Direttiva n. 6/18

Procura della Repubblica

presso il Tribunale ordinario di Cosenza

(procura.cosenza@giustizia.it)

Al Sig. Questore della Provincia di Cosenza
Al Sig. Comandante Provinciale dei Carabinieri di Cosenza
Al Sig. Comandante Provinciale della Guardia di Finanza di Cosenza
Al sig. Responsabile Polizia Postale Reggio Calabria
Al sig. Responsabile Polizia Postale Cosenza
Ai. Sigg.ri Responsabili Sezioni Pg. c/o Procura della Repubblica Cosenza
Al Procuratore Aggiunto
Ai Signori Sostituti Cosenza
Ai V.P.O. Sede

e p.c.
A S.E. Il Procuratore Generale
di Catanzaro

OGGETTO : **Protocollo investigativo inerente ai seguenti reati commessi attraverso la rete Internet. Aggiornamento del protocollo del 28.6.2018.**

D'intesa con il responsabile del Compartimento della Polizia Postale di Reggio Calabria si evidenziano nuove linee investigative, che aggiornano il precedente protocollo del 28.6.2018, in ordine ai seguenti reati :

- **indebito utilizzo e falsificazione di carte di credito e pagamento ex art. 493 ter c.p.**
- **frode informatica ex art. 640 ter c.p.**
- **truffa on line di cui all'art. 640 c.p.**

PREMESSA

La "*Direttiva sui comparti di specialità delle forze di polizia e sulla razionalizzazione dei presidi di polizia*", emanata del Ministro dell'Interno con decreto del 15/8/2017, definisce le modalità di esercizio, in via esclusiva o preminente, da parte delle Forze di Polizia, dei compiti istituzionali nei relativi comparti di Specialità, in ottemperanza a quanto prevsito dall'art. 2, comma 1, del d.lvo 177 del 2016.

Il decreto richiama le modifiche normative succedutesi nel tempo, che hanno visto l'introduzione nel nostro ordinamento dei reati informatici in senso proprio e le modifiche di quelli tradizionali, alla luce della possibilità che siano commessi avvalendosi di strumenti info-telematici. Esso contiene, inoltre, specifici riferimenti alle norme che individuano gli organi del Ministero dell'Interno deputati all'esercizio delle competenze specialistiche in materia di pedopornografia e di protezione delle infrastrutture critiche informatizzate, presso il Servizio Polizia Postale e delle Comunicazioni.

Giova, pertanto, premettere che il nostro ordinamento giuridico prevede i seguenti "crimini informatici", introdotti dalla Legge n° 547/1993 e dalla Legge n° 48/2008:

1. *Accesso abusivo ad un sistema informatico o telematico* (art. 615-*ter* CP);
2. *Detenzione e diffusione abusiva di codici di accesso a sistemi infotelematici* (art. 615-*quater* CP);
3. *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615-*quinquies* CP);
4. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617-*quater* CP);
5. *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche* (art. 617-*quinquies* CP);
6. *Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche* (art. 617-*sexies* CP);
7. *Danneggiamento di informazioni, dati e programmi informatici* (art. 635-*bis* CP);
8. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* (art. 635-*ter* CP);
9. *Danneggiamento di sistemi informatici e telematici* (art. 635-*quater* CP);
10. *Frode informatica* (art 640-*ter* CP);
11. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica* (art. 640-*quinquies* CP);
12. *Falsità materiale o falsità ideologica commesse dal pubblico ufficiale o dal privato, altre falsità ed uso di atti falsi, se riguardanti documenti informatici aventi efficacia probatoria* (art. 491-*bis* CP)[1];
13. *Violazione, sottrazione e soppressione di corrispondenza informatica o telematica* (art. 616 CP);
14. *Rivelazione del contenuto di documenti segreti - solo ipotesi 2° comma* (art. 621 CP);
15. *Rivelazione del contenuto di corrispondenza informatica o telematica* (artt. 618 e

[1] Si tratta delle ipotesi di falsità ed uso di atti falsi previste dagli artt. da 476 a 491 CP, se relative a documenti informatici.

632-*bis* CP);

16. *Danneggiamento di sistemi informatici o telematici di pubblica utilità* (art. 635-*quinquies* CP).

I suddetti reati vanno distinti da quelli nei quali il dispositivo informatico sia solo lo strumento attraverso il quale, in tutto o in parte, vengono commessi.

La casistica più significativa ricomprende i seguenti:

1. *Trattamento illecito di dati personali* (art. 167 del D.Lgs. n° 196/2003);
2. *Sostituzione di persona* (art. 494 CP);
4. *Diffamazione* (art. 595 CP);
5. *Minaccia* (art. 612 CP);
6. *Atti persecutori* (art. 612-*bis* CP);
7. *Truffa* (art. 640 CP);
8. *Indebito utilizzo e falsificazione di carte di credito e di pagamento* (493-*ter* CP)

Riguardo alle specifiche competenze assegnate dalla vigente normativa alla Polizia Postale e delle Comunicazioni, vanno rammentate le seguenti norme:

1. decreto-legge n. 144 del 27 luglio 2005 (convertito in Legge 155/2005, recante *"misure urgenti per il contrasto al terrorismo internazionale"*, il cui **Art. 7-bis. - in materia di Sicurezza telematica, recita: "*I. Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n.801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'Interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.*"**
   La normativa Pisanu ha previsto, quindi, l'**istituzione di un Centro incardinato presso il Servizio Polizia Postale e delle Comunicazioni**, quale Organo del Ministero dell'Interno per la sicurezza delle comunicazioni, dedicato per l'appunto alla protezione delle I.C. informatizzate, direttamente impegnato nel prevenire e contrastare attività criminali a matrice comune, organizzata e terroristica e garante istituzionale dell'attività di info-sharing tra le diverse I.C. Ai fini dell'attuazione di quanto stabilito dal citato art. 7 bis, il Ministro dell'Interno con il **decreto del 9 gennaio 2008** (art.3), ha previsto l'**istituzione del *"Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C.*** che il Capo della Polizia (**decreto del 7/8/2008**) ha successivamente istituito in seno al Servizio Polizia Postale e delle Comunicazioni.

2. Legge 3 agosto 1998 n. 269, art.14 e artt. 14-bis ter quater e quinquies, introdotti dalla Legge n.38 del 6/2/2006, istitutiva anche del C.N.C.P.O. presso il Servizio Polizia Postale e delle Comunicazioni, organo del Ministero dell'Interno cui è affidata in via esclusiva l'attività di prevenzione e contrasto in materia di pedo-pornografia online.

3. Legge 17/4/2015 n.43, di conversione del D.L. 18/2/2015 n.7 che all'art. 2, comma 2 affida il costante aggiornamento dell'elenco dei siti utilizzati per le attività e le condotte di cui agli artt. 270bis e 270sexies c.p. all'Organo del Ministero dell'Interno per la sicurezza e la regolarità delle telecomunicazioni.

Alla luce delle competenze sopra delineate e della crescita esponenziale dei reati commessi tramite l'utilizzo della rete internet e, in particolare, di quelli contro il patrimonio, si è ritenuto opportuno predisporre il presente protocollo investigativo, atto a fornire le linee guida circa le modalità di acquisizione delle denunce e gli accertamenti tecnici da espletare in ordine ai reati di:

- **indebito utilizzo e falsificazione di carte di credito e pagamento ex art. 493 ter c.p.**
- **frode informatica ex art. 640 ter c.p.**
- **truffa on line di cui all'art. 640 c.p.**

Indebito utilizzo e falsificazione di carte di credito/debito e frode informatica

Nelle ipotesi di uso di carta smarrita dal titolare o illecitamente sottrattagli, anche solo temporaneamente e in tutti gli altri casi, compreso l'uso dei soli dati identificativi visibili della carta (nome titolare, PAN, data scadenza, codice di sicurezza)[2], ovvero l'uso di carta falsificata o alterata (c.d. "clonazione"), quando la denuncia viene resa, risulta utile acquisire dalla parte lesa le seguenti informazioni:

- in caso di smarrimento o sottrazione, loro modalità (se riguardanti episodio precedentemente denunciato, allegare copia della relativa denuncia);
- attualità del possesso e modalità di custodia del PIN; andrà chiarito, in particolare, se tra le frequentazioni in ambito privato, anche familiare, o lavorativo vi siano soggetti che, sulla base delle modalità di custodia adottate, possono avere avuto accesso al PIN;
- lista delle operazioni disconosciute;
- lista delle operazioni immediatamente precedenti alla prima, in ordine di tempo, delle operazioni disconosciute[3];
- in caso di *phishing* (adescamento on-line della vittima, tramite invio di una *email* per convincerla a fornire dati riservati o contenente programmi malevoli nascosti, attivabili tramite azione su *link* o files allegati) su carta di credito o di pagamento, stampa completa[4] della *e-mail*.

- Di seguito si specificano gli accertamenti da eseguire suddivisi in base alla casistica più frequente riscontrata da quest'ufficio.

---

2 I dati identificativi visibili di alcune carte possono essere utilizzati per effettuare pagamenti o versamenti sul web; inoltre, i dati identificativi visibili di tutte le carte possono essere utilizzati, senza la materiale disponibilità della carta cui si riferiscono, per pagare beni o servizi tramite POS. In tale ultima ipotesi è evidente quantomeno la negligenza dell'esercente che gestisce il POS, per avere effettuato l'operazione senza esibizione materiale della carta.

3 Tale elenco è fondamentale per individuare, in caso di uso di carta alterata o contraffatta, il "punto fisico di compromissione", cioè il luogo ove la carta è stata "violata" (di norma all'interno di un esercizio commerciale, contestualmente ad un pagamento legittimo). Tale aspetto è quasi sempre sottovalutato, ma potrebbe fornire un contributo rilevante allo sviluppo successivo delle indagini.

4 Cioè la stampa anche dell'intestazione (c.d. *header*) del messaggio.

a) *Uso di carte per operazioni presso ATM*

- individuare l'ubicazione fisica dell'ATM e l'Istituto di Credito che lo gestisce;
- acquisire tempestivamente e visionare le immagini riprese dai sistemi di sicurezza dell'ATM e dell'Istituto di Credito;
- se si tratta di operazione di pagamento, acquisire gli estremi completi dell'operazione e del beneficiario; quest'ultimo dovrà essere escusso ai sensi dell'art. 351 CPP, procedendo ai sensi di legge qualora emergano indizi di reità;
- se si tratta di operazione di ricarica di un'utenza telefonica, acquisire gli estremi completi dell'operazione ed accertare presso il gestore telefonico interessato l'identità del titolare dell'utenza; quest'ultimo dovrà essere escusso ai sensi dell'art. 351 CPP, procedendo ai sensi di legge qualora emergano indizi di reità.

b) *Uso di carte per pagamenti presso POS*

- individuare l'ubicazione fisica del POS e l'esercente che lo gestisce;
- accertare preliminarmente se l'operazione è avvenuta tramite lettura della carta o tramite digitazione del PAN (Primary Account Number - numero composto da 16 cifre divise in gruppi da 4 stampato sul fronte della carta);
- acquisire tempestivamente e visionare le immagini riprese durante l'operazione fraudolenta dai sistemi di sicurezza dell'esercizio commerciale, qualora ne sia dotato;
- acquisire lo scontrino fiscale relativo ai beni acquistati o ai servizi erogati, verificando se data e ora corrispondono alla data ed all'ora dell'operazione di pagamento sul POS;
- escutere l'esercente ai sensi dell'art. 351 CPP, procedendo ai sensi di legge qualora emergano indizi di reità.

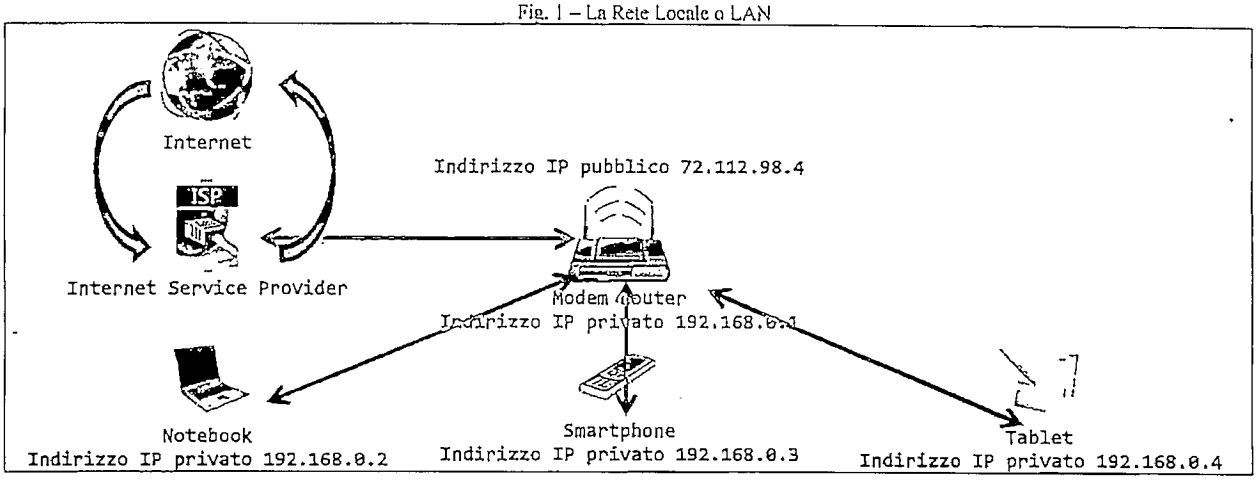
c) *Uso di carte per acquisto di beni o servizi via Internet*

- localizzare il sito sul quale l'operazione è stata compiuta e verificare se gestito da società con sede in Italia o all'estero (in questo caso accertare se esistano rapporti di collaborazione che permettano l'acquisizione delle informazioni anche in assenza di Ordine di Indagine Europeo o Rogatoria Internazionale);
- verificare se il venditore *on-line* del bene o il fornitore *on-line* del servizio hanno operato la vendita o la fornitura dal territorio nazionale (chiedere al gestore della piattaforma di *e-commerce* i relativi dettagli sulla transazione oppure dettagli al gestore dei canali telematici attraverso i quali sono avvenuti i contatti tra venditore ed acquirente);
- se il riscontro è positivo, acquisire i dati relativi al destinatario del bene o al beneficiario del servizio, se negativo darne atto nell'informativa trasmessa all'A.G.;
- qualora vengano forniti i dati di cui sopra, verificare la nazionalità dei gestori degli indirizzi IP (tramite i siti di *"who is"*) per eventuali ulteriori accertamenti;
- predisporre CNR interlocutoria richiedendo alla Procura della Repubblica, qualora sia necessario, l'emissione di ordine di esibizione dati da notificare al gestore del server o del sito per individuare ogni dettaglio utile in merito all'operazione compiuta, incluso l'indirizzo IP dal quale l'operazione è stata compiuta (o gli indirizzi IP nel caso di più operazioni);
- individuare l'ISP (Internet Service Provider) che ha rilasciato l'indirizzo IP dal quale l'operazione è stata compiuta (o gli ISP in caso di più indirizzi);
- facendo seguito alla CNR interlocutoria, richiedere alla Procura della Repubblica

l'emissione di ordine di esibizione dati da notificare all'ISP, allo scopo di associare l'indirizzo IP al titolare del contratto di fornitura del servizio internet;

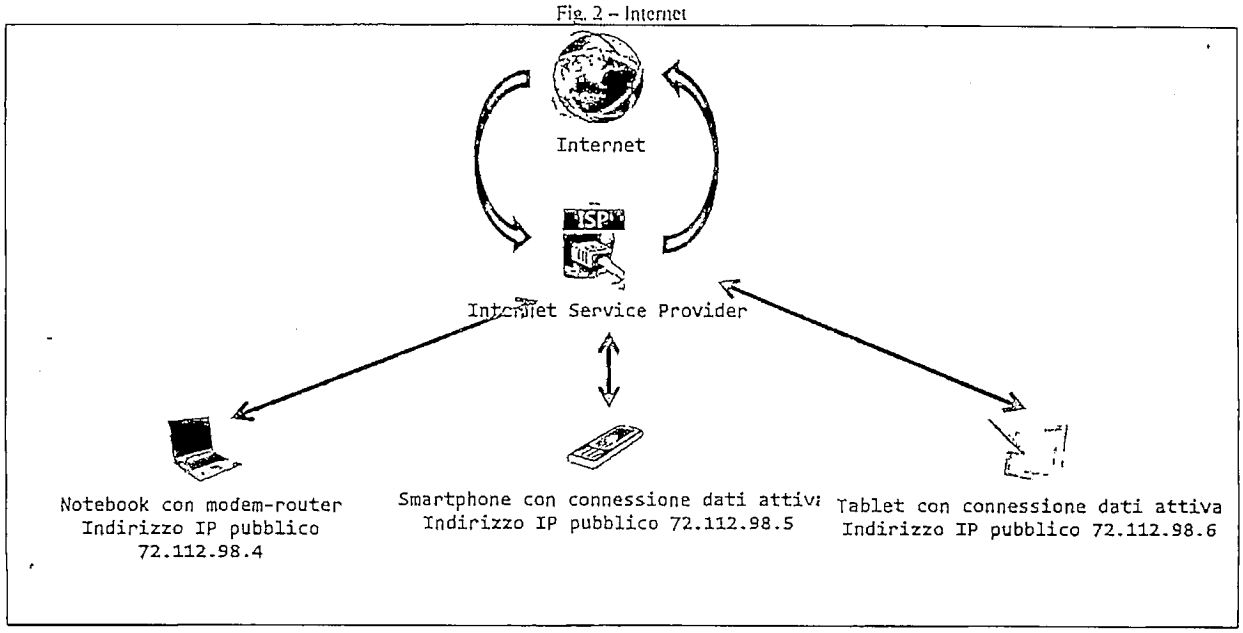
- escutere, ai sensi dell'art. 351 CPP, il titolare del contratto di fornitura del servizio internet ed il destinatario (se noto) dei beni o servizi acquistati, procedendo ai sensi di legge qualora emergano indizi di reità;
- predisporre CNR conclusiva, riferendo sull'esito delle indagini svolte.

Fig. 1 – La Rete Locale o LAN



Come si vede in Fig. 1, i dispositivi (un Notebook, uno Smartphone ed un Tablet) non possiedono un Indirizzo IP pubblico, ma viene loro assegnato dal modem-router un Indirizzo IP privato. Quindi, per accedere ad Internet, essi condividono l'Indirizzo IP pubblico assegnato al loro modem-router e sono identificabili univocamente solo all'interno della Rete Locale.

Fig. 2 – Internet



Come si vede nella Fig. 2, i dispositivi, che non fanno parte di una rete LAN, sono direttamente connessi al loro ISP attraverso un Modem USB (il Notebook) o attraverso una SIM telefonica

abilitata al traffico dati (Smartphone e Tablet); ciascuno di essi è quindi dotato di un differente Indirizzo IP pubblico che lo identifica univocamente.

d) ***Uso di carte per ricarica on-line di altre carte (PayPal, PostePay, Carta Lys) o "conti-gioco"***

- accertare le generalità complete del soggetto o dei soggetti che risultano titolari della carta o delle carte sulle quali le ricariche risultano effettuate;
- predisporre CNR interlocutoria richiedendo alla competente Procura della Repubblica l'emissione di ordine di esibizione dati da notificare al gestore (PayPal, PostePay, Carta-Lys o "conto-gioco") per individuare l'indirizzo IP dal quale l'operazione è stata compiuta (o gli indirizzi IP nel caso di più operazioni);
- individuare l'ISP che ha rilasciato l'indirizzo IP dal quale l'operazione è stata compiuta (o gli ISP in caso di più indirizzi);
- facendo seguito alla CNR interlocutoria, richiedere alla Procura della Repubblica l'emissione di ordine di esibizione dati da notificare all'ISP, allo scopo di associare l'indirizzo IP al titolare del contratto di fornitura del servizio internet;
- escutere, ai sensi dell'art. 351 CPP, il titolare del contratto di fornitura del servizio internet e l'intestatario o gli intestatari delle carte ricaricate, procedendo ai sensi di legge qualora emergano indizi di reità;
- predisporre CNR conclusiva, riferendo sull'esito delle indagini svolte.

Giova, tuttavia, precisare che la numerosa casistica investigativa ha dimostrato che, nella maggior parte dei casi, gli accertamenti sul beneficiario del denaro provento di reato risulta essere la principale, nonché fruttuosa attività per l'identificazione del reo.

Invero, gli ulteriori accertamenti esperiti a seguito dell'identificazione del soggetto a cui risulti intestata l'utenza telefonica abbinata agli IP delle connessioni tramite le quali è stato perpetrato il reato, possano essere privi di utilità.

Infatti, tali utenze risultano spesso attivate con documenti falsi o nominativi di fantasia o comunque riportano a persone per le quali non è possibile effettuare alcuna verifica in quanto non censite nelle anagrafi di interesse.

Altresì, gli intestatari delle utenze mobili inserite negli annunci dei siti internet il più delle volte sono fittizi, o qualora si tratti di persone reali risultano nella maggior parte dei casi del tutto ignare della truffa perpetrata.

Per di più, anche nel caso si tratti di utenze fisse, pur non potendo escludere la responsabilità di persone che vi abitano o frequentano le abitazioni ove l'utenza risulta installata, non è mai possibile determinare in modo certo il responsabile del reato che non può essere identificato automaticamente nell'intestatario della linea telefonica.

Truffa on line

Quale reato in ambito infotelematico, l'ipotesi ricorre quando taluno, anche senza commettere un crimine informatico in senso proprio, mediante il Web induce qualcuno in errore con artifizi o raggiri, procurando un ingiusto profitto con altrui danno.

Ciò può avvenire sia su un sito specializzato (*e-commerce*, quale ad es. *e-Bay*, o anche una semplice "bacheca annunci", ad es. "subito.it"), o molto più semplicemente attraverso contatti intercorsi su *chat* o *forum*.

Si possono quindi presentare situazioni tra loro diverse, in quanto, mentre i siti specializzati richiedono di norma, per venditore ed acquirente, una registrazione alla quale segue la generazione di un profilo, ciò non sempre avviene per i rimanenti siti.

In tutti questi casi è possibile che per la commissione del reato vengano utilizzati profili o caselle email riconducibili all'autore del reato e non fraudolentemente carpiti.

Quando la denuncia viene resa, risulta utile acquisire dalla parte lesa le seguenti informazioni:

1. sito sul quale è avvenuto il contatto tra acquirente e venditore
2. nome utente e/o ID-profilo del venditore o dell'acquirente (a secondo di chi, tra i due, ha realizzato la truffa), casella *e-mail* ad esso collegata (se nota);
3. stampa completa delle *e-mail* eventualmente inviate dal querelato;
4. modalità di pagamento del bene o del servizio e suoi estremi identificativi.

Nel caso in cui il crimine venga consumato tramite i portali di *e-commerce* è necessario svolgere la seguente attività:

1. Richiesta dati di registrazione dell'utente che ha posto in essere la truffa al gestore del sito;
2. Verifica dei dati e dei documenti utilizzati per l'attivazione delle carte di pagamento al fine di verificarne la conformità con l'ente che li ha emessi;
3. Accertamenti sulla titolarità della carta sulla quale è stato convogliato il denaro oggetto di truffa.
4. Qualora vengano comunicati indirizzi IP verificare se gli stessi risultino gestiti da ISP Italiani o stranieri.
5. Nel caso di IP italiani, circoscrivere l'arco temporale relativo alla commissione del reato e richiedere all'Autorità giudiziaria un decreto per l'acquisizione dei *caller* ID per l'dentificazione dell'utenza dalla quale proviene la connessione;
6. Richiesta di accertamenti anagrafici sulla persona intestataria della linea telefonica.

Come precisato in precedenza, tale crimine può essere stato commesso anche utilizzando profili o caselle *e-mail* generate, sotto il profilo tecnico, in modo lecito.

In tali casi:

- se si tratta di profilo (*social network, blog*, sito di *e-commerce*, ecc.):
  * localizzare il server o il sito web sul quale il reato è stato commesso;
  * predisporre CNR interlocutoria richiedendo alla competente Procura della Repubblica, qualora necessario, l'emissione di ordine di esibizione dati da notificare al gestore del server o del sito perché siano comunicate le informazioni relative alla registrazione del profilo (compresa la casella *e-mail* se prevista) e l'indirizzo IP dal quale l'utente si è connesso al sito (o gli indirizzi IP nel caso di più connessioni);
  * individuare l'ISP che ha rilasciato l'indirizzo IP dal quale l'autore si è connesso al sito per commettere il reato (o gli ISP in caso di più indirizzi);
  * facendo seguito alla CNR interlocutoria, richiedere alla competente Procura della Repubblica l'emissione di ordine di esibizione dati da notificare all'ISP, allo scopo di associare l'indirizzo IP al titolare del contratto di fornitura del servizio internet;

* escutere, ai sensi dell'art. 351 CPP, il titolare del contratto di fornitura del servizio internet e l'intestatario o gli intestatari delle carte ricaricate, procedendo ai sensi di legge qualora emergano indizi di reità;
* predisporre CNR conclusiva, riferendo sull'esito delle indagini svolte.

- se si tratta di casella *e-mail*, provvedere affinché l'*e-mail* non sia cancellata dal destinatario e, ove possibile, sia salvata su supporto digitale unitamente alla sua intestazione (c.d. *header*);
- richiedere all'A.G. un decreto di esibizione ed acquisizione dati relativo ai file di log alla casella di posta elettronica oggetto d'indagine da sviluppare nell'ulteriore richiesta di un decreto di acquisizione dei *caller id* abbinati agli stessi;
- se si tratta di truffa, oltre ai precedenti accertamenti, individuare anche le modalità del pagamento, se avvenuto, e tracciare le relative somme.

I sig.ri magistrati utilizzeranno le indicazioni di cui sopra nelle relative indagini. Si precisa che nel prossimo mese di marzo sarà cura dello scrivente indire una riunione, cui parteciperà anche la PG. interessata, per un confronto sulle modalità delle indagini portate avanti e la condivisione di utili elementi conoscitivi.

Sarà cura della PG., sin dal momento della recezione della denunzia, al fine di impedire la dispersione della prova, seguire le indicazioni di cui sopra e non limitarsi ad una mera trasmissione della denunzia alla AG.

Cosenza, lì 20 febbraio 2019

IL PROCURATORE DELLA REPUBBLICA
(Mario SPAGNUOLO)