diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Tecniche di indagine della Polizia Postale nell'ambito dei reati informatici e nella pedopornografia on line

Autore: Redazione
In: Diritto penale

Di Monica Delle Donne

I mezzi di comunicazione, le innovazioni tecnologiche, l'informatizzazione sono il risultato del progresso scientifico e sono, altresì, il sintomo di una società in evoluzione, che cerca sempre più di "semplificare" il proprio modo di vivere.

Ma se, da un lato, l'individuo gode dei benefici che questi strumenti gli offrono, si deve, dall'altra parte, convenire che l'evoluzione tecnologica ha comportato il proliferare sia di nuovi metodi di commissioni di reati, sia la nascita di nuove fattispecie criminose, attuate mediante la Rete delle reti.

Tutto questo comporta necessariamente una rivisitazione, non solo delle norme di diritto penale e di procedura penale, ma, altresì, delle tipologie e delle metodologie su cui si basavano le tradizionali indagini investigative attuate dalle Forze dell'Ordine.

Non che non esistano più i vecchi pedinamenti, o gli appostamenti, o le intercettazioni o le infiltrazioni di personale nel contesto criminoso (il cd. agente provocatore), ma tali figure investigative sono diventate peculiari nell'attività del "poliziotto virtuale"[2].

Le crescenti specializzazioni dei criminali informatici hanno reso indispensabile la creazione di un nucleo di esperti investigatori capaci di percorrere la grande autostrada di Internet, dove non si trovano più autoveicoli ma bit, "guidati" da alcuni utenti recalcitranti - che pensano che la Rete sia un Far West, senza regole – e dove vi sono gli "autovelox umani" che, invece, tendono a fotografare le connessioni illecite per snidare i malfattori.

POLIZIA POSTALE: LA STORIA, LA STRUTTURA, I COMPITI.

Il compito di "sceriffo informatico" è stato affidato alla Polizia Postale e delle Comunicazioni, corpo specializzato della Polizia di Stato, che era nato nel 1981 per tutelare le attività collegate alle Poste e ai servizi di telecomunicazione.

Per far fronte alle nuove tecnologie, tale organismo si evolve negli anni novanta, per poi concretizzarsi nella nascita del NOPT (Nucleo Operativo di Polizia delle Telecomunicazioni).

Diritto & Diritti ISSN 1127-8579

Il processo di modernizzazione e di riorganizzazione del servizio sfocia, poi, nel Decreto del Ministero dell'Interno del 31 marzo 1998 che ha istituito l'attuale Servizio di Polizia Postale e delle Comunicazioni[3].

Esso consta di 2 divisioni, 19 compartimenti e 76 sezioni che svolgono i loro compiti istituzionali su tutto il territorio dello Stato: una sezione è distaccata presso l'Autorità Garante per le Comunicazioni.

La 1° divisione ha competenze di gestione degli archivi, del personale, del coordinamento degli uffici interni e periferici, della pianificazione delle attività di monitoraggio e controllo dei servizi Audiotel e Videotel; cura, altresì, i rapporti con gli organismi sindacali e le Poste italiane, e si occupa anche dell'inquinamento elettromagnetico.

È la 2° Divisione che ha, invece, competenze investigative: all'interno di essa sono presenti 4 Sezioni con diversi ambiti specifici:

Sezione I: Attacchi a sistemi informatici;

Sezione II: Tutela del copyright:

Sezione III: Pedofilia;

Sezione IV: E-commerce[4].

Gli agenti di questo corpo speciale sono reclutati fra coloro che, durante i corsi di addestramento, dimostrano di possedere delle attitudini e delle conoscenze specifiche: sono maghi dell'informatica, esperti di tecnologia digitale che affiancano a tali doti materiali anche la spiritualità di Sherlock Homes, l'indomabile investigatore sempre proteso alla ricerca delle prove dei reati.

Peculiari sono, altresì, gli ambiti di intervento di questo organismo: dalla prevenzione e repressione dei crimini postali e informatici, al controllo delle licenze radio-amatoriali, degli apparati, degli impianti, delle emittenti radio e televisive; dal controllo degli esercizi che commercializzano materiali o apparecchiature di telecomunicazione che devono essere marcate o omologate, alla verifica del rispetto sulla normativa sulla privacy, con particolare riferimento alle banche dati, anche per la individuazione di quelle abusive.

Inoltre, la L. 3 agosto 1998, n. 269, "Norme contro lo sfruttamento della prostituzione minorile, della pornografia minorile e del turismo sessuale a danno di minori quali nuove forme di riduzione in schiavitù", assegna la competenza specifica alla repressione di tali delitti alla Polizia Postale.

Ad ogni buon conto, l'attività di contrasto al crimine informatico necessita di analisi approfondite dei fenomeni che si succedono in Rete per ricercare e sviluppare nuove strategie investigative in materia di computer crime e per tracciare i profili psicologici e comportamentali degli autori dei reati.

Diritto & Diritti ISSN 1127-8579

A questo fine, è stata creata l'U.A.C.I. (Unità di Analisi del Crimine Informatico), diretta da uno Psicologo della Polizia di Stato, esperto in Criminologia, i cui componenti sono dotati di capacità specifiche in ambito tecnologico, psicologico e giuridico.

L'U.A.C.I. si avvale al suo interno di un Comitato scientifico di Consulenza della Polizia Postale e delle Comunicazioni, composto da personaggi del mondo universitario e dell'I.C.T., che offrono la loro consulenza nella realizzazione di progetti e in alcune sperimentazioni scientifiche[5].

Altro problema che si pone nella lotta della repressione di tali tipologie di reati è che i fenomeni criminali, prodotti in questo campo, sono connotati dalla rapidità e dalla trasnazionalità delle condotte.

Infatti, sono ampie le possibilità di accesso a sistemi telematici ubicati in Paesi diversi da quello in cui si trova il criminale.

Ciò ha comportato lo sviluppo di proficui rapporti collaborativi con le omologhe realtà investigative presenti in altri Stati per la veicolazione e lo scambio delle informazioni relative alle tecnologie emergenti e alle nuove metodologie di operazioni[6] e la partecipazione con propri rappresentanti ai lavori di consessi internazionali quali G8, UE, EUROPOL, INTERPOL, Consiglio d'Europa[7].

LA NUVA FIGURA DEL CRIMINALE ON LINE

Ciò che, in primo luogo, ha impegnato le Forze dell'Ordine è stato lo studio di forme criminali nuove, rispetto a quelle tradizionali, che hanno comportato la rivisitazione delle convenzionali indagini in termini di psicologia criminale.

Da ricerche approfondite effettuate dal Dott. Marco Strano, Dirigente Psicologo dell'UACI, è risultato che il criminale informatico non è un teppista della strada, non è il mafioso tradizionale, non è il truffatore incallito.

Tale figura non rientra più nei paradigmi convenzionali che la società aveva fatto propri: la tipologia di criminale virtuale comprende al suo interno persone cd. "normali", con un livello sociale e culturale medio-alto, tendenzialmente non violente, che hanno una ridotta percezione del crimine, dei danni che potrebbero causare e della possibilità di essere scoperti e denunciati.

Potrebbe essere il bravo ragazzo della porta accanto, lo studente modello, il dipendente timido: tutte tipologie di persone che non sarebbero mai in grado di fare del male se avessero la loro vittima davanti: vengono meno i freni inibitori, in quanto tra il soggetto agente e la vittima si interpone in computer, attuandosi, in tal caso, la c.d. "spersonalizzazione" nel reato.

Tutto questo si realizza, quindi, perché il soggetto agente ha una minore percezione dell'illegalità e dei danni che il proprio comportamento illecito può provocare, in quanto molti crimini informatici non sono

Diritto & Diritti ISSN 1127-8579

percepiti come tali dalla maggior parte dei criminali.

Del resto, la stima, da parte dell' autore degli illeciti, della possibilità di essere scoperto e denunciato, è molto bassa: non ci si rende conto che la Rete è costantemente monitorata dalle Forze dell'Ordine[8].

La delineazione di tali nuovi profili di criminali comporta una rivisitazione e una progettazione di nuove strategie investigative e di prevenzione, anche con riferimento alle varie tipologie di reati commesse con gli strumenti informatici.

Pedopornografia on line, truffe e frodi telematiche, hacking, attacchi informatici, produzioni di virus, worm, malware, spamming, net-strike, stalking, pirateria satellitare, informazioni illegali on line, violazione della privacy: questi sono solo alcuni dei reati perpetrati per via telematica e che la Polizia Postale si trova ogni giorno a dover fronteggiare, attuando tecniche investigative sempre più sofisticate.

I REATI INFORMATICI

L'infinità di dati, informazioni, password transitanti su Internet costituisce l'humus nel quale proliferano e si determinano gli scenari che fanno da sfondo ai crimini informatici.

Di contro, i potenti mezzi hardware e software che sono utilizzati dalla Polizia Postale nello svolgimento delle indagini investigative.

I "poliziotti virtuali" si confrontano con insiders, hackers, crackers, terroristi, pedofili, truffatori telematici, personaggi spesso lontani dalle logiche criminali tradizionali.

Cambia anche la scena del delitto: criminale e vittima sono fisicamente lontani e spesso, addirittura, il crimine viene commesso da un Paese straniero.

Vengono, altresì, meno i rapporti personali, in quanto l'indagine è filtrata dal computer e l'investigatore non ha riferimenti concreti, in quanto manca il face to face con l'autore del reato.

Del resto, il computer può essere, non solo lo strumento attraverso il quale si realizza la commissione di un reato, ma anche il bersaglio dello stesso: in questo caso lo scopo del malintenzionato è quello di sottrarre o distruggere le informazioni contenute nella memoria dello stesso personal computer: è quello che accade con gli hackers, i crackers o gli insiders.

Il computer può, quindi, anche essere utilizzato quale mezzo per la perpetrazione un delitto, come accade con le truffe o le frodi o i furti, anche quelli di identità (c.d. Identity Theft).

La Rete può essere utilizzata anche in modo lecito da soggetti criminali o terroristi che ne sfruttano le potenzialità per migliorare l'efficacia della propria azione nel riciclaggio, nello scambio di informazioni,

Diritto & Diritti ISSN 1127-8579

evitando, in tal modo, il contatto diretto.

Altro delitto è quello della violazione della privacy con l'invio tramite e-mail di comunicazioni commerciali non richieste (spamming) o inserendo cookies all'insaputa del navigatore che ne tracciano le visite sul WEB e, di conseguenza, i gusti.

Si è portati erroneamente a credere che nel mondo di Internet vigano le regole dell'anonimato ed omologazione, caratteristiche che potrebbero facilitare l'occultamento delle prove e delle persone[9].

Tale circostanza è avallata anche dalla presenza del proxy server, strumento principe della navigazione anonima che protegge l'identità di rete dei suoi utilizzatori, presentando indirizzi IP contraffatti o mascherati.

Ciò non corrisponde a realtà: basti pensare al caso "www.svanityfair.com", il sito di un giornalista italiano che, sfruttando dei proxy di anonimizzazione e pubblicando le proprie pagine in Australia - rendendole accessibili tramite un redirect dagli USA - aggiornava detto sito con le conseguenze - in base alle accuse mosse nei suoi confronti - di macchiarsi di diffamazione in diverse occasioni nei confronti di nomi noti della politica, dello sport e dello spettacolo[10].

In questa occasione, l'attività di indagine era stata svolta dalla Guardia di Finanza ma è interessante, comunque, per spiegare le potenzialità delle tecniche e degli strumenti in dotazione alle Forze dell'Ordine per la repressione dei reati commessi on line.

Del resto, tale risultato positivo potrebbe spingere i "poliziotti virtuali" ad una più ampia adozione di siffatte procedure.

Nell'attività di repressione dei reati informatici ha avuto un'importanza vitale la collaborazione – in mancanza di una specifica disciplina - che si è instaurata tra l'Autorità Giudiziaria e i gestori dei servizi di telecomunicazione, degli Internet Service Provider, dei fornitori di connettività e degli altri operatori della Rete.

Tale collaborazione permetteva di acquisire le fonti di prova anche mediante la conservazione dei Files di Log.

Infatti, tra le altre, una complessa attività investigativa, scaturita dalla denuncia di alcuni impiegati di un istituto di credito che opera on line, ha permesso di individuare, attraverso vaste indagini condotte con approfondite analisi dei files di log relativi al sistema di accesso ai conti correnti interessati, all'individuazione di quattro persone che sono state denunciate all'Autorità competente[11].

LA PEDOPORNOGRAFIA ON LINE

Diritto & Diritti ISSN 1127-8579

La turpe piaga della pornografia minorile è, purtroppo, presente anche in Internet.

Da una recente indagine, portata avanti dall'ICAA con Symantec, nell'ambito del progetto "Pollicino nella Rete" sono scaturiti dei risultati alquanto preoccupanti.

Il 13% dei bambini intervistati ha fatto dei discorsi con risvolti sessuali on line, mantenendo il più delle volte il segreto con i propri genitori o perché se ne vergognavano o perché ritenevano di non poter essere da loro compresi[12].

Per combattere tale fenomeno, l'art. 14, comma 2, Legge 3 agosto 1998, n. 269 ha demandato alla competenza esclusiva della Polizia delle Telecomunicazioni la possibilità di attivare siti civetta su Internet, realizzare o gestire aree di comunicazione o di scambio tramite chat o e-mail, con la partecipazione alle stesse di agenti sotto copertura.

La Polizia Postale è l'unica delegata all'acquisto simulato di materiale[13], per scoprire chi realmente si nasconde anche dietro un sito contenete immagini pedo pornografiche.

In tal caso, gli agenti aprono un conto corrente intestato ad una persona fittizia, facendosi poi rilasciare una carta di credito con la quale acquistano il materiale illecito.

Individuato il conto corrente incriminato ed acquisiti i files di log, le Forze dell'Ordine sono in grado di individuare il beneficiario delle transazioni effettuate[14].

Anche l'apertura di siti civetta è un espediente per scoprire i pedofili nella Rete.

In tal caso esiste un software che è in grado di simulare perfettamente l'identità di un bambino, con le caratteristiche linguistiche e comportamentali dei minori ricompresi tra gli 8 e i 13 anni.

"Creato" il bambino virtuale da immettere in Rete, come esca ad eventuali molestie e/o tentativi di adescamento, si sono stabiliti gli ambiti delle indagini e le variabili da tenere sotto controllo.

Si è, infatti, convenuto un comportamento costante che il bambino deve tenere nei vari collegamenti, anche in presenza di molestie verbali: in tal caso il suo atteggiamento è caratterizzato da curiosità non eccessiva per continuare la conversazione[15].

TECNICHE DI INDAGINE

Quindi, nel momento in cui parte la denuncia/querela del reato, viene avviata la vera e propria attività investigativa, analizzando e incrociando i dati acquisiti.

I files di log devono essere forniti dagli utenti attaccati al fine di estrapolare gli indirizzi IP che hanno

Diritto & Diritti ISSN 1127-8579

provocato l'assalto, per i quali saranno richiesti gli intestatari e i caller id al provider fornitore del servizio.

Se gli assegnatari di tali IP sono provider italiani, il reperimento delle informazioni avviene in modo agevole mediante il decreto di acquisizione dei files di log notificato allo stesso provider. Se gli IP sono stati assegnati da fornitori di servizio Internet situati all'estero, allora tale attività verrà demandata all'INTERPOL.

Altre tecniche di indagine sono:

l'intercettazione di comunicazioni informatiche e telematiche, previste dall'art. 266 bis c.p.p. così come introdotto dalla L. 547/1993, prevista per i procedimenti che si riferiscono ai reati indicati all'art. 266 c.p.p. a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche e per il reato previsto dall'art. 600 ter c.p., così come indicato dalla L. 269/98.

Il P.M., ex art. 267 c.p.p., richiede al GIP l'autorizzazione a disporre le operazioni di intercettazioni telematiche, che viene concessa con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini.

La durata dell'autorizzazione è di 15 giorni, con la possibilità di proroga da parte del GIP con decreto motivato per periodi successivi di 15 giorni qualora permangono contingenti esigenze investigative;

duplicazione delle caselle di posta elettronica utilizzate dall'indagato. Questa è una forma particolare di intercettazione telematica e, pertanto, è sottoposta al nulla osta del GIP, il quale emetterà un apposito decreto, valido per la durata di 15 giorni con la possibilità di proroga.

Tale attività permetterà l'acquisizione della posta in giacenza, in arrivo e trasmessa dal giorno di inizio delle operazioni.

Perquisizione, successivo sequestro probatorio ex art. 253 c.p.p. e perizia del materiale sequestrato[16].

Per spiegare tale attività, è necessario approfondire il concetto di corpo del reato e di cose pertinenti al reato.

Infatti, il comma 2 dell'art. 253 codice di rito indica quale corpo del reato non solo le cose sulle quali o mediante le quali il reato è stato commesso ma anche quelle che ne costituiscono il prodotto, il profitto o il prezzo[17], comportando, quindi, la non conciliabilità della definizione materiale data dal legislatore con la natura immateriale delle tracce informatiche, di guisa che non se ne può prospettare il furto ma solo la duplicazione abusiva.

La giurisprudenza, dal suo canto, non ha dato risposte esaurienti sul tema, riconoscendo alternativamente

Diritto & Diritti ISSN 1127-8579

la natura del computer di corpo di reato, o di mezzo attraverso il quale si è perpetrato il reato, o di cosa pertinente al reato, il cui esame potrebbe dimostrare il fatto criminoso nel suo complesso.

Ma tale vincolo pertinenziale non sussiste in via sistematica tra il reato e l'intero supporto informatico, in quanto si avrebbe una arbitraria estensione del vincolo a tutti i dati e i programmi presenti sull'hard disk, anche quelli di contenuto lecito[18].

Ne consegue la necessità di valutare il ruolo del computer nell'attività illecita perché il sequestro possa essere motivato.

Del resto, il ricorso a questo mezzo di ricerca della prova si è spesso rivelato un boomerang per l'Autorità procedente, in quanto, a volte, è risultato lesivo dei diritti dei destinatari del provvedimento, così da essere caducato in sede di riesame[19].

Il computer può, quindi, essere solo il contenitore dentro il quale possono essere immagazzinate le prove del crimine.

In questo caso, non sarà necessaria un'azione di sequestro, ma sarà sufficiente, secondo alcuni, una masterizzazione delle tracce di reato da eseguirsi tramite una ispezione delegata ex art. 246 c.p.p. che, essendo atto irripetibile, necessita della cristallizzazione della procedura seguita in apposito verbale che, però, spesso contiene un'indicazione troppo generica dei beni sottoposti a vincolo, nulla dicendo sul contenuto dei dati, vero oggetto dell'indagine.

Ciò anche per evitare che, all'esito della consulenza tecnica disposta dal P.M. in sede di sequestro, venga restituito un hard disk contenente dati alterabili o non consultabili[20].

Tale attività è, però, poco adottata nella pratica, in quanto necessita di specifiche competenze tecniche e di pertinente materiale software ed è consigliata, soprattutto, per i piccoli reati (presenza di dialer, diffamazione, virus), in quanto si devono esplorare i supporti informatici degli indagati o della parte offesa per ricercarne i dati e le tracce informatiche.

Si pongono, infine, altri ordini di problemi: uno di ordine temporale, poiché non è sempre possibile analizzare sul posto un gran numero di dati, tra i quali anche quelli cancellati che dovranno essere, opportunamente, "ripescati"; l'altro di ordine difensivo, in quanto una successiva analisi del consulente tecnico di parte potrà essere effettuata su un supporto informatico o sull'hard disk oggetto dell'attività diversi da quello sul quale il criminale aveva operato.

Da qui l'esigenza, secondo altri, che tale tipo di attività venga utilizzata solo quando si ravvisi la necessità di non operare un sequestro sproporzionato rispetto al fatto contestato o quando l'hard disk sia il contenitore di documenti informatici inerenti le indagini o nel caso di attività presso terzi estranei alla vicenda.

Diritto & Diritti ISSN 1127-8579

In altre ipotesi, invece, l'hard disk può essere il frutto dell'attività criminale o uno strumento per la commissione del reato, per cui è previsto il sequestro dell'intero hardware, qualunque sia il materiale contenuto. Una successiva analisi indagherà sulle risorse informatiche dell'indagato.

La possibilità di utilizzare il sequestro come mezzo di ricerca della prova dovrebbe essere soggetta alla pertinenza probatoria delle cose effettivamente sequestrate in relazione al contenuto del reato contestato nel provvedimento stesso, con una valutazione caso per caso della sua attuazione[21].

CONCLUSIONI

Quindi, punto di partenza dell'attività di indagine è il tracciamento degli indirizzi IP tramite l'analisi dei files di log.

Tale procedura è stata regolamentata dal T.U. n. 196/2003 sul trattamento dei dati personali, che ha introdotto una distinzione tra le finalità civilistiche e penali sulla conservazione dei dati da parte delle società di telecomunicazione.

Infatti, dal punto di vista civilistico, l'art. 123 prevede la cancellazione o l'anonimizzazione, da parte del fornitore della rete pubblica di comunicazione, dei dati personali relativi al traffico quando non sono più necessari per la trasmissione della comunicazione elettronica.

L'unica eccezione è rappresentata dalla tenuta e dal trattamento dei dati strettamente necessari ai fini della fatturazione o dei pagamenti in caso di interconnessione, per la documentazione in caso di contestazione della relativa fattura o per la pretesa al pagamento per un periodo non superiore a sei mesi, tranne il caso di una successiva contestazione in sede giudiziale.

Da parte della dottrina si è ritenuto ricomprendere all'interno della categoria dei dati personali relativi al traffico anche quelli del traffico web raccolti e memorizzati dai fornitori di accesso alla rete e dei relativi servizi nella gestione dei files di log e dei correlati data base contenenti i codici identificativi e i dati anagrafici dei clienti.

Di contro, dal punto di vista penale, l'art. 132 del T.U., così come modificato dall'art. 3 D.L. 24 dicembre 2003, n. 354 – convertito con modifiche proprio a tale articolo nella L. n. 45/2004 - ("Disposizioni urgenti per il funzionamento delle acque, nonché interventi per l'amministrazione della giustizia"), ampliava il termine previsto dall'art. 123 per la conservazione dei dati a fini investigativi, da parte delle società di telecomunicazione, per favorire l'accertamento e la repressione dei reati.

L'originario art. 132 prevedeva la tenuta dei dati per un periodo non superiore a trenta mesi. La formulazione dell'articolo de quo, invece, nell'originario testo inserito nel Decreto Legge 354/2003, prevedeva l'elevazione del termine a complessivi cinque anni, tra la formulazione del primo e del secondo comma, oltre che i criteri soggettivi, tecnici e procedurali per la conservazione e l'accesso degli stessi.

Diritto & Diritti ISSN 1127-8579

Contro la previsione della schedatura per cinque anni aveva mostrato preoccupazione anche il Garante per la privacy in quanto tale disciplina poteva entrare in conflitto con le norme costituzionali di libertà e di segretezza delle comunicazioni e sulla libertà di manifestazione del pensiero.

Sulla scorta di ciò, la conversione del Decreto Legge in esame ha visto la modifica, all'art. 3, proprio della formulazione dell'art. 132 D. Lgsv. n. 196/2003, prevedendo la tenuta dei dati relativi al solo traffico telefonico per un periodo complessivo non superiore a quarantotto mesi.

Da qui sorge l'impossibilità di conservazione dei files di log, in quanto la nuova dizione dell'art. 132 parla di dati relativi al traffico telefonico, provocando l'allarme di Telefono Arcobaleno – associazione che combatte ogni forma di pedofilia - che auspica un intervento legislativo che modifichi il testo dell'articolo o una sua interpretazione autentica[22].

Dalla necessità prorompente del tracciamento degli IP per la repressione dei reati, scaturisce la stesura di un accordo intervenuto tra la Polizia Postale e delle Telecomunicazioni e i provider sulla tenuta dei tabulati di tutti i collegamenti alla Rete per una durata di sei mesi[23].

Viene spontaneo, allora, chiedersi se tale accordo possa considerarsi legittimo o meno.

In tal caso, sempre nell'ottica della certezza de diritto, sarebbe auspicabile demandare ad un successivo intervento normativo in materia l'emanazione delle regole sulla tenuta e conservazione dei files di log per finalità di accertamento e repressione dei crimini informatici, anche con la promulgazione dell'auspicato codice di autoregolamentazione per i fornitori di servizi Internet.

BIBLIOGRAFIA

Mauro Milesi: Il poliziotto virtuale, pubblicato su www.libero.it

Mauro Milesi: Specialisti in prima linea, pubblicato su www.libero.it.

Attività ed organizzazione, dal sito www.poliziadistato.it

Unità di Analisi sul crimine Informatico (Computer Crime Analysis Unit), dal sito www.poliziadistato.it

L'attività in materia di contrasto della criminalità informatica, dal sito www.innovazione.gov.it

Domenico Vulpiani: La criminalità informatica: metodi di indagine e la collaborazione delle aziende bancarie, dal sito www.poliziadistato.it.

Marco Starno: Cybercriminologia, lezione tenuta presso il Corso di Alta Formazione in Diritto delle Reti Telematiche, Reggio Calabria, 29 maggio 2004.

Domenico Vulpiani: L'esperienza italiana nel contrasto al crimine informatico, intervento alla Cybercrime International Conference, Palermo, 3, 4 e 5 ottobre 2002, tratto dal sito www.criminologia.org

Beccato cyber-diffamatore anonimo, dal sito www.punto-informatico.it

Domenico Vulpiani: La criminalità informatica: metodi di indagine e la collaborazione delle aziende bancarie, dal sito www.poliziadistato.it.

Vittoria Ardino: Se la Rete è una trappola, articolo tratto da @ Il Sole 24 Ore del 20 maggio 2004.

Nella "rete" della criminalità - Internet sorvegliato speciale, dal sito www.poliziadistato.it

Laura Turini: Vita difficile per chi acquista foto illegali, articolo tratto da @Il Sole 24 Ore dell'11 marzo 2004.

Carlo Serra: Pedofilia e Internet: caratteristiche e spunti di ricerca, Rivista Minori giustizia, Franco Angeli Editore, pagg. 63,64

Filippo Leonardo: I reati informatici nell'attività investigativa della Polizia Postale e delle telecomunicazioni, dal sito www.fiammella.it

Cass., Sez. II, sentenza 17/12/1990, n. 6331.

Reati connessi a Internet: profili processuali penali e tutela dell'indagato, dal sito www.e-privacy.firenze.linux.it

I sequestri informatici in Italia, risposta del Dott. Gerardo Costabile a Punto Informatico, dal sito www.punto-informatico.it

Comunicato stampa, dal sito www.pariopportunità.gov.it.

Daniele Dell'Aglio: Il pericolo? È in ufficio, intervista a Domenico Vulpiani, tratta da @lfa Il Sole 24 Ore del 3 giugno 2004

Note:
[1] Pubblicazione redatta durante l'attività di stage e ricerca presso L'Osservatorio CSIG di Reggio Calabria

[2] Mauro Milesi: Il poliziotto virtuale", articolo pubblicato su www.libero.it

[3] Mauro Milesi: Specialisti in prima linea, articolo pubblicato su www.libero.it.

[4] Attività ed organizzazione, dal sito www.poliziadistato.it

[5] Unità di Analisi sul crimine Informatico (Computer Crime Analysis Unit), dal sito www.poliziadistato.it

[6] L'attività in materia di contrasto della criminalità informatica, dal sito www.innovazione.gov.it

[7] Domenico Vulpiani: La criminalità informatica: metodi di indagine e la collaborazione delle aziende bancarie, dal sito www.poliziadistato.it.

[8] Marco Starno: Cybercriminologia, lezione tenuta presso il Corso di Alta Formazione in Diritto delle Reti Telematiche, Reggio Calabria, 29 maggio 2004.

[9] Domenico Vulpiani: L'esperienza italiana nel contrasto al crimine informatico, intervento alla Cybercrime International Conference, Palermo, 3, 4 e 5 ottobre 2002, tratto dal sito www.criminologia.org

[10] Beccato cyber-diffamatore anonimo, dal sito www.punto-informatico.it

[11] Domenico Vulpiani: La criminalità informatica: metodi di indagine e la collaborazione delle aziende bancarie, dal sito www.poliziadistato.it.

[12] Vittoria Ardino: Se la Rete è una trappola, articolo tratto da @ Il Sole 24 Ore del 20 maggio 2004.

[13] Nella "rete" della criminalità - Internet sorvegliato speciale, dal sito www.poliziadistato.it

[14] Laura Turini: Vita difficile per chi acquista foto illegali, articolo tratto da @Il Sole 24 Ore dell'11 marzo 2004.

[15] Carlo Serra: Pedofilia e Internet: caratteristiche e spunti di ricerca, Rivista Minori giustizia, Franco Angeli Editore, pagg. 63,64

[16] Filippo Leonardo: I reati informatici nell'attività investigativa della Polizia Postale e delle telecomunicazioni, dal sito www.fiammella.it

[17] Cass., Sez. II, sentenza 17/12/1990, n. 6331.

[18] Reati connessi a Internet: profili processuali penali e tutela dell'indagato, dal sito www.e-privacy.firenze.linux.it.

[19] Laura Turini: Vita difficile per chi acquista foto illegali, articolo tratto da @Il Sole 24 Ore dell'11 marzo 2004.

[20] Reati connessi a Internet: profili processuali penali e tutela dell'indagato, dal sito www.e-privacy.firenze.linux.it.

[21] I sequestri informatici in Italia, risposta del Dott. Gerardo Costabile a Punto Informatico, dal sito www.punto-informatico.it.

[22] Comunicato stampa, dal sito www.pariopportunità.gov.it.

[23] Daniele Dell'Aglio: Il pericolo? È in ufficio, intervista a Domenico Vulpiani, tratta da @lfa Il Sole 24 Ore del 3 giugno 2004.

https://www.diritto.it/tecniche-indagine-della-polizia-postale-nellambito-dei-reati-informatici-nella-pedopornografia-line/

Diritto & Diritti ISSN 1127-8579