovi comportamenti ha fatto sì che anche la legislazione italiana si adeguasse inserendo un nuovo filone inerente alla disciplina informatica.

Si sa ogni campo applicativo dispone di un proprio dizionario tecnico, di una terminologia ben precisa per poter esprimere con chiarezza determinati concetti che stanno alla base della materia che si sta affrontando e in questo

caso il legislatore prima di poter legiferare è necessario che abbia maturato preventivamente una buona conoscenza dei punti cardine che ne stanno alla base

E' impossibile che il legislatore possa conoscere nei minimi dettagli qualsiasi argomento in cui viene richiesto il suo operato ma ciò dovrebbe essere una buona condotta per evitare confusione e causando successivi errori durante il giudizio degli imputati.

In giurisprudenza è nota la seguente locuzione latina *iura novit curia* traducibile in "il giudice conosce le leggi". L'operato di chi viene chiamato ad esprimere una decisione in merito a degli eventi accaduti si basa su quanto prodotto dalle parti in base a perizie, memorie e applicando nei loro confronti ciò che viene affermato dalla normativa vigente.

Non penso che dietro a tutto ciò vi sia un intenzione criminale da parte del legislatore. Ritengo più opportuno affermare che in taluni casi, essendo l'informatica una scienza la cui nascita è ancora recente non vi sia ancora l'adeguata conoscenza della materia e che questa "ignoranza" provochi degli errori nella fase preliminare della definizione legislativa creando a cascata delle conseguenze e incongruenze nella fase decisionale.

In Italia la prima volta che il mondo legislativo si interessa all'informatica è nel 1989 quando il Consiglio d'Europa emette la Raccomandazione sulla Criminalità informatica che classifica i possibili illeciti in due categorie: quelli perseguibili penalmente (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 di prodotti a semiconduttore) seguiti da un successivo elenco la cui adozione era facoltativa basata sulla discrezionalità del singolo stato. L'esigenza di essere in grado di poter punire questa tipologia di reati nacque nei primi anni '80.

Successivamente attraverso la Legge 547 del 1993 vennero introdotte alcune modifiche al Codice Penale italiano considerando anche le seguenti attività illecite: la frode informatica, la falsificazione di documenti informatici (equiparata ai tradizionali documenti cartacei), le aggressioni all'integrità dei dati ed infine le aggressioni alla riservatezza dei dati e delle comunicazioni informatiche.

Nel 2001venne stipulata la Convenzione di Budapest, un accordo tra gli stati firmatari il cui scopo base era quello di intraprendere un percorso comune di collaborazione atto allo scambio di informazioni su illeciti commessi negli stati aderenti dotandoli degli strumenti legislativi necessari per poter iniziare questa nuova tipologia investigativa. Entra in vigore a partire dal 1° luglio 2004, lo stato italiano la ratifica con la Legge del 18 marzo del 2008 n.48 inserendola così nel proprio ordinamento. La sua sottoscrizione è aperta a qualsiasi stato anche se non facente parte del Consiglio d'Europa.

Il web è una miniera di informazioni pertanto anche la Legge del 22 aprile 1941 n.633, in materia sul diritto d'autore, con l'avvento di nuovi formati di fruizioni contenuti ha dovuto adattarsi regolamentandoli

Soffermandoci proprio sulla Legge sul Diritto d'autore all' art. 71-sexies viene affermato che: "*la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale, a condizione che tale possibilità non sia in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechi ingiustificato pregiudizio ai titolari dei diritti*". Allo stesso tempo però viene negato a chi detiene una copia di un supporto regolarmente acquistato di poter eludere tali sistemi di protezione (che il produttore del bene ha diritto

di inserire per prevenire riproduzioni illeciti dei contenuti che distribuisce). In merito alla problematica emersa è da far notare la decisione presa dal Tribunale di Milano in data 14 maggio 2009 a seguito di una causa da parte di un consumatore presentata nei confronti di Universal Pictures Italia S.r.l accusandola di non poter effettuare regolare copia di backup del bene regolarmente acquistato e detenuto. L'esito finale della procedura termina con un insuccesso da parte del fruitore del bene in quanto il Giudice identifica il diritto alla copia nella seguente forma: "quale eccezione o limitazione diritto esclusivo di riproduzione che costituisce uno dei profili più significativi ed economicamente rilevanti dei diritti di utilizzazione economica delle opere protette".

Alcuni distributori di contenuti (Warner Bros, 20th Century Fox) hanno introdotto la possibilità di avere una copia digitale del prodotto regolarmente acquistato. Warner Bros tramite un'apposita area dedicata sul sito www.wbdigitalcopy.com inserendo un codice presente nella confezione permette (entro specifici limiti temporali) di effettuare il download di un file protetto. E' da far notare che il file fornito è basato su tecnologia DRM offerta da Microsoft e pertanto la fruizione dell'opera è possibile solo su computer che dispongono di sistema operativo Windows escludendo a priori gli utilizzatori di altre piattaforme quali ad es. Apple Mac OS X o Ubuntu.

Un altro caso, questa volta legato al supporto con cui vengono distribuiti i contenuti multimediali: il DVD. Esso è caratterizzato da un codice regionale. I codici disponibili sono nove di cui i primi sette suddivisi per regione geografica e i rimanenti destinati per altri usi.

Si potrebbe verificare la seguente situazione: per lavoro una persona trascorre alcuni in uno stato estero e durante la sua permanenza acquista alcuni DVD (cod.reg. 1). Terminata la propria missione fa ritorno in Italia dove è presente il codice regionale 2. L'utente non è più in grado di fruire dei film regolarnente acquistati se non attraverso applicazioni specifiche che permettono di aggirare tale ostacolo.

Altra situazione interessante è quella riguardante i modchip della Playstation: un apposito hardware il cui scopo è quello di modificare il funzionamento della console in modo da poter eseguire videogiochi illegalmente riprodotti. Per giungere ad una decisione finale si è dovuto aspettare il 2009 attraverso una sentenza della Cassazione (1243/2009) che assolve l'imputato per non aver commesso il fatto (superare una limitazione imposta dal produttore).

I concetti chiave su cui si è basato l'intero iter processuale sono stati i seguenti: individuare la natura tecnica giuridica della console in modo da stabilire ed individuare la disciplina applicabile (console o computer), riconoscere i videogiochi come una particolare categoria di software ed infine verificare l'illegittimità e lo scopo primario dell'hardware in oggetto.

La sentenza 2451/2010 emessa dalla Corte di Cassazione ci offre un altro spunto di riflessione per poter discutere di casi realmente accaduti in cui l'aspetto decisionale richiede che il giudicante sia a conoscenza di alcune nozioni incluse nella disciplina informatica. Il fatto riguarda l'attività di stalking informatico a mezzo di posta elettronica. Il giudice giunge a conclusione che l'invio di e-mail fastidiose non possa essere equiparato allo stalking telefonico in quanto la ricezione di tali comunicazioni è asincrona rispetto alla classica telefonata/SMS e non costringe l'utente a dover spegnere il computer (limitandone dei diritti) per procedere all'interruzione di tali molestie. L'email non può inoltre essere equiparata ad una telefonata anche se ad essa possono essere allegati contenuti quali file audio o di altra tipologia. Questa decisione crea un precedente non ininfluente riguardo all'invio di mail indesiderate da parte degli spammer. Anche la seguente considerazione presente nel testo della sentenza: "utilizza la rete telefonica e la rete cellulare delle bande di frequenza, ma non il telefono, né costituisce

applicazione della telefonia che consiste, invece, nella teletrasmissione, in modalità sincrona, di voci o di suoni." lascia alquanto stupiti sul provvedimento emanato dal giudice. Sia l'operazione di connessione ad Internet che una telefonata sfruttano la frequenze operative di un telefono cellulare e non si comprende perché tale modalità di disturbo non venga considerata tale.

Un blog può essere equiparato ad una testata giornalistica?

La Sentenze della Cassazione del 16 luglio 2010 e del 29 novembre 2011 hanno deciso che il direttore di una testata online non risponde necessariamente per omesso controllo ex art. 57 c.p. Nei casi qui citati chi ha intentato la causa voleva accusare il responsabile del sito internet per non aver provveduto con celerità alla rimozione di contenuti diffamatori.

La sentenza del novembre 2011 afferma che :"La diffusione del contenuto del periodico on line avviene non mediante la distribuzione del supporto fisico in cui è inserito quanto piuttosto attraverso la visualizzazione del suo contenuto attraverso i terminali collegati alla rete."

Nel testo emesso dal Giudice vengono anche specificati i vincoli per poter considerare quando si è in presenza di diffusione a mezzo stampa di determinate notizie:

"Affinchè possa parlarsi di stampa in seno giuridico occorrono due condizioni:

a) che vi sia una riproduzione tipografica;

b) che il prodotto di tale attività (quella tipografica) sia destinato alla pubblicazione attraverso una effettiva distribuzione tra il pubblico."

In contrasto a queste due decisioni vi è quella emessa dal Tribunale di Modica nei confronti del giornalista Carlo Ruta condannato per aver violato l'art.16 della Legge dell' 8 febbraio 1948 n.47 (uno dei rari casi di applicazione di questa vecchia norma) per non aver registrato il proprio blog come testata giornalistica presso il Tribunale ed è stato accusato di stampa clandestina anche se la propria attività di aggiornamento del blog, data la cadenza temporale con cui veniva effettuata, non poteva essere paragonata a quella di un quotidiano.

Internet come si è affermato precedentemente è un network a cui ogni giorno si connettono milioni di persone. Il nostro unico dato di riconoscimento al suo interno è l'indirizzo IP un numero organizzato in quattro blocchi di tre cifre che viene assegnato temporaneamente in modo univoco ad un cliente al momento della connessione e rilasciato al termine della propria sessione di navigazione.

Questo numero ci identifica come se fosse la targa del nostro autoveicolo? La risposta può variare a seconda del punto di vista della persona a cui viene posto tale quesito.

In merito alla questione è utile parlare di un caso accaduto nel nostro Paese qualche anno fa tra la Peppermint Logistep e alcuni clienti di alcuni ISP (uno di questi Wind-Infostrada) che offrono servizi di connettività nel territorio italiano. Alcuni cittadini si videro recapitare al proprio domicilio una lettera da parte dello Studio Legale Mahlknecht & Rottensteiner in cui veniva richiesto loro il pagamento di 330,00 € al fine di risolvere in via bonaria la controversia per aver scaricato in modo illecito materiale coperto da diritto d'autore.

Ci furono tre sentenze (l'unica a favore della casa discografica è la prima nella quale si affermava che un indirizzo IP non può essere considerato un dato protetto dalla norma sulla privacy). Le ultime due decisioni

ribaltarono negando ai vari ISP di fornire alla casa discografica Peppermint le anagrafiche dei propri clienti in quanto l'acquisizione dell'indirizzo IP era avvenuta in modo illecito attraverso un software sviluppato dalla società svizzera Logistep. In questo procedimento il codice della privacy ha prevalso sugli illeciti commessi in merito alla violazione della legge su diritto d'autore.

Nel caso di una connessione ad Internet tramite un router Wi-Fi a chi può essere attribuita la responsabilità di determinate azioni? Supponiamo di avere due computer connessi alla nostra rete casalinga, entrambi accesi. Ad ogni postazione viene assegnato un indirizzo privato interno alla rete ma entrambi gli elaboratori saranno affacciati al network di Internet con il medesimo indirizzo IP. Analizzando il log del provider non sarà possibile distinguere i due flussi telematici ma sarà possibile affermare che la connessione è pervenuta da una determinata utenza. Solo attraverso il router di casa sarà possibile testimoniare che il traffico sia stato generato da due computer differenti.

Una recente sentenza emessa nel Regno Unito afferma che non possa essere considerato responsabile il titolare di una connessione ad Internet per illeciti commessi attraverso il proprio router in quanto l'indirizzo IP identifica una connessione ad Internet e non in modo univoco la persona.

Situazione differente si ha nel caso si installi una rete Wi-Fi e quest'ultima non venga protetta in modo adeguato con meccanismi che vietino la connessione di terzi. In questo caso la responsabilità ricade sull'utente. La legge non ammette ignoranza. In certi casi la connessione alla rete non protetta potrebbe avvenire in modo automatico dall'utente senza che quest'ultimo se ne renda conto. Basterebbe possedere un pc dotato di scheda wireless per poter essere accusati di accesso abusivo ad una rete informatica. Non avrebbe senso una considerazione del genere. Il fatto va punito quando vi è un'evidenza della sua intenzionalità

Negli ultimi anni la diffusione delle reti wireless in Italia ha subito dei rallentamenti anche per l'entrata in vigore del Decreto Pisanu (D.L 144/2005 poi convertito in Legge 155/2005 e recentemente abolito) introdotto per contrastare possibili reati terroristici attraverso la rete. Attraverso questo metodo di identificazione non so quanti terroristi siano stati arrestati ma penso che la cifra sia prossima allo zero. Piuttosto che farsi identificare anche con documenti falsi penso che per chi ha intenzione di commettere un reato tramite Internet la procedura più semplice sia quello di agganciarsi ad una delle tante reti wireless aperte che non fanno uso di tecniche di protezione.

L'assenza di chiavi (sia WEP/WPA/WPA2) permette a chiunque di potersi collegare alla nostra connessione apparendo sulla rete con la nostra identità. Il malintenzionato di turno potrebbe non solo sfruttare il collegamento per la semplice navigazione ma anche per intercettare le nostre comunicazioni simulando successivamente la nostra identità. Si ricorda che l'accesso abusivo ad un sistema informatico è un reato punibile con la reclusione.

Analizziamo ora un altro aspetto interessante offerto sempre più dai service provider in questi ultimi anni: l'identificazione tramite SMS. Questa pratica dovrebbe garantire che la persona che sta effettuando la registrazione abbia la titolarità all'uso degli stessi. Tale pratica più che garantire l'identità ha il solo scopo di verificare che il registrante abbia con sé il cellulare per poter inserire il codice di conferma ricevuto via SMS. Il matching tra intestatario del numero e i dati inseriti nel modulo on-line non può essere eseguito in tempo reale. Alcuni servizi ad esempio il servizio wireless presente sui treni Freccia Rossa o la connessione agli hotspot dei fast-food della catena McDonald's usano questo sistema per identificare gli utenti dei propri servizi.

Trovo più utile e più sicuro anche se certamente più scomodo procedere con una iniziale procedura on-line che va conclusa recandosi fisicamente presso un ufficio locale del fornitore di servizi.

Ogni SIM del cellulare è intestata realmente ad una persona (fisica/giuridica)? Navigando in rete ho trovato una notizia relativa ad un distributore automatico di SIM per cellulari presente all'aeroporto di Stansted di Londra. Con 11,5 sterline è possibile acquistare una qualsiasi scheda di un operatore a scelta. Non ho trovato ulteriori notizie in merito all'argomento ma se tale procedura funziona realmente i problemi legati all'identificazione non sono pochi. In Italia l'acquisto di un numero di cellulare è preceduta da una procedura che prevede l'identificazione dell'utente che sta richiedendo l'abilitazione a dei servizi. Senza troppa difficoltà in rete è possibile trovare lettori e scrittori di SIM card in grado di clonarne contenuto realizzando copie perfette a quelle fornite dal proprio operatore.

Skype e alcuni nuovi servizi di telefonia tramite Internet che sfruttano il VoIP prevedono la possibilità di richiedere un numero geografico su cui poter ricevere telefonate effettuate dai tradizionali telefoni. Questo secondo me ha creato una grande confusione in questo già variegato mercato offrendo la possibilità ad un cittadino ad es. di Bolzano di richiedere una numero telefonico appartenente geograficamente alla provincia di Venezia con prefisso 041 ricevendo però tale telefonata mentre si trova in un albergo a Capri. Alcuni gestori permettono inoltre di impostare direttamente il numero da visualizzare al chiamante per farsi riconoscere al momento dell'instaurazione della telefonata. Alcuni gruppi criminali organizzati hanno sfruttato tale problematica di sicurezza per camuffare l'identità del chiamante e commettere il reato di Vishing sottraendo agli ignari clienti (credendo di essere contattati dalla propria banca/operatore telefonico) importanti informazioni per l'accesso ai loro conti correnti oppure a importanti informazioni per l'esecuzione di reati di sostituzione di persona. Alcune organizzazioni a stampo mafioso potrebbero sfruttare le nuove tecnologie per la conduzione di traffici illeciti di droga o poter effettuare operazioni di riciclaggio senza poter essere intercettate dalle forze di polizia.

Il prefisso telefonico sta perdendo un po' il suo significato per cui era stato progettato tanto che recentemente sono nate una nuova tipologia di numeri telefonici caratterizzati dalla decade 5 offerti da alcuni operatori, uno tra questi è Tiscali che con il servizio Indoona permette richiedere un numero nomade caratterizzato dalla decade 5XYZABC. Esso non appartiene ad una determinata area geografica.

Skype durante la creazione dell'account non richiede particolari informazioni: nome, cognome (che possono essere facilmente inventati), un nickname a discrezione dell'utente ed una casella di posta elettronica (esistono quelle temporanee usa e getta che non richiedono nemmeno la registrazione). Per quale motivo Skype non dovrebbe essere equiparato ad un classico servizio di telefonia obbligando quindi ad identificare l'utente?

Una delle recenti novità introdotte in Italia è l'introduzione e l'utilizzo di posta elettronica certificata (pioniere di tale iniziativa è stato il l'ex Ministro Brunetta) tra il cittadino e le Pubbliche Amministrazioni. Questa nuova forma di posta elettronica avrebbe dovuto sensibilmente ridurre l'onere cartaceo a carico del servizio postale nazionale ma ciò non si è verificato.

Uno dei problemi legati a questo sistema è la mancata interoperabilità con i sistemi di posta elettronica esteri. Lo standard è riconosciuto solo a livello nazionale e pertanto non vi è la garanzia che la propria comunicazione arrivi correttamente a destinazione.

Anche se tale indirizzo di posta elettronica prevede una fase di registrazione non è detto che il suo utilizzatore coincida con chi ne effettua la richiesta basti pensare ad un software in grado di gestire più account di posta in contemporaneamente. Il poter accedere a tale software permette di inoltrare richieste come se si fosse il

proprietario della casella postale e non garantisce pertanto l'univocità del mittente e la titolarità dei relativi allegati ad essa connessi.

Un'identificazione tramite smartcard è decisamente più sicura perché oltre a disporre fisicamente della tessera è necessario essere a conoscenza del pin per il suo utilizzo. La Regione Lombardia offre la possibilità di utilizzare la CRS (Carta Regionale dei Servizi) anche per firmare i documenti da inviare tramite la posta elettronica certificata alle amministrazione oltre che a garantire l'accesso a particolari servizi. Poche righe più in alto si è affermato che tale tecnologia risulta essere più sicura ma non da poter escludere il titolare da possibili truffe nei propri confronti. In un recente servizio andato in onda al TG1 delle 20.00 del 26 marzo 2012 si è parlato di una frode nei confronti di un imprenditore romano a cui, grazie la complicità di un'agenzia di servizi, è stata clonata la propria smartcard con la quale veniva gestita l'intera operatività dell'azienda. Grazie ad essa è stato possibile eseguire transazioni finanziarie a nome del titolare a cui è stato sottratto l'intero patrimonio societario che si è accorto per caso di quanto gli fosse capitato grazie ad una verifica effettuata alla Camera di Commercio. Il Col. Rapetto ha affermato che il fenomeno del furto d'identità è in continua espansione. Il nucleo investigativo della Guardia di Finanza GAT in questa operazione ha individuato i seguenti illeciti: sostituzione di persona, furto identità, falso in atto pubblico e scritture private e frode informatica ascritti nei confronti di chi ha compiuto questi illeciti

L'uso della crittografia è una tra le tecniche più sicure per poter trasmettere documenti senza che la propria comunicazione possa essere intercettata non essendo a conoscenza della chiave usata per la cifratura. Tale attività in alcuni stati è considerata un'operazione non lecita in quanto potrebbe essere usata per usi non

Negli Stati Uniti vige il divieto per l'esportazione di prodotti che fanno uso di strumenti crittografici. Il caso Zimmermann ha suscitato interesse alcuni anni fa. Zimmermann è l'autore del software PGP (Pretty Good Privacy) un software crittografico. L'esportazione del software al di fuori degli USA è stata possibile stampando i sorgenti del software e procedendo al loro invio tramite il tradizionale sistema postale. Una volta ricevuti sono stati ricopiati è l'applicazione originale è stata ricompilata e distribuita attraverso la rete

Alcune delle problematiche emerse da questa trattazione (ve ne sono altre ma che in questa sede non vengono menzionate), la diffusione dei pc e dell'accesso alla rete nelle abitazioni hanno fatto sì che vi fosse un incremento di tali reati ed è stati riconosciuto che questi ultimi fossero equiparati ai tradizionali illeciti perseguendoli. Il nostro ordinamento li classifica in due categorie: *puri* comprende tutte le figure di illecito indicate nelle leggi precedentemente menzionate (sistema informatico tutelato come bene da attacchi e truffe) e spuri i reati comuni con l'ausilio di sistemi informatici (ad.es l'operazione di diffamazione).

Possono essere raggruppati nelle seguenti categorie di intervento: frodi informatiche, falsificazioni, integrità dei dati e dei sistemi informatici, riservatezza dei dati e delle comunicazioni informatiche.

I riferimenti agli articoli qui sotto riportati sono relativi al Codice Penale italiano

L'art. 491 bis è relativo alla falsificazione nei documenti informatici, l'art. 635 bis si pone l'obiettivo di chiarire cosa è il "danneggiamento di sistemi informatici e telematici", l' art.420 specifica cosa si intende per "attentato ad impianti di pubblica utilità"

L'art. 615 ter punisce l'accesso non autorizzato ad un sistema informatico, il successio 615 quater vieta la diffusione a persone non autorizzate delle credenziali per l'accesso ad un sistema ed infine l' art. 615-quinquies

tratta in merito alla: “Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico”. Qui si apre un’ampia categoria di software partendo dai dialer per giungere ai malware.

L’art 617 e alcuni dei seguenti perseguono chi illecitamente intercetta, impedisce o interrompe illecitamente comunicazioni informatiche o telematiche.

Anche chi divulga informazioni segrete senza le opportune motivazioni viene condannato dalla legge.

E’ importante evidenziare che alcuni dei reati sono punibili anche mediante la reclusione mentre in altri casi l’estinzione della pena inflitta è effettuata tramite il pagamento di una sanzione pecuniaria.

Le forze dell’Ordine impegnate nella repressione degli illeciti sopra menzionati sono il GAT un nucleo appartenente alla Guardia di Finanza diretto dal Colonnello Umberto Rapetto specializzato a contrastare le frodi telematiche e una sezione della Polizia di Stato il nucleo della Polizia Postale e delle Telecomunicazioni presente in molti uffici dislocati nell’intero territorio nazionale.

BIBLIOGRAFIA DI RIFERIMENTO ARTICOLO

[1] Indovina Barbara, Reati Informatici e Prova Digitale, 2011 - http://www.giustizia.abruzzo.it/formazione_magistrati_onorari.aspx?file_allegato=558

[2] ICTLEX: Diritto, politica, cultura della rete (possibili rif. a materiale presente nella categoria Giurisprudenza Italiana - Sentenze) - http://www.ictlex.net/?cat=20

[3] Luberto Mario, di Mario Luberto (2008) I reati informatici contro il diritto alla privacy. La tutela fornita dal D.LG. N. 196 del 2003 e dal Codice Penale – Fonte Banca Dati De Jure – Ed. Giuffrè

[4] Sartor Giovanni, (1998) I linguaggi (e i sistemi informatici): un vincolo per il giurista? - Riv. notariato 1998, 05, 825 – Fonte Banca Dati De Jure – Ed. Giuffrè

[5] Rossello Carlo , (2006) (Dottrina) La governance di Internet tra diritto statuale, autodisciplina, soft law e lex mercatoria – Fonte Banca Dati De Jure – Ed. Giuffrè

[6] Rodriguez Simona, (2011) – L'amministrazione digitale e il nuovo codice: vera rivoluzione o esagerato ottimismo – Fonte Banca Dati De Jure – Ed. Giuffrè

[7] Ziccardi Giovanni – () – Crittografia e diritto - www.ziccardi.org/docs/crittografia.pdf

[8] Butta Mattia – (2009) – Decreto Pisanu ed identificazione tramite SMS – http://www.butta.org/?p=593

[9] Studio Legale Finocchiaro - (2011) - Regno Unito: gli indirizzi IP non identificano persone - http://www.blogstudiolegalefinocchiaro.it/diritto-dautore-e-copyright/regno-unito-gli-indirizzi-ip-non-identificano-persone/

[10] Fioriglio Gianluigi - (2004) – Temi di Informatica Giuridica – http://www.informaticagiuridica.com/temiig/fioriglio-temi_di_informatica_giuridica.pdf

[11] Piva Antonio, D'Agostini David – (2004) - ICT e Diritto – Riv. Mondo Digitale n.1

[12] Vizzarro Danilo - (2006) – I reati informatici nell'ordinamento italiano – www.danilovizzarro.it

[13] Ministero per l'Innovazione e le Tecnologie – (2002) – Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura

[14] ADOC - (2011) – Truffe telematiche: Attenti al vishing! – http://www.adoc.org/notizie/5460/truffe-telematiche-attenti-al-vishing

[15] Bassoli Elena – () – Libro VI Produzione normativa e tecnologie dell'informazione

[16] Giustizia Penale: diritto penale, dell'informatica e delle nuove tecnologie – (2011) – post http://www.giustiziapenale.it/?p=43

[17] Corriere del Mezzogiorno – (2011) – Blog equiparato a stampa clandestina. Confermata in appello la condanna a Ruta - http://corrieredelmezzogiorno.corriere.it/napoli/notizie/cronaca/2011/26-maggio-2011/blog-equiparato-stampa-clandestinaconfermata-appello-condanna-ruta-190729911360.shtml

[18] Pomhey Claudio – (2011) – Fai scrivere il computer da solo con digitazione automatica del testo - http://www.navigaweb.net/2011/03/fai-scrivere-il-computer-da-solo-con.html

[19] CNIPA – () – Raccolta normativa ICT - http://archivio.cnipa.gov.it/site/it-IT/Normativa/Raccolta_normativa_ICT/

[20] Di Corinto A, Tozzi - (2002) - Hacktivism. La libertà nelle maglie della rete - http://www.hackerart.org/storia/hacktivism/3_4_4.htm (PGP Zimmermann)

[21] Ventura Maurio - - Reati Informatici, Codice Penale e Regolamentazione Comunitaria

[22] Greco Angelo – 2010 - Stampa su internet: Bisogna registrare in Tribunale un blog? - http://www.loudvision.it/rubriche-stampa-su-internet-bisogna-registrare-in-tribunale-un-blog--970.html

[23] Warner Bros – Digital Copy - http://www.wbdigitalcopy.com/support/#GetStarted&discid=C17B0A47-9E57-451c-88F3-E67A84C78BA1&country=it

Mi scuso a priori con chi per dimenticanza non è stato incluso nel presente elenco.