Dirett. Servizio 45/18

Procura della Repubblica
presso il Tribunale ordinario di Cosenza

prot. Nr.

Protocollo investigativo inerente ai seguenti reati commessi attraverso la rete Internet: truffe, utilizzazione fraudolenta di carte di pagamento, diffamazioni.

Oggetto di questo protocollo sono le indagini riguardanti reati, commessi attraverso la rete INTERNET ovvero l'utilizzazione di un sistema informatico, per i quali non ricorre la competenza del giudice distrettuale ai sensi dell'art.11 l.18 marzo 2008 nr.48.

L'elevato numero dei procedimenti iscritti con caratteristiche seriali, la necessità di una specifica professionalità investigativa e la natura specialistica degli accertamenti da compiere impone l'adozione di un protocollo investigativo, che magistrati dell'Ufficio e polizia giudiziaria sono tenuti ad osservare.

PREMESSA

Per accedere alla rete Internet occorre un computer (fisso, portatile, telefonino di ultima generazione), una linea telefonica (fissa, mobile) ed un abbonamento Internet con un I.S.P.[1] (Internet Service Provider, ad es. Tiscali, Virgilio)

La rete Internet è globale, per cui gli I.S.P. rispondono alla normativa dello stato ove hanno la sede legale.

Nel caso di I.S.P. stranieri, per acquisire i dati di interesse, non sempre è necessario avviare una commissione rogatoria.

In particolare, quanto agli Stati Uniti d'America, ove hanno sede i più importanti gestori Internet, come ad esempio Facebook, Gmail, Hotmail, Yahoo e Twitter, è necessario presentare una rogatoria internazionale al Dipartimento di Giustizia degli Stati Uniti solamente al fine di ottenere i contenuti degli account o profili, come ad esempio comunicazioni private, altre informazioni non pubbliche, dati internet riguardanti il traffico dell'account, come ad esempio i nomi e gli indirizzi IP dei mittenti e destinatari dei messaggi, così come le informazioni sulle date e gli orari delle comunicazioni.

---

[1] Un **internet service provider** (termine mutuato dalla lingua inglese che tradotto letteralmente in italiano significa "fornitore di servizi Internet"), in sigla **ISP**, anche abbreviato in **provider**, è una struttura commerciale o un'organizzazione che offre agli utenti (residenziali o imprese) servizi inerenti Internet i principali dei quali sono l'accesso a Internet e la posta elettronica.

Diversamente, non è necessario presentare una rogatoria verso gli USA per i seguenti fini:

- Chiedere il congelamento dei contenuti dell'account. Infatti, dopo aver appreso l'esistenza dell'account, la conservazione dei dati in esso contenuti dovrebbe essere fatta immediatamente, seguendo la procedura di seguito indicata, in quanto se non si procede con il congelamento dei dati informatici, questi potrebbero essere cancellati. La polizia giudiziaria può richiedere la conservazione dei dati, per un periodo fino a 180 giorni, accedendo direttamente ai siti web dedicati in materia e indirizzati alle forze dell'ordine (ad esempio, facebook.com/records).

- Ottenere i dati anagrafici dell'intestatario dell'account. La polizia giudiziaria può chiedere questi dati tramite i siti web sovramenzionati.

- Ottenere i dati di accesso dell'utente (i cosidetti "access logs," ad esempio, dati, orari, indirizzi IP associati a ciascun accesso dell'utente), tramite l'utilizzo degli stessi siti. Successivamente, la polizia potrà scaricare i dati direttamente sul proprio computer in Italia.

Un **crimine informatico** è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica. Tutti i reati informatici sono accomunati da:

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

PANORAMA EUROPEO

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

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

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

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

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

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

PANORAMA ITALIANO

Il legislatore, con la L. 547/93, ha scelto di collocare i nuovi reati informatici accanto alle figure di reato già esistenti.

- La *frode informatica* viene associata alla frode "tradizionale" con la differenza che viene realizzata per mezzo di uno strumento informatico. La legge 547 del 1993 aggiunge al Codice Penale l'art. 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Non viene identificato come frode informatica l'indebito utilizzo di carte di pagamento magnetiche che è invece disciplinato dall'art. 55, comma 9 del Decreto Legislativo 231/07.
- La *falsificazione di documenti informatici*. I documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali e l'art. 491-bis c.p. prevede l'applicabilità delle disposizioni sulla falsità in atti pubblici e privati. La falsificazione in comunicazioni informatiche ricalca invece il delitto di falsità in scrittura privata (art. 485 c.p.).
- Le *aggressioni all'integrità dei dati*. La legge 547 del 1993 amplia le precedenti disposizioni in materia e integra al Codice Penale l'art. 635-bis sul danneggiamento dei sistemi informatici e telematici, l'art. 615-quinquies sulla diffusione di virus e malware, l'art. 392 sulla violenza sulle cose (a tal proposito la legge 547 del 1993 precisa le situazioni dove le aggressioni riguardano beni informatici) ed infine l'art. 420 sul reato di attentato ad impianti di pubblica utilità. Forse l'unico caso giudiziario di diffusione di virus per cui si è celebrato un dibattimento (sia in primo grado, sia in appello) è quello deciso dal Tribunale penale di Bologna con la sentenza 1823/05 (la cui decisione è stata parzialmente ribaltata in appello) a proposito del "Caso Vjierika".
- Le *aggressioni alla riservatezza dei dati e delle comunicazioni informatiche*. Riguardo le forme di intrusione nella sfera privata altrui si incriminano l'accesso abusivo ad

un sistema informatico o telematico (art. 615-ter c.p.), la detenzione o diffusione abusiva di codici di accesso (art. 615-quater c.p.) e la rivelazione del contenuto di documenti segreti (art. 621 c.p.), includendo i documenti protetti contenuti su supporti informatici.

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

La legge 48/08, che recepisce la Convenzione di Budapest sul crimine informatico, ha modificato il codice penale e quello di procedura penale riconoscendo implicitamente il ruolo dell'informatica forense nel processo penale.

L'art.11 della citata legge innova il c.p.p. in materia di competenza:

Art. 11.

(Competenza)

1. All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma:

«*3*-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter* e 640-*quinquies* del codice penale, le funzioni indicate nel comma 1, lettera *a)*, del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

L'art. 8 introduce la perquisizione informatica:

Art. 8.

(Modifiche al titolo III del libro terzo del codice di procedura penale)

1. All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

2. All'articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente:

«*1*-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

3. All'articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti,

documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».

CIO' PREMESSO

1. In relazione ai reati che prevedono l'utilizzo dello strumento informatico, di competenza della Procura Ordinaria, l'attività di indagine sarà normalmente delegata alla Sezione di Polizia Giudiziaria della PS. In tal senso i magistrati, assegnatari del fascicolo processuale, qualora ritengano necessario, ai fini della definizione del procedimento, espletare attività investigativa, delegheranno detta Sezione di PG. Resta inteso che, in relazione alla natura del procedimento, gli stessi potranno delegare altra PG. (in particolare nei casi di assoluta complessità la Polizia Postale di Reggio Calabria). In tale eventualità informeranno il Procuratore della Repubblica, che ha il compito di monitorare l'efficacia e la funzionalità di questo protocollo.
2. Nel conferimento della delega d'indagine si terrà conto che l'attività può essere proficuamente proseguita, senza particolari difficoltà, laddove vi siano riferimenti italiani: indirizzi IP (vedi nota 2), siti, indirizzi di posta elettronica. Per accertare la nazionalità degli stessi si possono interrogare, tra gli altri, i seguenti siti Internet attraverso i quali si possono reperire anche i numeri telefonici o e-mail di contatto:
    a. www.samspade.org
    b. www.ripe.net

   Di seguito si evidenziano indicazioni operative quanto ai reati informatici di competenza delle procure ordinarie.

3. Per quanto riguarda il reato di truffa ex art. 640 c.p., posta in essere attraverso siti Internet, si rende necessario acquisire:
    a. anagrafica relativa alla registrazione della mail utilizzata per contatti, comprensiva di Indirizzo IP[2], giorno ed ora. La richiesta può essere effettuata direttamente dalla P.G. al Provider di riferimento. Ottenuto l'indirizzo IP, per individuare la linea telefonica attraverso la quale è stata effettuata la connessione incriminata si rende necessario richiedere un decreto di acquisizione al P.M.
    b. dati di registrazione dell'utente che ha posto in essere la truffa al gestore del sito. Nel caso del sito di EBAY, la richiesta può essere effettuata direttamente dalla P.G. a "eBay Europe S a.r.l." LUSSEMBURGO, Nr. FAX: 0230410366.-

[2] Un **Indirizzo IP** è un numero che identifica univocamente un dispositivo collegato a una rete informatica che comunica utilizzando lo standard IP (Internet Protocol). Un indirizzo IP può essere visto come l'equivalente di un indirizzo stradale o un numero telefonico riferito a dispositivi collegati ad una qualsiasi rete telematica. Infatti, così come un indirizzo stradale o un numero telefonico identificano rispettivamente un edificio o un telefono, un indirizzo IP identifica univocamente uno specifico computer o dispositivo di rete. Gli indirizzi IP possono essere assegnati localmente per realizzare una LAN (Local Area Network), come succede con la numerazione degli interni di un edificio. Ma, al contrario degli indirizzi stradali, gli indirizzi IP possono mutare il loro valore a seconda di molti fattori (diversa LAN, indirizzamento dinamico) o a seconda della volontà dell'utente.

c. documenti utilizzati per l'attivazione delle carte di pagamento (nel caso di POSTEPAY indirizzare la richiesta direttamente all'ufficio postale emittente la carta, ovvero nel caso in cui ciò non si evinca, a POSTE ITALIANE S.p.A. Bancoposta – Operazioni - Servizio di Clientela e Condizioni – ROMA, tel. fax 06/59580666
d. E' opportuno verificare la conformità dei documenti con l'Ente che li ha emessi.

In questi casi gli utenti si accordano, tramite servizi di commercio online (in particolare eBay), per vendere ed acquistare della merce, prevedendo come modalità di pagamento·

- il trasferimento di denaro tramite Western Union/Money Gram,

- l'uso di vaglia online,

· l'effettuazione di ricariche di carte di credito prepagate (ad esempio Postepay)

· altri sistemi di pagamento elettronico (es. paypal).

Molto diffuso anche l'utilizzo di assegni circolari falsi (molto spesso stranieri): tale tipologia di truffa è inizialmente emersa soprattutto in relazione alla piattaforma di secondamano.it, le cui modalità sono peraltro segnalate agli utenti dal relativo sito.

Dall'esperienza investigativa maturata si è rilevato che le connessioni ad Internet usate per commettere gli illeciti vengono effettuate a partire da macchine in precedenza violate (cd. macchine "bucate" o "zombie"20) o da postazioni presenti all'estero. In quest'ultimo caso i relativi accertamenti investigativi saranno di difficileesecuzione se non con ricorso a collaborazioni di Polizia Giudiziaria di differenti Stati e/o richieste rogatoriali

La persona offesa dovrà fornire tutti gli elementi utili al proseguo delle indagini (indicando innanzitutto la piattaforma di commercio elettronico/sito internet relativo all'acquisito), ed in particolare allegare tutti i dati relativi alla inserzione/annuncio di vendita apparso sulle pagine Internet, comprensivo di URL completa della pagina relativa alla vendita; dovrà altresì indicare eventuali dati relativi allapartita IVA/codice fiscale del venditore (ove reperibili dalla inserzione/annuncio o dal sito internet); copia (meglio se informatica) di tutte le comunicazioni intercorse via e-mail (comprensive degli header) con il sedicente venditore, indicando altresì – in caso di contatti telefonici – il numero chiamato ed (ove disponibile) anche il numero chiamante; indicazione degli elementi che fanno presuppone la truffa, e segnatamente gli artifizi e raggiri posti in essere dal sedicente venditore per conseguire l'ingiusto profitto, che sostanziano il reato distinguendolo dal semplice inadempimento di natura civilistica.

4. Per quanto riguarda il reato di utilizzazione fraudolenta di carta di pagamento, ex art. 493 ter cp, attraverso Internet, si rende necessario:
   a. acquisire estratto conto dettagliato sulle spese contestate;
   b. esperire accertamenti sui siti web verso i quali siano stati effettuati pagamenti (per i motivi sopra specificati, in caso di siti stranieri, si rende necessario la commissione rogatoria);
   c. nel caso di addebiti per ricariche telefoniche, esperire accertamenti tradizionali nei confronti degli intestatari delle utenze telefoniche ed accertamenti presso i siti delle compagnie telefoniche delle utenze SIM ricaricate al fine di acquisire gli indirizzi IP che hanno disposto la ricarica (es. nel caso di ricarica di telefono mobile WIND, l'operazione illecita sarà stata effettuata sul sito della società "wind", alla quale dovrà essere inoltrata richiesta di fornire gli indirizzi IP con data ed orario.

5. Per quanto riguarda il reato di Diffamazione ex art. 595 c.p., si rende necessario:
   a. esperire accertamenti sui siti web;
   b. acquisire, con richiesta della P.G. i LOGFILE[3] relativi ad eventuali utenti Internet (identificati da NICK[4]) che hanno inserito commenti su siti Internet di natura diffamatoria

Si deve prestare particolare attenzione agli orari dei LOGFILE forniti dai vari PROVIDER che, seppur italiani, potrebbero avere i propri SERVER settati con orari internazionali, suscettibili pertanto di variazioni rispetto all'orario nazionale, in ragione del differente fuso.

In tal caso, per ottenere il corrispondente orario italiano si può interrogare, tra gli altri, il seguente sito Internet, www.timeanddate.com

Al fine di acquisire ulteriori indizi a carico del reo, sarebbe opportuno completare la fase investigativa con un provvedimento di perquisizione che consentirebbe, intanto, di accertare chi, all'interno di un nucleo familiare, abbia la materiale disponibilità del materiale informatico e, soprattutto, di sequestrare ciò che si ritiene utile alle indagini (materiale informatico, documenti cartacei ed altro).

Ulteriore ed importantissima fase è costituita dall'analisi del materiale in sequestro che potrebbe consentire di trovare riscontri alle ipotesi investigative (utilizzatore, connessione a siti oggetto d'indagine, documenti). Durante tale fase si dovrà tenere conto del dettato normativo introdotto dalla L. 48/08 sopra citata, ovvero, laddove l'accertamento venga effettuato in modalità irripetibile (per es. accendendo un PC) prevedendo le garanzie di cui all'art. 360 c.p.p.. Si segnala, al fine di evitare future problematiche sull'utilizzabilità processuale dell'atto d'indagine, l'opportunità di procedere al backup dei dati, avvalendosi dell'ausilio, quale ausiliario di PG., di esperto tecnico, con tutte le garanzie difensive per l'indagato, che si concretano nella possibilità di assistere personalmente e/o tramite il proprio difensore ovvero persona di propria fiducia alle operazioni di backup su cui l'ufficiale di PG, una volta terminate, redigerà verbale che verrà sottoscritto da tutti i presenti.

[3] Tabulati relativi alla connessione Internet
[4] Soprannomi

6. Per quanto concerne il furto di identità di cui all'art. 494 codice penale si tratta di un fenomeno variegato, ricomprendente:

   A) tutti i tentativi di phishing tramite invio di e-mail (in questo caso la più corretta qualificazione giuridica deve essere quella di 56, 494, 640-ter c.p.)

   B) altri furti di identità, anche consumati, rispetto ai quali la persona offesa non lamenta di aver ricevuto – al momento della denuncia/querela – un danno.

Si rileva che gli accertamenti di tipo tecnico informatico sugli illeciti riconducibili al fenomeno del "phishing" risultano spesso impossibili alla luce delle informazioni raccolte in sede di denuncia/querela poiché i link relativi ai siti clone sono visualizzabili a partire dall'e-mail in formato elettronico e per breve tempo.

Se tali dati vengono acquisiti, le verifiche, anche se teoricamente perfezionabili, non forniscono elementi utili per l'identificazione dell' autore dei reati posti in essere, dato che si è visto in pregresse indagini che l'invio dei messaggi avviene dall'estero, che l'ubicazione delle macchine ospitanti siti web clone è estera e che vengono usate macchine già violate o senza protezioni; tali circostanze non permettono di svolgere ulteriori attività investigative senza il ricorso di una rogatoria internazionale (spesso impossibile perché non sussistono le condizioni giuridiche di reciprocità con lo stato estero da cui proviene l'attacco), il cui esito, anche se potenzialmente positivo, comunque difficilmente consentirebbe di giungere all'individuazione dei responsabili della frode.

Occorrerà innanzitutto verificare – dandone ampia descrizione nel testo della querela – cosa è stato fatto in concreto con i propri dati.

E' importante ribadire che se la persona offesa ha cancellato la e-mail di phishing ricevuta, nessun tipo di accertamento sarà possibile.

Copia di questo protocollo sarà inviata ai magistrati in servizio presso questa Procura, ai responsabili dei servizi e delle sezioni di Polizia giudiziaria, operanti nel circondario di Cosenza, nonché, per opportuna conoscenza, a S.E. il Procuratore Generale presso la Corte di Appello di Catanzaro, al sig. Presidente del Tribunale.

Cosenza 8 giugno 2018

IL PROCURATORE DELLA REPUBBLICA
Mario SPAGNUOLO