UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Edizione italiana a cura di ALSI e Tecnoteca
http://upgrade.tecnoteca.it

Analisi legale di un caso di criminalità informatica

di Nadina Foggetti

Versione italiana, a cura dell'autrice, dell'articolo
" Legal Analysis of a Case of Cross-border Cyber-crime"
pubblicato sul vol. IV, No. 6, December 2003 della rivista online UPGrade, a cura del CEPIS

Riassunto
La criminalità informatica trascende i confini dei singoli stati e le condotte criminose compiute attraverso internet comportano dei problemi ingenti in relazione al diritto applicabile. Il diritto non è sempre pronto a far fronte alle esigenze della globalizzazione del mercato e della stessa criminalità. Nel caso di specie l'attacker ha compiuto un accesso illegittimo a sistema informatico di pubblico interesse in svizzera ai danni di utenti italiani. L'attacco è stato realizzato attraverso una scalata di privilegi, da utente normale ad utente root. In seguito l'attacker ha installato sul sistema violato un rootkit per copiare le password degli utenti che si allocavano dal e sul sistema violato. Il sistema era di pubblico interesse per i dati ivi contenuti e perché permetteva di gestire degli esperimenti di grande interesse generale. Sul sistema era attivo un sistema di posta elettronica per gli utenti registrati. Sulla base della normativa italiana risultano applicabili l'art. 615-ter del CP italiano - accesso illegittimo a sistema informatico - con l'aggravante di cui al terzo comma; l'art. 617-quinques - Installazione di apparecchiature dirette ad intercettare ed interrompere una comunicazione; l'art. 615-quater CP - detenzione abusiva di codici d'accesso. Risulta inoltre applicabile l'art. 35 della legge 675/96 che sanzione il trattamento illegittimo dei dati personali contenuti nel sistema. Tuttavia, in seguito all'analisi dei presupposti relativi all'applicazione della legge penale italiana nello spazio il fatto non ricade nella giurisdizione italiana. Il principio della difesa non risulta applicabile, poiché non risultano integrati tutti i requisiti richiesti dalla norma, il principio di territorialità non risulta applicabile in quanto in Italia non è avvenuto neppure un tentativo punibile Risulta applicabile la legge penale Svizzera. Dopo l'analisi della normativa svizzera risulta applicabile solo l'art. 143-bis del CP svizzero, non essendosi verificato il requisito della sottrazione di dati che risulta essenziale ai fini della configurabilità del reato di cui all'art. 143-CP svizzero. La risposta europea al problema dei computer crimes non risulta adeguata in relazione all'eccessivo ricorso alla sanzione penale. Tutti gli sforzi di armonizzazione della normativa europea vertono sulla sanzione penale. Risulta indispensabile trovare una risposta alternativa ed adeguata al fenomeno della criminalità trasnazionale.

Parole chiave: Accesso illegittimo, Territorialità, Computer crimes, Crminalità transnazionale, Rootkit, Dati, Misure di sicurezza, Convenzione sul crimine informatico.

1. Introduzione.

La globalizzazione dell'informazione, generata dall'avvento delle nuove tecnologie, ha permesso la realizzazione di un libero mercato senza confini , in cui la criminalità informatica assume sfondi e riflessi di tipo transnazionale. Il caso ipotizzato in questa sede ci fornirà un quadro d'insieme dei problemi che è possibile affrontare, soprattutto in relazione al diritto applicabile, ad un'ipotesi di criminalità informatica transnazionale.

Nel caso di specie l'attacker ha compiuto la condotta in Svizzera violando un sistema di pubblico interesse, cagionando danni agli utenti Italiani che si erano collegati al sistema attaccato. Ipotizziamo che il sistema violato dall'attacker risulti essere di "pubblico interesse", poiché, ad esempio, alle macchine di cui si compone si allocano migliaia di utenti da tutte le parti del mondo, ma anche in relazione agli esperimenti che possono essere analizzati e realizzati attraverso l'utilizzo delle risorse hardware e software presenti a Ginevra. In particolare, si può ipotizzare la presenza di database inerenti agli esperimenti realizzati, in quanto fondamentali e di grande rilevanza ai fini della ricerca scientifica e tecnologia , per il miglioramento dello sviluppo sostenibile riguardante la popolazione globale e di un servizio di posta elettronica per gli utenti registrati.

Ipotizziamo che l'attacker in questione sfrutti una vulnerabiltà locale del sistema, in particolare del Kernel Linux 2.4, imputabile ad una mancata implementazione delle credenziali d'accesso al sistema stesso grazie al quale abbia effettuato una scalata di privilegi da utente normale a utente root. Si delinea in questo modo la condotta principale: l'accesso illegittimo puro e semplice sferrato dall'interno, ovvero dal sistema ginevrino stesso.

Ipotizziamo altresì che l'attacker abbia poi installato un rootkit: si tratta di un attacco di tipo trojan. Il software utilizzato presentava una composizione complessa, completa di sniffer per copiare le password digitate in dinamico dal e sul sistema violato, dei software che garantivano delle backdoor, ovvero degli accessi privilegiati e nascosti da utilizzare, dopo aver sferrato l'attacco, per rientrare nel sistema senza violarlo nuovamente. Il rootkit conteneva altresì dei tools per nascondere ogni traccia dell'attacco, modificando i comandi del sistema che permettono di verificare l'intrusione e riusciva a cancellare i logs, ovvero le tracce lasciate dall'attacker in seguito all'accesso illegittimo. Infine è possibile ipotizzare che l'attacco sia stato sferrato a Ginevra, che le passwords copiate appartenessero agli utenti italiani che si collegavano al sistema informatico violato e che non sia stato registrato alcun attacco ponte nei confronti dei sistemi le cui passwords erano state copiate. Partendo da questi dati di carettere tecnico, indispensabili per mettere a fuoco il proplema, possiamo analizzare i profili di diritto applicabile.

2. Applicazione della normativa italiana.

Internet ha permesso la definizione di un profilo criminale nuovo, diretto nella maggior parte dei casi a muoversi nello spazio giuridico globale ponendo, quindi, complessi problemi in relazione sia al diritto applicabile al caso concreto, sia alla giurisdizione competente a conoscere del reato.

Nel caso di specie, *l'attacker* ha portato a termine la condotta criminosa in Svizzera, ledendo l'integrità del sistema informatico, ma *crackando* le *password* degli utenti che si erano collegati dall'Italia e che avevano un account alle macchine violate per poter accedere alle risorse di calcolo fisicamente situate a Ginevra.

Analizzando i profili concreti del caso in esame è possibile individuare diverse condotte criminose ed ipotizzare un concorso di reati facenti parte di un unico progetto criminoso che indicheremo a titolo esemplificativo, per occuparci poi in maniera più accurata, del problema attinente all'applicazione della normativa italiana esaminata.

Innanzitutto l'*attacker* ha effettuato un accesso illegittimo a sistema informatico, ponendo così in essere, astrattamente, la condotta di cui all'art. 615-*ter* c. p. italiano che punisce, con la reclusione da uno a tre anni, "*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di ha il diritto di escluderlo*".

La fattispecie di cui all'art. 615-ter, così come gli atri reati introdotti dalla l. 547 del 1993[1], è stata formulata prendendo come modello l'ipotesi criminose cui accede: il reato di violazione di

[1] La legge che ha introdotto in Italia i computer crimes risulta decisamente ancorata al metodo casistico, tipico della cultura giuridica d'oltre Oceano, caratterizzata da un'elevata elasticità nel cogliere i segnali provenienti dalla vita di relazione ed a rivestirli di rilevanza giuridica. In questo modo le singole categorie di crimini informatici sono state

domicilio comune di cui all'art. 614 c.p. L'elaborazione è frutto della politica legislativa, che emerge dai lavori preparatori[2] e che tende a indentificare le nuove condotte criminose come delle aggressioni diverse ai beni giuridici tradizionali, non identificando i computer crimes in una categoria nuova ed autonoma da definire in base ai nuovi beni giuridici oggetto di protezione.

In questo caso al soggetto in questione erano stati attribuiti i permessi di utente normale, non di utente root, elemento di per sé sufficiente, secondo la giurisprudenza dominante[3], a manifestare lo *ius excludendi* da parte del titolare del sistema.

La stessa norma contempla anche una serie di ipotesi aggravate, che influiscono sulla procedibilità del reato e permettono di elevare la pena prevista ad un massimo di cinque anni. Avendo ipotizzato che si tratta di sistema di pubblico interesse, risulta applicabile l'aggravante di cui al terzo comma dell'art. 615-*ter* c.p., che prevede la procedibilità d'ufficio e la pena della reclusione da uno a cinque anni, qualora il reato in questione sia commesso ai danni di un sistema di interesse pubblico. L'art. 615-*ter* richiede che le misure di sicurezza, cui deve dotarsi il sistema siano "adeguate"[4], senza peraltro che la norma definisca indicazioni di sorta o parametri diretti ad individuarle.

I dati tecnici a disposizione permettono di individuare una seconda condotta passibile di sanzione penale: *l'attacker*, installando il *rootkit*, avrebbe integrato la condotta di cui all'art. 617-*quinquies* c.p[5]. L'installazione dello *sniffer*, compreso nei vari *tools* del *rootkit*, ha permesso all'*attacker* di captare le password degli utenti che si collegavano dall'Italia allo scopo di garantirsi la possibilità di attaccare nuove macchine e di estendere il raggio d'azione della propria condotta criminosa.

Inoltre l'articolo 615-*quater* c.p. contempla il reato di detenzione abusiva di codici d'accesso a sistemi informatici e telematici[6], applicabile al caso di specie. Si tratta di un reato di

---

formulate a prescindere dalla definizione di tipologie di omogenee ipirate a profili criminali comuni, risultando invece saldamente ancorate alla reale manifestazione delle condotte stesse nella realtà fattuale. Cfr. **TRENTACAPILLI D.**, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, Diritto Penale e Processo, n. 10, 2002, pag. 1280 e seg.

[2] La relazione che di accompagnamento alla l. 547/93 mette chiaramente in evidenza l'intento del legislatore di tutelare, mediante creazione della fattispecie di accesso abusivo "l'espansione dell'area di rispetto della persona umana garantita dalla Costituzione all'art. 14 e personalmente tutelata nei suoi aspetti essenziali e tradizionali dagli art. 614 e 615 del codice penale".

[3] La problematica delle misure di sicurezza sarà oggetto di trattazione successiva. È possibile, tuttavia, anticipare che la giurisprudenza prevalente ritiene che le misure di sicurezza, pur essendo un elemento costitutivo della fattispecie di accesso abusivo a sistema informatico di cui all'art. 615-*ter* c.p., rilevino in senso meramente ideale. Le misure di sicurezza non rilevano, cioè, tanto in qualità della concreta idoneità a tener lontani eventuali intrusi, bensì soprattutto quale fonte di manifestazione dello *ius excludendi*, in parallelo alla norma che tutela il domicilio reale (art. 614 c.p.). Cfr. TRENTACAPILLI D., A*ccesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, Dir. Pen. e Proc., n. 10/2002, pag. 1280 e seg. In linea con questa interpretazione v. NUNZIATA M., *La prima applicazione giurisprudenziale del delitto di accesso abusivo ad un sistema informatico – ex art. 615-ter*, Nota alla sentenza del Trib. Torino, 7 febbraio 1998, *Giur. Merito*, 1998, II, pag.711. In senso contrario v. la sentenza del G.u.p. Trib. Roma, 21 aprile 2000, in www.penale.it .

[4] Come si avrà modo di vedere in seguito, anche in questo caso la giurisprudenza di merito e legittimità ha inteso la necessità, prevista dalla norma, di elevare le misure di sicurezza nelle ipotesi in cui si tratti di un sistema di pubblico interesse. In senso ampio si veda, in particolare, Cass. 6 dicembre 2000, con nota di GALDIERI P., *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Dir. e Inf.*, 2001, I, pag. 17 e seg.

[5] L'art. 617-quinquies C.P. sanziona con la reclusione da uno a quattro anni "chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature dirette ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico oppure intercorrenti tra più sistemi".

[6] Punisce, con la reclusione sino ad un anno e con la multa sino a lire 10 milioni, "chiunque, al fine di procurare a sé 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".

pericolo, che si consuma non in dipendenza del danno o del turbamento effettivo del sistema, ma per il fatto di essere venuto a conoscenza degli strumenti descritti nella fattispecie[7].

La giurisprudenza [8], tuttavia, tende a considerare questa condotta assorbita nella condotta principale e quindi punibile, unitamente all'accesso abusivo, a norma dell'art. 615-*ter* c.p., non individuando due diverse condotte criminose.

L'art. 615-ter c.p., data la sua formulazione, però, configura un tipico reato di pericolo sanzionando in realtà il mero accesso abusivo, indipendentemente dal danneggiamento del sistema, dalla sottrazione dei dati custoditi o dall'interruzione del suo funzionamento[9].

L'intento legislativo risulta essere chiaro: anticipare la tutela ad un momento prodromico al compimento di un'azione delittuosa ben più grave e lesiva di interessi maggiormente meritevoli di tutela[10].

Il delitto di accesso abusivo può essere, quindi, considerato anche come "reato mezzo" rispetto ad ulteriori "reati fine" a sfondo meramente patrimoniale. Questa considerazione trova piena conferma nella disposizione normativa in esame, ove il legislatore ha scelto di considerare già penalmente rilevante l'accesso abusivo "puro", diretto cioè alla semplice presa di visione del contenuto del sistema violato, ma caratterizzandolo da un trattamento sanzionatorio di minore afflittività. Gli altri reati inseriti dalla stessa legge 457/93 risultano, quindi, complementari e non concorrenti rispetto al reato di accesso abusivo a sistema informatico, legati quindi da un nesso teleologico e strutturale nell'ambito della medesima condotta criminosa che si estrinseca nel compimento di più condotte tipiche.

Inoltre, nell'ipotesi di specie, lo stesso sistema violato garantisce uno spazio di posta elettronica cui i diversi utenti si allocano quotidianamente per controllare le mails. Le password captate quindi non erano solo quelle che consentivano l'accesso al sistema, ma anche quelle relative agli account degli utenti del servizio di posta. Le Password e gli Username sono considerati "dati personali", poiché diretti ad identificare un soggetto determinato e specifico, come anche lo stesso Garante per la privacy ha puntualmente precisato[11].

Si potrebbe, infine, ipotizzare anche l'applicazione dell'art. 35 della legge n° 675/96 a tutela dei dati personali, che sanziona il trattamento illegittimo dei dati stessi. Non vi sono tuttavia notizie certe in merito al trattamento illegittimo dei dati personali raccolti dall'attacker, risulta soltanto che l'attacker è entrato in possesso dei dati, poiché Suckit gli ha captati e copiati per lui.

Il sistema violato aveva un preciso obbligo di garanzia, in quanto responsabile del trattamento dei dati personali ai sensi della legge 675/96 con cui il legislatore ha inteso tutelare la riservatezza dei dati,ma anche la loro integrità.

L'art. 15 della legge, al primo comma, prescrive chiaramente "*l'adozione di idonee e preventive misure di sicurezza al fine di scongiurare la perdita o la distruzione dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*". Il D.P.R. 28 luglio 1999 n. 318 ha individuato le misure di sicurezza da adottare[12]. L'analisi delle misure di sicurezza da adottare, a seconda della diversa tipologia di sistema

---

[7] "E' in qualche modo una fattispecie paragonabile a quella dell'art. 707 c.p. che sanziona il reato di possesso ingiustificato di chiavi"; cfr PARODI C., *Detenzion e abusiva di codici d'accesso a sistemi e illecito impedimento di comunicazioni telematiche,* in Diritto Penale e Processo, n.)/1998, pag. 1149 e seg.

[8] Cfr. Trib. Torino, sez IV, 17 febbraio 1998, con commento di C. PARODI, *Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare,* in *Dir. Pen. e Proc.*, n. 8/1998, pag. 1038 e seg.

[9] Tutte ipotesi che valgono ad aggravare la figura delittuosa di base. Cfr TRENTACAPILLI D., *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione,* op. cit., pag. 1283 e seg.

[10] PECORELLA C., *Il diritto penale dell'informatica, Padova, 2000,* pag. 336; contra MANTIVANI F., *Diritto penale. Parte speciale,* Padova, 1995, pag. 451 e seg.; per il quale la semplice indiscrezione informatica non è meritevole di rilevanza penale, intesa come introduzione in sé e per sé.

[11] Sul punto si veda la decisione 16-29 aprile del 2001 che ha precisato che sono dati personali anche quelli forniti per la registrazione ad un dominio web. Cfr. BARBARISI M, *La raccolta indiretta di indirizzi elettronici costituisce violazione della privacy?,* in , settembre 2002.

[12] www.interlex.it/675/minotti.4.htm

informatico, con particolare riguardo agli elaboratori accessibili alla rete, esula dalla presente analisi. In questa sede è sufficiente rilevare che, qualora il responsabile del trattamento trascuri di adottare le misure di sicurezza atte a tutelare l'integrità e la riservatezza dei dati, è punito con la reclusione sino a due anni e con l'ammenda da dieci a ottanta milioni a norma dell'art. 36 della legge 675 del 1996.

Presupposti per l'efficacia della legge penale italiana.

La caratteristica che contraddistingue la criminalità informatica riguarda essenzialmente i profili transnazionali che possono assumere le condotte criminose consumate in Internet.

L'individuazione del *locus commissi delicti* non è sempre agevole quando l'autore del reato si serve di mezzi informatici e telematici per commettere la condotta criminosa, in quanto spesso la stessa si realizza attraverso più azioni dirette a realizzare il medesimo intento criminoso, compiute però attraverso dei sistemi ponte. È possibile, in sostanza, che l'attacker violi più sistemi informatici con un unico accesso illegittimo e compia più condotte criminose su computers, collegati tra di loro, ma ubicati in territori diversi, a volte in Paesi differenti. In altri casi può accadere che il luogo della violazione iniziale sia il luogo in cui fisicamente si trovi anche l'attacker, ma la persona offesa dal reato si trovi invece in un luogo diverso.

Nel caso di specie si pone, quindi, il problema preliminare di stabilire se risulti o meno applicabile la normativa italiana.

L'art. 3 CP definisce il principio della "obbligatorietà della legge penale"[13] espresso anche dalla collocazione sistematica della stessa norma che precede, infatti, le norme relative all'efficacia della legge penale nello spazio e lo stesso principio di inescusabilità dell'*ignoranza legis*[14], ed è successiva all'enunciazione del principio di legalità e alle norme relative all'efficacia della legge penale nel tempo.

L'art. 3 enuncia l'inderogabilità dell'applicazione della legge penale italiana *ratione personae*, in quanto applicabile a tutti i soggetti (cittadini o stranieri, si trovino sul territorio nazionale o all'estero), disponendo come unici limiti il principio di legalità e le norme stabilite dal diritto internazionale[15].

La formulazione della norma, definita tecnicamente impropria da parte di autorevole dottrina[16], non esclude comunque l'applicazione degli altri criteri individuati successivamente dal legislatore al fine di definire l'ambito di applicazione della legge penale nazionale[17].

Il principio di territorialità, di cui all'art. 6 comma 1 c.p., definisce l'applicabilità del diritto penale italiano entro i limiti di tutto il territorio dello Stato. Risulta, quindi, essenziale la definizione del luogo in cui il reato è stato commesso e l'art. 6, al comma 2, prevede che "*il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione o dell'omissione*".

---

[13] Ai sensi dell'art. 3 c.p. "*la legge penale italiana obbliga tutti coloro che, cittadini o stranieri, si trovano nel territorio dello Stato, salve le eccezioni stabilite dal diritto pubblico interno o dal diritto internazionale. La legge penale italiana obbliga altresì tutti coloro che, cittadini o stranieri, si trovano all'estero, ma limitatamente ai casi stabiliti dalla legge medesima o dal diritto internazionale*".

[14] Cfr. PICOTTI L., *La legge penale*, in *Giurisprudenza sistematica di diritto penale, parte generale, I*, II Ediz., (a cura di) F.BRICOLA-ZAGREBELSKY, Torino, 1996, pag. 154 e seg.

[15] La norma si inserisce evidentemente nella prospettiva politica e ideologica propria del legislatore fascista dell'epoca, nonché dell'affermazione assoluta della sovranità e dell'autorità dello Stato. Parte della dottrina ritiene l'art. 3 norma prodromica rispetto all'affermazione del principio di territorialità – enunciato nel successivo art. 6 c.p. -, quale principio base ispiratore dei limiti di efficacia del diritto penale italiano nello spazio. In realtà, la norma aspira ad un'affermazione dell'opposto principio dell'universale applicabilità della legge penale nazionale *ratione personae*, ponendo il principio dell'individuazione della legge penale applicabile in virtù del locus *commissi delicti* come ipotesi eccezionale rispetto al principio generale da essa ispirato.

[16] BRICOLA F., *Fatto del non imputabile e pericolosità*, Milano, 1961, pag. 87 e seg.

[17] Lo stesso art. 3 c.p., al capoverso, demanda infatti la definizione dei limiti al principio dell'obbligatorietà della legge penale nazionale al legislatore interno e alle norme derivanti dal diritto internazionale.

Il nostro codice accoglie, quindi, il criterio dell'ubiquità al fine di espandere al massimo l'applicabilità della legge penale italiana, sollevando l'annosa questione interpretativa relativa alla determinazione dei presupposti minimi per la realizzazione della "parte minima" della condotta criminosa sufficiente a far considerare l'intero reato commesso in Italia.

Il problema esegetico evidenziato non trova soluzione unanime in dottrina e riscontra divergenze anche nella giurisprudenza.

In dottrina si è dibattuto, in particolare, circa la possibilità di ritenere che gli atti compiuti nel territorio nazionale, ai fini dell'applicabilità della giurisdizione italiana, debbano integrare almeno gli estremi del tentativo punibile e non si limitino ad un semplice atto preparatorio, ovvero considerare che il reato sia stato commesso in Italia anche quando si sia ivi verificato anche solo un suo "frammento", quindi anche un mero atto preparatorio[18].

Secondo un altro indirizzo interpretativo, invece, che fa leva sul tenore del disposto normativo, il reato dovrebbe appartenere alla giurisdizione italiana quando anche solo una parte di esso, consumato o tentato, sia stata realizzata sul territorio nazionale, a condizione che tale "parte" costituisca un anello essenziale della condotta conforme ad un modello criminoso. Un tale giudizio andrebbe effettuato *ex post* e in concreto, e non semplicemente *ex ante* ed in astratto[19].

La giurisprudenza dominante sembra orientata ad accogliere quest'ultima opzione interpretativa[20].

Per quanto concerne i requisiti minimi necessari all'integrazione del reato nella forma tentata, ai fini dell'applicabilità della giurisdizione italiana *ex* art. 6 comma 2, la giurisprudenza dominante ritiene necessario che "*la parte dell'azione commessa in Italia non abbia i requisiti di idoneità e di univocità, ma valga tuttavia a far ritenere commessa in Italia quella parte di azione che considerata unitamente ai successivi atti commessi all'estero, sostanzi un delitto tentato o consumato*". Questa interpretazione sembrerebbe sposare la teoria della "realizzazione potenziale dell'evento"[21]. Tuttavia la stessa sentenza prosegue con un'interpretazione restrittiva, in quanto richiede che "*al proposito criminoso maturato in Italia corrisponda una estrinsecazione obiettiva che incida sul mondo esterno, modificandolo*".

Applicabilità del principio di territorialità.

Il criterio dell'ubiquità trova particolare applicazione nell'ambito dei reati commessi in Internet. Parte della dottrina ritiene che risulta applicabile la giurisdizione italiana quando i dati, che costituiscono l'oggetto del reato, pur essendo stati immessi in rete all'estero, transitino sui servers collocati in Italia o quando ivi sia avvenuta la memorizzazione e la duplicazione[22].

Il principio di ubiquità trova, poi, specifica applicazione in materia di diffamazione commessa a mezzo internet. La Cassazione afferma che, in base al principio dell'ubiquità, è consentito al giudice italiano di conoscere del fatto costituente reato, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto nel caso in cui un *iter criminis* iniziato all'estero si sia concluso con un evento realizzato in Italia[23]. La diffamazione si qualifica come reato

---

[18] La dottrina in questione ipotizza che si possa considerare commesso in Italia il delitto tentato, anche quando neppure gli atti preparatori siano stati compiuti nel territorio nazionale, ma se almeno potenzialmente l'evento si sarebbe potuto verificare nello stesso. Cfr. PICOTTI L., *La legge penale,* op. cit., pag. 172 e seg.

[19] FIANDACA G. MUSCO M., *Manuale di diritto penale,* Bologna, 1989, pag. 109 e seg.

[20] La Cassazione, infatti, in numerose decisioni ha sancito che il temine "*in parte*", previsto all'art. 6 comma 2 c.p., deve essere inteso in senso naturalistico, cioè come un momento dell'iter criminoso che, considerato unitamente ai successivi atti conseguenti commessi all'estero, si sostanzi in delitto tentato o consumato Cfr. Cass. Sez. I, 28 Novembre 1980, in Cass. Pen., 1982, pag. 735; Cass. Sez. III. 27 Novembre 1984, in *Cass. Pen*. 1986, pag. 476; Cass. Sez. I, 30 Luglio 1984, *in Giust. Pen*., 1985, II; Cass. Sez. VI, 19 Gennaio 1988, in *Riv. Pen*., 1989, pag. 416.

[21] Cass. Sez. III., 10 Gennaio 1961, Cass. Pen., II, pag. 811 e seg; per la giurisprudenza più recente si veda Cass. Sez. I, 20 Marzo 1963, Riv. It. Di Proc. Pen., 1965, pag. 118 e seg.; Cass. Sez. IV, 22 Febbraio 1993, in Giust. Pen. 1993, II, n. 517, pag. 629.

[22] PICOTTI L., *I profili penali delle comunicazioni illecite via internet,* in *Dir. Dell'Inf. e dell'Inf*., 1999, pag. 322 e seg.

[23] Cass., sent. 17 Novembre 2000, 17 dicembre 2000, n. 4741, reperibile on line all'URL www.interlex.it/testi/cp4741.htm oppure www.comellini.it/reatiinformatici_file%5C.sntcass2000-4741.htm

di evento, inteso come avvenimento esterno all'agente e causalmente collegato al comportamento del reo, un evento peraltro non fisico, ma psicologico, consistente nella percezione da parte del terzo del messaggio offensivo. L'evento può non verificarsi, ad esempio, perché nessuno visita il sito, oppure si realizza un tentativo, ovvero il reato risulta impossibile, come nelle ipotesi in cui l'autore fa uso di uno strumento difettoso che solo apparentemente gli consentiva l'accesso ad uno spazio web, mentre in realtà il suo messaggio non è mai stato immesso in rete.

Se nel caso della diffamazione la diffusione del messaggio, essendo avvenuta in Italia, costituiva "requisito minimo necessario" al fine dell'applicabilità della giurisdizione Italiana, nel caso da noi analizzato non risulta applicabile il principio dell'ubiquità.

L'attacker, infatti, ha agito a Ginevra, copiando le password digitate dagli utenti che si collegavano al sistema violato.

La circostanza che le password venissero digitate dagli utenti italiani, da computer fisicamente collocati sul territorio nazionale, non risulta integrare gli estremi del "requisito minimo" ai fini dell'applicazione della legge italiana. L'evento "copia di password" è, infatti, avvenuto integralmente a Ginevra in quanto i tool di Suckit che hanno consentito di copiare in dinamico i dati, sono stati installati sulle macchine del sistema ginevrino ed ivi gli utenti italiani si allocavano per accedere alle risorse di calcolo disponibili.

Non risulta quindi applicabile il principio della "territorialità" al fine si individuare la punibilità sulla base della legge italiana al caso di specie.

Applicabilità del principio della difesa.

Il nostro ordinamento giuridico, al fine dell'applicabilità della legge penale nazionale e in deroga al principio di territorialità, prevede l'applicazione del principio della difesa, in base al quale l'individuazione della legge penale applicabile avviene non già in funzione del luogo in cui è stato commesso il reato, nè in relazione alla nazionalità del soggetto attivo del reato[24], ma in virtù del soggetto passivo del reato. Secondo tale principio, la legge penale italiana risulta quindi applicabile ogniqualvolta il reato sia commesso a danno dello Stato italiano o di un cittadino italiano, indipendentemente dal *locus commissi delicti*.

L'art. 10 c.p. stabilisce, infatti, che lo straniero che "*commette in territorio estero, a danno dello Stato o di un cittadino italiano, un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo ad un anno, è punito secondo la legge medesima*".

La norma si pone come corollario dell'art. 3 c.p., in virtù del quale la legge italiana è universalmente obbligatoria, ad eccezione dei limiti interni ed internazionali.

La punibilità della condotta criminosa realizzata dallo straniero sul territorio estero in base alla legge italiana è sottoposta, peraltro, ad alcune condizioni: la presenza del reo nel territorio nazionale e la richiesta del Ministero della Giustizia, ovvero l'istanza o la querela presentata dalla persona offesa[25].

Alla luce delle considerazioni svolte, si può affermare che nel caso di specie il fatto non risulti punibile ex art. 10 CP in base alla legge italiana, in quanto non ricorre alcuna delle condizioni previste al comma 2 dello stesso articolo. Risulta, infine, indispensabile sottolineare che l'avvenuta copia delle passwords è un dato certo, in quanto i dati tecnici attinenti all'attacco al sistema testimoniano che lo sniffer copiava e rimandava all'attacker le passwords in transito sul sistema. Indipendentemente dall'uso che ne abbia fatto successivamente, l'attacker aveva la materiale disponibilità sia dei codici d'accesso degli utenti italiani al sistema violato, sia le password degli utenti che controllavano la loro posta elettronica ivi allocandosi.

---

[24] Costituisce anch'essa un'eccezione al principio della territorialità e si fonda sul principio della personalità attiva. È prevista dall'art. 9 c.p., in base al quale il cittadino che, fuori dai casi indicati dagli art. 7 e 8 "commette in territorio estero un delitto per il quale la legge italiana stabilisce l'ergastolo o la pena della reclusione nel minimo non inferiore a tre anni, a condizione che si trovi nel territorio dello Stato" è punibile sulla base della legge italiana. Cfr. CONTENTO G., *Corso di diritto penale,* Bari, 1996, pag. 142 e seg.

[25] Cfr. PICOTTI L., *I profili penali delle comunicazioni illecite via Internet,* op. cit., pag. 196 e seg.

Come anticipato, qualora gli utenti italiani avessero presentato denuncia nei confronti dell'attacker, ai fini dell'applicabilità della legge italiana, avrebbe trovato applicazione l'art. 10, comma 2 CP.

Nell'ipotesi in cui, invece, gli utenti italiani avessero sporto denuncia dopo aver effettuato l'installazione di CHKrootkit, al fine di verificare la presenza di rootkit, e il procedimento avesse dato esito positivo, il fatto sarebbe rientrato nella giurisdizione italiana non in applicazione del principio della nazionalità della persona offesa dal reato, ma sulla base del principio di ubiquità.

L'installazione di un rootkit sulle macchine degli utenti italiani poteva essere effettuato solo con lo stesso procedimento con cui è stato effettuato sul sistema violato: l'attacker dopo aver copiato le password degli utenti italiani che si allocavano al primo sistema, è entrato in possesso degli user name e delle password che consentivano i privilegi attribuiti ai loro titolari.

Se l'operazione di controllo fosse andata a buon fine e gli utenti italiani avessero riscontrato la presenza di un rootkit sul proprio sistema informatico, da un punto di vista tecnico si sarebbe verificata un prosecuzione dell'attacco informatico attraverso sistemi ponte precedentemente violati, mentre da un punto di vista strettamente giuridico si sarebbe registrato un proseguimento dell'*iter criminis* iniziato in Svizzera e conclusosi in Italia.

La violazione dei sistemi italiani avrebbe costituito l'anello conclusivo del progetto criminoso dell'attacker, con conseguente applicabilità della legge penale italiana in virtù non del principio della nazionalità del soggetto passivo, ma del criterio dell'ubiquità di cui all'art. 6 comma 2 CP.

Alla luce della giurisprudenza e della dottrina dominante, in precedenza analizzata, l'ulteriore attacco ai sistemi informatici italiani avrebbe permesso, in quanto "requisito minimo necessario", la punibilità dell'intera condotta criminosa sulla base del diritto italiano.

Nel caso di specie, peraltro, per quanto sinora detto, non risulta applicabile la legge penale italiana, bensì quella svizzera, che sarà oggetto di immediata analisi.

3. Applicazione del diritto penale svizzero.

Il Codice Penale Svizzero è stato recentemente novellato e modificato al fine di prevedere una regolamentazione dei reati informatici, data la particolarità di queste figure criminose.

Il sistema introdotto dal legislatore elvetico risulta di netta ispirazione tedesca quanto alla tecnica legislativa utilizzata, mentre la formulazione delle singole fattispecie delittuose è stata modellata sulla base delle indicazioni fornite dalla Raccomandazione n. R (89/9) del Consiglio d'Europa[26].

Come anticipato, il legislatore svizzero ha introdotto, nell'ambito dei reati contro il patrimonio, delle forme delittuose nuove dirette a sanzionare le condotte criminose realizzate attraverso l'uso di un elaboratore e quelle dirette a ledere, in particolare, i dati che transitano o che sono registrati in un sistema informatico[27].

La legge del 1993 ha introdotto l'art. 143-*bis* del c.p., che corrisponde sostanzialmente al reato di accesso abusivo in un sistema informatico, conosciuto anche nell'ordinamento giuridico italiano.

La norma sanziona, infatti, chiunque si introduce senza autorizzazione, attraverso un sistema di trasmissione di dati, in un sistema informatico altrui specialmente protetto contro ogni accesso. La punibilità prescinde completamente dal fine per il quale è stato commesso l'accesso abusivo: l'art. 143-*bis* c.p. trova dunque applicazione anche nelle ipotesi in cui il soggetto attivo del reato abbia agito semplicemente per prendere visione del sistema target.

---

[26] Cfr. Raccomandazione n. R (89/9) del Consiglio d'Europa sulla criminalità informatica e il rapporto finale del comitato europeo per i problemi penali, Strasburgo, 1990.

[27] STRAUFFACHER E., *Infractions contre le patrimonie: le nouveau droit, Schweizerische Seiteschrift für Strafrecht,* 1996, pag. 7 e seg.

Caratteristica di questa nuova fattispecie è, infatti, l'assenza di uno scopo di lucro in capo all'agente, elemento che invece originariamente assurgeva a mera circostanza attenuante del reato[28].

Secondo parte della dottrina, l'esigenza avvertita dal legislatore di sanzionare le ipotesi di intrusione anche in assenza di un reale danneggiamento, configurerebbe la fattispecie come reato di pericolo astratto, per il quale lo scopo con cui il reo ha agito non rivestirebbe alcun ruolo[29].

La dottrina dominante obietta che se anche l'art. 143-*bis* c.p. prevede effettivamente un'ipotesi di reato di pericolo astratto, lo stesso non troverebbe tuttavia applicazione nelle ipotesi in cui ricorrano gli estremi per sanzionare la condotta alla stregua dell'art. 143 c.p. che, nonostante contempli anch'esso una fattispecie di pericolo astratto, prevede *ex lege* il dolo specifico, cioè l'intenzione di procurare a sè o ad altri un profitto[30].

Alla luce di questa interpretazione, l'art. 143-*bis* c.p. assurge a ruolo di norma residuale, applicabile alle limitate ipotesi in cui l'attacker abbia agito al fine di fare "il mero ingresso" nel sistema informatico, senza l'intenzione di cagionare un danno o di sottrarre i dati contenuti nel sistema. L'art. 143 c.p, nella nuova formulazione, sanziona con la reclusione nel minimo di cinque anni o con la detenzione[31], chiunque, con l'intenzione di procurare a sé o ad altri un indebito profitto, procura, per sé o altri, dati a lui non destinati e specialmente protetti contro il suo accesso non autorizzato, registrati o trasmessi elettronicamente o secondo un modo simile.

Qualora la condotta dell'attacker sia compiuta con l'intenzione di danneggiare o di copiare dati di un sistema, ma l'autore non riesca a portare a termine l'intento criminoso, potrebbe sorgere il dubbio circa la punibilita' della condotta ai sensi dell'art. 143-*bis* c.p., come reato consumato, oppure *ex* art. 143 c.p., come ipotesi di delitto tentato.

La stessa dottrina svizzera si interroga circa la possibilita' di punire ai sensi dell'art. 143 c.p. il soggetto che si sia introdotto abusivamente in sistema informatico, prendendo semplicemente visione delle sue potenzialita' o delle sue vulnerabilita'[32], al fine di utilizzare queste informazioni per garantire a sè o ad altri un ingiustificato profitto[33].

Nel disegno di legge presentato al Consiglio Federale il 24 aprile 1991, l'accesso abusivo veniva considerato un mero "atto preparatorio" rispetto all'acquisizione di dati e previsto, quindi, all'interno dello stesso articolo diretto a reprimere quest'ultima condotta criminosa[34]. In seguito alla discussione parlamentare, all'accesso abusivo è stata attribuita autonoma rilevanza ed una sanzione ben più mite rispetto a quella di acquisizione indebita dei dati. Nella stesura definiva ed approvata dalle Camere, sono state tenute distinte le due ipotesi delittuose, prevedendo accanto all'art. 143 c.p., l'art. 143-*bis*. In realtà, risulta molto discutibile la struttura della norma in questione, in quanto non solo si configura come un reato di pericolo astratto, ma contempla una fattispecie di mera condotta alla stregua dell'art. 615-*ter* del codice penale italiano.

---

[28] Nel progetto preliminare si leggeva "*se il colpevole ha agito senza volerne trarre profitto è punito, a querela di parte, con la detenzione o con la multa*"; cfr PECORELLA C., *Il diritto penale dell'informatica,* Padova, 2000, pag. 308, nota n. 124.

[29] SCHMID N., *Das neue Coputerstrafrecht, ZStrR*, 1995, pag. 25 e seg.

[30] STRAUFFACHER E., *Infraction conte le patrimoine: le nouvelle droit,* op. cit. pag. 13. « *on peut toutefois répondre a cette objection au rappelant que le faux dans les titre est également un délit de mise en danger abstraire mais qu'il contient bel est bien comme condition subjective le dessin de porter aux intérêts pécuniaires.*

[31] Nel diritto penale svizzero la reclusione e la detenzione rientrano nella tipologia delle pene privative della liberta' personale. La reclusione, definita dall'art. 35 c.p., è la più grave delle pene privative della libertà personale: la sua durata minima è di un anno, quella massima di vent'anni; essa può essere inoltre perpetua nelle ipotesi in cui al legge disponga espressamente in tal senso. Per quanto concerne la detenzione, definita dal successivo art. 36, la sua durata minima è di tre giorni, mentre quella massima è di tre anni, salvo che la legge disponga espressamente in altro modo.

[32] Ad esempio si potrebbe ipotizzare che il soggetto effettui semplicemente una fase di Information Ghatering, raccogliendo generiche informazioni sul sistema target e rivendendo le stesse, per procurarsi un guadagno illegittimo.

[33] CASSANI U., a proposito della formulazione previdente dell'art. 143 c.p., ipotizzava un contrasto con il principio di legalita'; nello stesso senso anche SCHWBARTH M., *Kommentar zum Schweizerischen Strafrecht, Bes. Tail*., 2 Band, 1990, pag. 98-99. In senso contrario cfr. S. TRECHSAIL, *Schweizerischs Strafgesetzvbuch* Kurkkommentar, Zurich, 1989, pag. 445.

[34] Cfr. Messaggio del Consiglio Federale n. 91032, concernente la modifica del codice penale svizzero e del codice militare, in *Feuille Fédérale,* n. 23 del 18 giugno 1991, pag. 933 e seg.

La diversa collocazione sistematica delle due fattispecie nelle diverse legislazioni, fa sorgere dubbi circa la corretta portata dell'art. 143-*bis*.

L'accesso abusivo, essendo collocato dal legislatore elvetico nei reati contro il patrimonio, dovrebbe prevedere almeno la potenziale possibilità per l'intrusore di poter sottrarre alla vittima dei dati, quindi il requisito del dolo specifico dovrebbe essere inteso come elemento che giustifica la meritevolezza della sanzione penale. Unitamente, essendo una fattispecie di pericolo prodromica rispetto al furto di dati, dovrebbe considerarsi impossibile la condotta di accesso abusivo sferrata ai danni di un sistema che non contiene dati.

La norma italiana si presenta, invece, maggiormente coerente con la sua collocazione sistematica, anche se non pienamente condivisa in dottrina poiché diretta a tutelare non il patrimonio, ma la libertà e, in particolare, il domicilio, quale luogo in cui si manifesta e si forma la personalità. Questa collocazione sistematica e la natura del bene giudico protetto risultano alla base della punibilita' della mera condotta di accesso abusivo a sistema informatico e telematico.

L'articolo 143 c.p. punisce, come evidenziato, l'acquisizione illecita di dati. La collocazione sistematica della norma, inserita nei delitti contro il patrimonio, e la dizione francese del termine "*soustraction*", hanno spinto la dottrina ad interpretare pacificamente il termine "acquisizione" alla stessa stregua dell'omonimo termine utilizzato nella definizione normativa del reato di furto di cui all'art. 139 c.p.

Al fine dell'integrazione della fattispecie di "*soutraction des donnée*" risulta indispensabile, secondo la dottrina svizzera, lo spossessamento ("*soutraction*" nel testo francese e "*wegnehmen*" nella dizione tedesca) dei dati ai danni del legittimo titolare.

Sulla base di questo orientamento, il semplice fatto di copiare i dati non costituisce reato ai sensi dell'art. 143 c.p.[35]. In questo caso la dottrina ritiene possa trovare applicazione l'art. 143-*bis*, a condizione che non sia presente l'intenzione di procurarsi un indebito arricchimento, e quindi il dolo specifico.

Alla luce dell'interpretazione dominante, non si può fare a meno di sottolineare che la norma *de qua* trovera' applicazione solo in casi rarissimi, poiche´facilmente eludibile dall'attacker, il quale potra' limitarsi a copiare i dati - sia pur al fine di realizzare un indebito guadagno - e tuttavia non incorrere in nessuna delle fattispecie analizzate.

Segue: l'applicazione del diritto svizzero.

Nel caso di specie l'attacker ha compiuto un accesso illegittimo a sistema informatico, agendo con dolo e con l'intenzione di copiare i dati in transito nel sistema. Il dolo risulta palesemente dimostrato dalla circostanza che l'attacker ha installato degli sniffer, compresi nel rootkit, che copiavano le password digitate in dinamico dagli utenti.

Il fatto che l'attacker abbia copiato le password potrebbe far ritenere integrata la fattispecie di cui all'art. 143 c.p.: non risulta, tuttavia, perfezionato il requisito della "sottrazione materiale" dei dati dal sistema oggetto dell'intrusione. La disposizione svizzera prevede, inoltre, ai fini della punibilità della condotta, che il soggetto abbia agito per procurare a se o ad altri un vantaggio. Nel caso di specie l'intenzione di cagionare un profitto non può essere provata e, qualora si volesse interpretare la norma in senso estensivo, attribuendo a "lo scopo di danneggiare" un sistema la stessa portata lesiva della condotta di chi agisce con l'intento di cagionare a s o ad altri un ingiusto guadagno, si realizzerebbe una violazione del principio di legalità sancito dall'art. 1 del codice penale svizzero.

A parere di chi scrive non risulta, pertanto, possibile applicare al caso di specie l'art. 143 c.p.

Anche il reato di accesso abusivo a sistema informatico di cui all'art. 143-*bis* c.p. risulta di difficile applicazione nei confronti della condotta tenuta dall'attacker, poiché la stessa non era diretta al mero fine di prendere visione del sistema informatico, ma alla sottrazione di dati.

[35] STRAUFFECHER E., *Infraction countre le patrimonie: le nuoveau droit,* op. cit., pag. 14.

Si potrebbe comunque, nonostante i pareri discordanti emersi in dottrina, ritenere applicabile l'art. 143-*bis* c.p., che però presenta una portata general-preventiva e sanzionatoria ridotta rispetto all'offesa effettivamente cagionata dall'attacker.

Le altre disposizioni svizzere dirette alla protezione dei dati non risultano parimenti applicabili, poiché il fatto di specie non soddisfa i requisiti oggettivi e soggettivi richiesti per la punibilità del soggetto agente[36].

La normativa svizzera risulta, in definitiva, lacunosa in quanto lascia ampi spazi di non punibilità; nel contempo risulta anche scarsamente adeguata ad essere applicata alle ipotesi delittuose consumate attraverso l'utilizzo di sistemi informatici, data la rigidità del dettato normativo che si contrappone nettamente al continuo progresso che caratterizza il W W W.

Nel caso di specie il nostro attacker potrà vedersi comminare una sanzione detentiva - sicuramente non eccessivamente lunga - qualora la magistratura svizzera ritenga applicabile l'art. 143-*bis* c.p. Nell'ipotesi in cui il fatto non dovesse rientrare nell'applicazione della norma richiamata, la condotta risulterebbe beneficiaria della diversa punibilità dello stesso fatto nell'ambito di sistemi giuridici diversi ed il nostro attacker avrebbe sfruttato la presenza di un paradiso penale in cui portare a termine le condotte criminose.

L'applicazione dell'art. 143-*bis* del cod. pen. svizzero risulta strettamente connessa alla presenza nel sistema target di dati, essendo questi ultimi oggetto espresso di tutela.

In una sentenza del 31 Marzo 1999, la Corte Svizzera ha condannato uno studente di Losanna ritenuto responsabile di un accesso abusivo a sistema informatico, realizzato attraverso una scalata di privilegi nell'ambito di un sistema Linux, prendendo in questo modo possesso della macchina[37] .

Come nel caso analizzato in questa sede, anche l'attacker di Losanna aveva provveduto ad installare degli sniffer per le password che venivano digitate in dinamico. Con le password ottenute era riuscito ad attaccare altri sistemi informatici. La Corte Svizzera ha condannato l'attacker ai sensi dell'art. 143-*bis* del cod. pen. svizzero, per il reato di accesso abusivo in un sistema informatico, ai sensi dell'art. 144-*bis* per i danni compiuti al sistema violato.

Da un'analisi della giurisprudenza costante delle Corti Svizzere emerge chiaramente come le norme dirette a sanzionare l'accesso abusivo a sistema informatico siano poste a tutela di sistemi contenenti dati e che grande importanza viene attribuita, anche in sede di accertamento dei fatti, all'esistenza di misure di sicurezza poste a tutela del sistema informatico stesso[38].

In una rete globale il principio di territorialità, quale fonte di legittimazione della potestà sanzionatoria dello Stato – in cui le norme giuridiche sono tradizionalmente pensate per una comunità di cittadini localizzati entro confini determinati – va sgretolandosi, rischiando di determinare spazi di impunità per chiunque sappia di potersi porre al riparo delle più tolleranti leggi del paese in cui agisce.

E' possibile constatare che spesso le condotte criminose poste in essere da attacker professionisti restano fuori dall'area realmente sottoposta a sanzione penale, poiché questi soggetti sfruttano le loro conoscenze tecniche e giuridiche per garantirsi spazi di impunità.

---

[36] L'art. 144-*bis* c.p. contempla il reato di danneggiamento dei dati, che non può trovare applicazione poiché non risulta che l'attacker abbia danneggiato i dati o interrotto la funzionalità del sistema. Le altre norme – il riferimento è agli art. 141–*bis* e 150-*bis* c.p. - risultano strettamente connesse al reato di frode attraverso l'utilizzo di sistemi informatici o di carte di credito.

[37] Sentenza emanata dal Prosecutor Judge of Vaud 31 March 1999.

[38] Cfr a quanto riportato da SCHWARZENNEGGER C., *Computer crimes in Cyberspace*, *Jusletter 14 Ottobre 2002*, Pubblicata sul sito www.weblaw.ch e gentilmente fornitami dal dott. Franz Kummel. Esempi di sentenze sono il caso WEF –hacker, in cui un hacker effettuò un'intrusione in un sito di pubblico interesse Il World Economic Forum, in cui viene effettuata uno specifico accertamento rispetto alle misure di sicurezza adottate a tutela del sistema stesso al fine di scongiurare accessi non autorizzati. In particolare l'attacker aveva compiuto una serie di port scanning sul sito oggetto dell'attacco, quindi ai fini della prova il titolare del sistema ha dovuto dimostrare l'adeguatezza delle misure di sicurezza adottate per tutelare il sistema stesso.

Si potrebbe dire che gli attacker professionisti sfruttano non solo le falle dei sistemi informatici per garantirsi un ingresso illegittimo e compromettere il sistema stesso, ma anche i "bug" dei sistemi informatici e l'inadeguatezza degli strumenti predisposti per la repressione delle condotte illecite compiute in rete.

4. Aspetto Europeo e Internazionale.

A fronte delle innumerevoli problematiche di ordine pragmatico poste dalle nuove tecnologie informatiche, adoperate quale strumento ed oggetto delle moderne forme di criminalità e che si estrinsecano nelle difficoltà connesse all'individuazione del *locus commissi delicti* o alla scoperta dell'identità del soggetto agente, cresce l'esigenza di ricorrere ad un sistema alternativo a quello penale e contemporaneamente di creare una normazione comune a livello europeo ed internazionale al fine di superare l'inadeguatezza del principio di stretta territorialità e lo stesso principio di ubiquità. I riflessi che la globalizzazione dei mercati apporta in ambito giuridico obbligano a ripensare le finalità e gli strumenti del diritto di fronte a problemi che hanno una valenza di massa, quale non si era mai verificata prima. Occorre prestare attenzione ai nuovi soggetti e alle nuove condotte che possono divenire fonte di contraddizione e di conflitto tra il diritto degli Stati e quello di natura sovrannazionale o internazionale[39].

Di fronte a questi problemi sicuramente la risposta fornita dal diritto internazionale di tipo classico non è sufficiente, né può servire a mascherare le tensioni generate dai principi generali del diritto dei singoli Stati che invocano l'universalità delle proprie regole, nonostante la pluralità di attori presenti sullo scenario giuridico globale[40].

Per ovviare a questi inconvenienti risulta, quindi, necessario ripensare al ruolo e al significato che la sovranità degli Stati dovrà assumere rispetto ai possibili strumenti di tutela diretti a combattere e prevenire la criminalità transnazionale. La cooperazione internazionale costituisce, infatti, un requisito indispensabile e la maggior parte dei paesi europei si è accorta che il problema della criminalità[41] transfrontierana necessita di una risposta globale soprattutto in materia di *cyber crimes*, al fine di proporre strumenti efficaci e adeguati per la lotta alla criminalità di nuovo conio.

I maggiori progressi sono da ricercare nell'atto istitutivo dell' Europol[42], e nella decisione del Consiglio dell'Unione Europea ha creato Eurojust[43] diretti soprattutto alla cooperazione giudiziaria in relazione alla raccolta di prova ed all'esecuzione delle sentenze e dei mandati di cattura nella rete transnazionale.

La Convenzione Europea sulla cybercriminalità, aperta alla firma il 23 novembre 2001, rappresenta il maggiore sforzo sinora effettuato a livello europeo per tentare di combattere in modo efficace questo particolare tipo di criminalità, i cui sviluppi minacciano seriamente, oltre che i

---

[39] Cfr FLICK G. M., *Globalizzazione dei mercati e globalizzazione della giustizia,* Riv. Trim. Dir. Pen. Dell'Econ., 2000, pag. 591 e seg.

[40] Gli Stati, gli individui, le imprese multinazionali, le organizzazioni non governative, le istituzioni sovrannazionali sia regionali che uniuversali, i rispettivi sistemi di giurisdizione.

[41] Sin dagli anni Sessanta il Consiglio dell'Unione Europea ha contribuito a dare un notevole impulso alla normazione in materia di computer crimes, tentando di indirizzare gli Stati membri verso un'uniformità delle legislazioni nazionali che consentisse un'adeguata lotta al crimine informatico. Cfr MILITELLO D., *nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in Riv. Trim. Dir. Pen. Econ., 1992, pag. 365 e seg; FROSINI F., *La criminalità informatica,* in Dir. Inf., 1997, pag. 487 e seg.

[42] L'Europol si occupa essenzialmente di agevolare lo scambio di informazioni in materia giudiziaria tra gli Stati membri, attraverso la gestione di in sistema informatizzato di dati alimentato direttamente dagli Stati stessi e direttamente accessibile alla consultazione delle unità nazionali, e dai dirigenti dell' Eurogol stessa; cfr. www.eroparl.it

[43] Il 14 dicembre 2000, il Consiglio ha adottato la decisione istitutiva dell'Eurojust, un organismo giudiziario sopranazionale, composto da magistrati e funzionari di polizia distaccati di ogni Stato membro, cui è conferito il compito di agevolare il coordinamento tra le autorità nazionali responsabili dell'esercizio dell'azione penale, di prestare assistenza nelle indagini riguardanti casi di criminalità organizzata, in particolare cooperando con l' Europol e la rete giudiziaria, soprattutto al fine di semplificare l'esecuzione delle rogatorie. V. DE AMICIS, *Erojust : le indicazioni del ministero per rendere effettivo il coordinamento,* in *Dir. Gist.,* I, 24, 2001. pag. 54.

settori dell'economia e della finanza internazionale, lo stesso equilibrio politico dei Paesi industrializzati.

La Convenzione si compone di tre parti fondamentali, la prima delle quali individua un numero minimo di fattispecie che gli Stati firmatari devono adottare al fine di reprimere in modo uniforme la criminalità organizzata[44], prevede che le fattispecie siano punite nella forma di reati consumati e tentati, prevedendo altresì la responsabilità per le persone giuridiche responsabili dei crimini di natura informatica.

La seconda parte della Convenzione prevede misure procedurali relative al regime di comunicazione degli atti e alla loro pubblicazione: l'ordine di esibizione, la perquisizione e il sequestro dei dati informatici, la raccolta dei dati di traffico, l'intercettazione del contenuto dei dati e le misure giurisdizionali.

L'ultima parte è dedicata alla cooperazione internazionale; fa riferimento ai principi generali in materia di cooperazione e nel contempo prosegue con le disposizioni relative all'estradizione e all'assistenza giudiziaria.

Gli obiettivi fondamentali della Convezione sono quelli di armonizzare gli elementi delle infrazioni relative ai computer crimes, di fornire al diritto processuale nazionale i poteri e gli strumenti necessari per perseguire le infrazioni commesse mediante un sistema informatico o nel quadro dei quali esistono prove sotto forma elettronica e di realizzare un regime rapido ed efficace di cooperazione internazionale.

L'Unione Europea, in materia di attacchi contro sistemi informatici, ha proposto una decisione quadro ed ha giustificato il suo intervento in materia di accessi abusivi a sistema informatico, puntando sulla configurabilità di una minaccia per la creazione di un società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia. Questi obiettivi richiedono, infatti, una risposta adeguata da parte dell'Unione Europea[45].

La decisione quadro prevede una serie di definizioni puntuali e specifiche in relazione ai crimini informatici ed agli elementi costitutivi della fattispecie; richiede inoltre l'utilizzo della sanzione penale al fine di reprimere le condotte illecite enunciate.

Le diverse proposte di armonizzazione procedurali e sostanziali a livello europeo ed internazionale si basano, sulla scorta dei dati relativi ai crimini informatici che hanno colpito gli Stati europei negli ultimi anni, su una sanzione penale.

La giustizia penale rappresenta una sfera delicata dei governi nazionali poiché direttamente coinvolta con la libertà degli individui, pertanto stenta a staccarsi dal concetto di sovranità nazionale per migrare nelle competenze normative e giurisdizionali di enti ed organismi sovrannazionali[46].

Lo strumento penale, tuttavia, non appare il più idoneo o comunque non appare sempre adeguato a sanzionare in maniera adeguata le condotte illecite realizzate tramite Internet.

Il diritto penale, infatti, non ha una funzione preminentemente repressiva, il suo scopo principale si identifica nella sua funzione preventiva; nella sua capacità di intervenire a monte della condotta illecita prevenendone la realizzazione. Solo in questo modo è in grado di tutelare realmente il bene giuridico protetto dalle possibili aggressioni. E' stato rilevato che spesso per svolgere questa importante funzione, il diritto penale può ricorrere alla collaborazione da parte dei privati, imponendo loro, ad esempio, l'adozione di idonee misure di sicurezza a protezione dei propri sistemi informatici.

---

[44] Le fattispecie da adottare sono previste dagli art. 2 a 9, per un maggiore approfondimento si rinvia a SARZANA DI SANT'IPPOLITO C., *La Convenzione europea sulla cibercriminalità,* in *Dir. Pen. e Proc.,* n. 4/2002, pag. 509 e seg.

[45] Proposta di decisione quadro n. 2002/0086 del 19/04/2002, COM(2002) 173 definitivo, reperibile sul sito internet www.eu.int

[46] SAVONA E. U., LASCO F., DE NICOLA A,, ZOLFI P., *Processi di globalizzazione e criminalità organizzata transnazionale,* relazione presentata al convegno: "La questione criminale nella socità globale", Napoli, Italia, 10-12 dicembre, 1998 e riportata nel sito ufficile www.transcrime.unitn.it alla voce working papers.

In altre circostanze la condotta criminosa non è eccessivamente lesiva del bene giuridico tutelato e richiede delle forme diverse, rispetto al diritto penale, ed alternative, ad esempio il diritto amministrativo.

Bisogna infine rilevare che molte iniziative dirette a potenziare sistemi informatici di interesse scientifico e tecnologico, sono finanziati direttamente dall'UE attraverso i sui fondi. La lesione cagionata nei confronti di questo genere di sistemi causa sicuramente dei danni ai privati che si vedono "copiare" i propri dati personali a fronte della non perseguibilità degli autori delle condotte illecite, ma lede indirettamente gli interessi economici della stessa UE.

Sarebbe auspicabile un intervento diretto dell'UE al fine di armonizzare la disciplina dei "cybercrimes" e contemporaneamente permettere all'UE di agire con strumenti efficaci alla sanzione di alcune condotte illecite.

L'Unione europea non ha competenza penale, ma ha a sua disposizione gli strumenti propri del diritto amministrativo, soprattutto in relazione all'adozione del Regolamento n. 2988/95 che può definirsi la "*la parte generale"* del diritto amministrativo comunitario. Il regolamento, infatti, raccoglie principi e garanzie generali mutuandoli al diritto penale[47]

5. Conclusioni

La globalizzazione dei mercati e delle telecomunicazioni porta innegabilmente all'esigenza di globalizzare il diritto e le risposte del sistema globale nei confronti di problematiche che si muovono in spazi che trascendono i confini del territorio statale. Lo strumento penale è ben lungi dall'essere inteso come uno strumento disgiunto dalla potestà normativa Statale, dato anche il difficile collegamento tra sistemi di civil law e di common law presenti nel panorama giuridico europeo ed internazionale.

Ancora una volta l'utilizzo dello strumento penale può risultare inadeguato, data l'impossibilità per l'UE di intervenire direttamente in materia penale.

Sarebbe quindi auspicabile un intervento diretto ad unificare e diversificare, a seconda del grado di aggressione al bene giuridico protetto, la disciplina degli accessi abusivi a sistema informatico, in modo da non garantire spazi di impunità e paradisi penali ai soggetti che operano nel mondo della criminalità informatica, soprattutto a livello di criminalità organizzata ,e in grado di sfruttare le differenze tra gli ordinamenti giuridici a proprio vantaggio.

D'altro canto non sembra giusto neppure utilizzare la sanzione penale nei confronti di soggetti denominati White Hacker ,che non sfruttano le proprie conoscenze al fine di danneggiare i sistemi, ma offrono il frutto della propria ricerca al fine di migliorare i sistemi informatici stessi.

Dopotutto un hacker non è un criminale, ma semplicemente un soggetto che, a differenza dell'attacker, ha una spiccata curiosità e che spesso non ha la minima intenzione di arrecare danno alcuno, e che talvolta non concepisce neppure la natura penale della propria condotta, tecnicamente "innocua"!

[47] Il regolamento riconosce apertamente quest'esigenza di tutela sancendo l'obbligo di rispetto dei principi fondamentali quali il principio di legalità, quello di proporzionalità nella commisurazione della pena, del ne bis in idem, di colpevolezza, nonché la garanzia del doppio grado di giudizio, grazie alla presenza del Tribunale di primo grado e della Corte di Giustizia. Cfr BERNARDI F., *Sulle definizioni dei principi di diritto penale*, in *Annali dell'Univeristà di Ferrara-Scienze Giuridiche,* 1992, vol. VI, p. 102; RUGGIERO A., *Gli elementi normativi della fattispecie penale*, I, Napoli, 1965.

Notizie sugli autori

Nadina Foggetti. Nadina Foggetti ha una Laurea in Legge conseguita presso l' Università degli Studi di Modena e Reggio Emilia, con una tesi su "Legalità penale ed Unione Europea" per la quale ha conseguito il massimo dei voti. Ha partecipato a diversi corsi specialistici sulla legislazione informatica, soprattutto nel campo dell'applicazione del Diritto Penale a casi transnazionali. Attualmente lavora come praticante avvocato nello studio di A. G. Orofino a Casamassima. Email rosmina AT tiscalinet.it