DIRITTO PENALE CONTEMPORANEO

LA RICEZIONE DI SOMME DI DENARO PROVENTO DI *PHISHING*: RISULTANZE INVESTIGATIVE E PROBLEMI APPLICATIVI IN PUNTO DI QUALIFICAZIONE GIURIDICA

Nota a Trib. Milano, uff. g.i.p., sent. 10 aprile 2013, n. 2507, giud. Ferraro, imp. Ciavarella e Trib. Milano, sez. VI penale, sent. 28 maggio 2013, n. 6753, giud. Bernazzani, imp. Trozzola

di Sara Piancastelli

Abstract. *Due recenti sentenze del Tribunale di Milano (le nn. 2507/2013 e 6753/2013) affrontano il tema dell'inquadramento giuridico della condotta di colui che riceve somme di denaro provento dell'attività di* phishing. *A seconda del materiale probatorio raccolto durante le indagini, tale condotta potrebbe configurare un concorso nel reato di frode informatica e di accesso abusivo o, piuttosto, il reato di ricettazione (eventualmente accompagnata da una successiva condotta di riciclaggio). Ciò premesso, si sottolineerà come l'una o l'altra qualificazione giuridica comporti importanti differenze dal punto di vista sostanziale e processuale.*

1. Inquadramento del problema.

È ormai tristemente nota la tecnica del *phishing*[1] mediante la quale il criminale informatico cerca di procurarsi, attraverso raggiri di varia natura perpetrati su *Internet*,

[1] Sul tema: ARONICA G., *Il "*fishing*" tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, in *Riv. di giurispr. ed econ. d'azienda*, 4, 2008, pp. 83 e ss.; CAJANI F., *Profili penali del* phishing, in *Cass. pen.*, 2007, pp. 2294 e ss.; ID., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen*, 2014, pp. 1094 e ss.; CAJANI F., COSTABILE G., MAZZARACO G., Phishing *e furto d'identità digitale*, Milano, 2008; DI RONZO A., *Uso non autorizzato di carte di credito e concorso di reati nel* phishing, in *Dir. inf.*, 2009, pp. 82 e ss.; FEROLA L., *Il riciclaggio da* phishing*: tra vecchie e nuove questioni interpretative*", in *Giur. merito*, 11, 2009, pp. 2831 e ss.; FLOR R., Phishing, identity theft *e* identity abuse*. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, pp. 899 ss.; ID., *Realizzare furti di identità tramite tecniche di* phishing *integra più fattispecie penali e costituisce un reato transnazionale*, in *Riv. di giurispr. ed econ. d'azienda*, Milano, 3, 2008, pp. 136 e ss.; PERRI P., *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Int.*, 3, 2008, pp. 265 e ss.; SORGATO A., *Il reato informatico: alcuni casi pratici*, in

dati riservati – come credenziali di accesso ai sistemi di *home banking* – al fine di impossessarsi di somme di denaro di ignari correntisti.

Occorre da subito distinguere la condotta (che soltanto si può definire di *phishing*) consistente nell'acquisire fraudolentemente i dati/le informazioni personali altrui, dalla successiva ed ulteriore condotta con la quale le informazioni così ottenute vengono (dallo stesso *phisher* o da soggetti terzi) utilizzate per procurarsi un ingiusto profitto.

Precisamente, con la prima si fa riferimento all'attività fraudolenta posta in essere, il più delle volte, attraverso l'invio ad un numero indeterminato di persone di *email* che simulano nella grafica e nel contenuto quella di una Istituzione nota al destinatario, come una determinata banca o Poste italiane, al fine di indurre i destinatari a rivelare dati di carattere personale. Tale condotta è riconducibile al reato di truffa (*ex* art. 640 c.p.).

La seconda, invece, consiste nel successivo utilizzo dei dati così ottenuti per effettuare operazioni bancarie in danno del titolare del conto[2], come bonifici bancari o ricariche di carte prepagate. Saranno, in tal modo, integrati i reati di accesso abusivo ad un sistema informatico o telematico e di frode informatica (rispettivamente *ex* artt. 615-*ter* e 640-*ter* c.p.)

A questo punto, avuto "libero accesso" al conto corrente *online* della vittima e dopo averle sottratto somme di denaro, si pone all'agente il problema di entrare nella materiale disponibilità delle stesse, vale a dire di trasferirle a soggetti terzi che, a loro volta, le pongono all'incasso (per poi, successivamente, ritrasferirle secondo le indicazioni di volta in volta ricevute).

L'attività investigativa inerente a questo fenomeno illecito prende avvio, di regola, dalla ricezione di tali proventi illeciti, a seguito della denuncia-querela sporta dalla vittima.

L'esperienza delle Procure distrettuali registra – allo stato – alcuni problemi ancora irrisolti circa l'inquadramento giuridico della condotta di colui che riceve somme di denaro provento dell'attività truffaldina sopra descritta.

Infatti, a tal fine la prassi rivela la presenza di soggetti sul territorio italiano che attivano appositamente delle carte di pagamento ricaricabili e, previa comunicazione dei relativi dati identificativi ad altri soggetti (di regola questi tutti operanti all'estero), si rendono disponibili a prelevare in contanti somme di denaro fatte confluire su tali carte mediante trasferimenti *online.* Successivamente, previo trattenimento di una percentuale a titolo di ricompensa (di quanto a loro indebitamente accreditato), consegnano personalmente a terze persone la residua somma o la trasferiscono all'estero tramite il sistema di *Western Union* e/o *Money Gram*.

Giurispr. pen., 11, 2008, pp. 40 e ss.; VACIAGO G., GIORDANO M. T., *La qualificazione giuridica del* phishing *in una delle sue prime applicazioni giurisprudenziali*, in *Dir. int.*, 1, 2007, pp. 65 e ss.

[2] Cfr. PECORELLA C., *Commento all'art. 640-*ter *c.p.*, in *Cod. pen. comm.*, IPSOA, 2011, p. 6424.

Partendo da due recenti decisioni del Tribunale di Milano, scopo di questo lavoro sarà quello di analizzare le due diverse soluzioni giuridiche astrattamente ipotizzabili.

Anticipando quelle che saranno le conclusioni della nostra analisi giurisprudenziale, la prima è quella che individua, a carico di colui che riceve tali somme, un concorso nel reato di frode informatica e di accesso abusivo, ipotesi che si configura non solo nei casi di concorso morale, ma anche nel caso di contributo materiale consistente nella messa a disposizione della propria carta per consentire lo spostamento di denaro attraverso la frode informatica, senza che sia rilevante la conoscenza del complessivo disegno criminoso: basta la consapevolezza che la propria carta/conto servano per ricevere il denaro ad altri sottratto.

La seconda, invece, individua in capo a colui che riceve ed occulta il denaro la fattispecie della ricettazione (eventualmente accompagnata da una successiva condotta di riciclaggio[3]) ove, nella fattispecie concreta, difettino invece tutti gli elementi sopra descritti, vale a dire il concorso nel reato di truffa, accesso abusivo ad un sistema informatico e frode informatica.

2. Il concorso nei reati di frode informatica e accesso abusivo al sistema informatico o telematico.

Con la prima sentenza che qui si commenta il Tribunale di Milano[4] ha preso in esame la condotta dell'imputato che, in concorso con altri soggetti rimasti ignoti, facendo abusivamente accesso al sistema informatico protetto da misure di sicurezza di Poste Italiane S.p.a. e intervenendo "informaticamente" sul conto corrente postale di un ignaro correntista, (vale a dire senza diritto su dati, informazioni e programmi ivi contenuti) disponeva una ricarica *online* a suo favore (priva di giustificazione ed all'insaputa dell'intestatario), così procurando a sé o ad altri un ingiusto profitto con equivalente danno per il titolare del conto[5].

---

[3] Cfr. sul punto Tribunale di Milano, Giudice per le indagini preliminari, 29 ottobre 2008, n. 8542, in *Foro Ambr.*, 4, 2008, pp. 406 e ss.

[4] Cfr. Tribunale di Milano, Giudice per le indagini preliminari – sent. 2507/2013 (est. Ferraro), inedita.

[5] Si riporta, per completezza, l'imputazione: "*1) reato di cui agli arti. 110, 615*-ter *primo e terzo comma e 61 n. 2 c.p. perché, in concorso con ignoti e previo accordo, al fine di realizzare il reato di cui al capo 2, si introduceva abusivamente nel sistema informatico o telematico della società Poste Italiane S.P.A., protetto da misure di sicurezza e da considerarsi di interesse pubblico perché preposto alla gestione e tutela del credito in ambito nazionale ed internazionale. Con l'aggravante di aver commesso il reato al fine di commetterne un altro. Con l'aggravante di aver commesso il fatto con riguardo a sistemi informatici di interesse pubblico.*

2) Del reato previsto e punito dagli arti. 110 e 640-ter *c.p. perché, in concorso con ignoti e previo accordo, intervenendo senza diritto su dati, informazioni o programmi contenuti nel sistema informatico o telematico della società Poste Italiane S.P.A., mediante predisposizione di ricarica online a favore della Postepay n. 4023600581288166 a sé stesso intestata, procurava a sé o ad altri un ingiusto profitto con pari danno patito da D. L. A. di 489,23 euro. Con la recidiva reiterata ed infraquinquennale* ex *art. 99 c.p.".*

Come già anticipato, l'affermazione di una responsabilità a titolo di concorso nei reati di frode informatica ed accesso abusivo[6] (tesi accolta dalla sentenza in esame), piuttosto che per il reato di ricettazione, corre sul sottile crinale che si colloca tra la previa piena consapevolezza, in capo all'imputato, dell'intero *modus operandi* e la semplice generica consapevolezza della illiceità dell'operazione precedente (circostanza quest'ultima che escluderebbe, ove non accompagnata da altri elementi, una responsabilità dell'imputato per i reati presupposti)[7] e, per essa, delle somme ricevute.

In altre parole, per concludere nel senso del concorso nei reati di frode informatica ed accesso abusivo occorrono elementi di prova idonei a dimostrare che l'imputato o abbia contribuito personalmente e direttamente – in concorso con altri – all'attività fraudolenta di carattere informatico (diretta, in seguito all'accesso abusivo, ad intervenire senza diritto su dati, informazioni o programmi contenuti nel sistema di *home banking*, per effettuare la successiva disposizione di ricarica), oppure che lo stesso abbia tenuto in tal senso una condotta di contributo morale ossia di istigazione o di rafforzamento dell'altrui proposito delittuoso.

Dunque, l'aspetto più problematico riguarda proprio l'accertamento probatorio, in capo a colui il quale mette a disposizione la propria carta di pagamento ricaricabile per ricevere i proventi illeciti del *phishing* e dei successivi reati accesso abusivo e frode informatica, dell'esistenza di un consapevole e volontario contributo materiale o morale fornito per la realizzazione dei reati.

Accertamento non certamente agevole se non in indagini complesse (come quelle relative ad organizzazioni criminali dedite a tali tipi di reato) ove spesso gli investigatori possono far ricorso anche ad intercettazioni telefoniche e/o telematiche, oltre che ad attività di osservazione e controllo degli indagati (con eventuali ulteriori elementi di prova, anche di natura dichiarativa a seguito di interrogatorio). Anche perché nella maggior parte dei casi al fascicolo processuale gli unici elementi che riescono ad essere acquisiti sono la querela della vittima e i conseguenti accertamenti investigativi volti ad identificare il beneficiario[8].

Alla luce di queste considerazioni, nel caso in cui sussistano elementi di prova che colui il quale pone all'incasso somme di denaro sia ben consapevole dell'attività truffaldina ed assicuri la propria collaborazione, ben sapendo che è proprio grazie al trasferimento *online* sulla sua carta ricaricabile che viene reso difficile o addirittura

---

[6] Si veda sul punto anche Cass., Sez. V, 19 dicembre 2003, n. 2682, in *Foro italiano*, II, 2005, pp. 660 e ss. che ha dichiarato che "*va ammesso il concorso del reato di frode informatica con quello di accesso abusivo ad un sistema informatico o telematico essendo diversi i beni giuridici tutelati e le condotte sanzionate, in quanto quest'ultimo tutela il domicilio informatico sotto il profilo dello* ius excludendi alios*, anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, mentre la frode informatica tutela il patrimonio e contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto*".

[7] Si veda sul punto Tribunale di Milano, 15 ottobre 2008, n. 1935, in *Corr. del Merito*, 3, 2009, pp. 285 e ss. con nota di AGNINO F., *Computer crime e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*.

[8] Si vedano sul punto le Direttive per la Polizia Giudiziaria del Distretto di Milano *"Sui primi accertamenti investigativi in materia di reati informatici"* (in vigore dal 1 luglio 2011).

impossibile l'accertamento della provenienza delittuosa del denaro illecitamente sottratto e, dunque, la individuazione dell'autore del reato, non vi è dubbio che l'imputato debba rispondere a titolo di concorso nell'attività delittuosa (vale a dire a titolo di concorso nei reati di accesso abusivo a un sistema informatico o telematico e frode informatica *ex* artt. 615-*ter* e 640-*ter* c.p.).

E dunque, come nel caso che si commenta, l'imputazione elevata dalla Pubblica Accusa lascia doverosa traccia che trattasi di ipotesi contestate all'imputato "*in concorso con ignoti e previo accordo*".

Occorre infine sottolineare, quale ulteriore aspetto interessante, l'applicazione dell'aggravante del sistema di "pubblica utilità/pubblico interesse", così come prevista dal terzo comma dell'art. 615-*ter* c.p. E infatti il Giudice, accogliendo la pena concordata tra le parti e ritenendola congrua, ha considerato il sistema informatico di Poste Italiane S.p.a., oggi equiparato ai sistemi informatici degli istituti di credito, sistema di interesse pubblico in quanto riferito ad attività direttamente rivolta al soddisfacimento di bisogni generali della collettività, il cui regolare funzionamento appare sempre più essenziale per la vita quotidiana di ogni soggetto (essendo stata lesa, nel caso di specie, l'integrità e la funzionalità di questo sistema, il quale appare meritevole di una tutela ben più incisiva e ad ampio spettro).

3. Il reato di ricettazione.

La seconda decisione[9] oggetto della nostra analisi riguarda il caso in cui un soggetto riceva da terzi solamente la mera richiesta di farsi accreditare, dietro compenso, delle somme sulla propria carta ricaricabile e di trasferirle successivamente in altro modo agli autori dei reati presupposti e, quindi, rimanga del tutto ignaro del disegno criminoso complessivo (ed, in particolare, della attività informatica sottesa al ricordato *modus operandi*)[10]. Difficile quindi, in questi casi, sostenere per colui che si limita a ricevere i proventi del *phishing* la tesi del concorso nei reati presupposti commessi da altri soggetti, ma può, invece, ritenersi sussistente, sulla base della valutazione degli elementi concreti a lui noti e sicuramente della conoscenza della provenienza illecita delle somme di denaro ricevute, una responsabilità per il reato di ricettazione *ex* art. 648 c.p.

Al riguardo, la prassi applicativa evidenzia un dato allarmante che non può essere taciuto: a fronte di attacchi massicci e periodici di *phishing* a far data dal 2005, le indagini spesso iniziano (con la ricezione della querela della vittima) e si concludono

[9] Cfr. Tribunale di Milano, Sez. VI penale in composizione monocratica – sent. 6753/2013 (est. Bernazzani), inedita.

[10] Si riporta, per completezza, l'imputazione: "*del delitto p. e p. dall'art. 648 c.p., perché nella piena consapevolezza della provenienza illecita, riceveva una somma di denaro pari ad Euro 499,63 sulla propria carta postepay n. 4023600580524892 tramite operazione online (operazione bancaria effettuata ai danni di P. P., titolare della carta postepay n. 4023600452834080 e vittima di* phishing *somma quindi provento dei reati di cui agli artt. 81, 494, 640 e 615-*ter *c.p.)*".

solo con l'individuazione di coloro che ricevono tali somme[11], e cioè l'ultimo anello di una catena ben più lunga e articolata, rispetto alla quale l'identificazione dei *phisher* (soggetti – come già precedentemente accennato – il più delle volte operanti all'estero) e soprattutto la loro condanna appare difficoltosa[12], rimanendo sullo sfondo di processi celebrati nei confronti di soggetti secondari rispetto al fenomeno illecito, ma paradossalmente accusati del più grave reato di ricettazione.

Un esempio di tale impostazione è proprio il caso processuale che qui si commenta: all'esito del dibattimento il Tribunale di Milano ha ritenuto – sulla base delle risultanze processuali in atti – che potesse ritenersi dimostrata la prospettazione accusatoria per il reato di ricettazione rivolta nei confronti dell'imputato, in quanto gli elementi probatori acquisiti dimostravano – oltre ogni ragionevole dubbio – la sussistenza degli estremi, oggettivi e soggettivi, della fattispecie incriminatrice di cui all'art. 648 c.p.

Le prove logiche sono state desunte mediante l'accertamento e l'individuazione sia della carta Postepay ricaricata illecitamente, sia del relativo titolare identificato – senza ombra di dubbio – nell'imputato. Si accertava, altresì, che tale carta Postepay "*risultava essere stata attivata in data 12-2-10 con consegna effettuata in data 28-4-10, ossia il giorno stesso dell'illecito accredito*" a favore dell'imputato.

Il Tribunale, sulla base di tale evidenze processuali, pertanto afferma come sul piano obiettivo sia "*indubbio che la somma di denaro accreditata sulla carta Postepay intestata all'imputato aveva illecita provenienza, costituendo corpo dei reati di cui agli artt. 81, 494, 640, 640-*ter *c.p., nell'ambito di una "canonica" operazione di* phishing, *così come è palese che l'intervenuto accreditamento della provvista configura gli estremi della condotta di ricettazione contemplata dall'art. 648 c.p.*".

A differenza della prima ipotesi analizzata, il Giudicante, in riferimento alla "*riconducibilità della vicenda alla condotta cosciente e volontaria*" dell'imputato, dà poi atto che in questo caso non sussistono elementi probatori idonei ad avvalorare un concorso nel reato presupposto, né che egli fosse a conoscenza del *modus operandi* del *phisher*.

Così il passo centrale di tale motivazione: "*va premesso che dalle risultanze acquisite non emergono elementi utili ad avvalorare la conclusione che lo stesso imputato sia stato l'autore del reato presupposto, tenuto conto del rilievo che non risulta da alcuna fonte di prova che lo stesso abbia posto in essere personalmente e direttamente – da solo ovvero in concorso con altri – l'attività fraudolenta diretta ad ottenere i dati della carta Postepay della p.o. per effettuare la successiva disposizione di bonifico mediante prelevamento di parte della provvista esistente sul conto della p.o., né che lo stesso T. abbia tenuto una condotta*

---

[11] Tanto è vero che, anche aderendo alla impostazione del concorso nei reati presupposti, essi vengono contestati – come abbiamo fatto cenno – "*in concorso con persona non identificata*".

[12] Nel 2007 si è avuta, per la prima volta in Italia, la condanna di membri di una associazione transnazionale dedita alla commissione di reati di *phishing*: cfr. Tribunale di Milano, Uff. Indagini preliminari, 10 dicembre 2007, n. 888, (commentata in FLOR R., *Frodi identitarie e diritto penale*, in *Riv. di giurispr. ed econ. d'azienda*, 4, 2008, pp. 184 e ss.; SORGATO A., *Il reato informatico: alcuni casi pratici*, cit.). Tale sentenza è stata confermata in Cassazione nel 2011.

qualificabile sub specie *di istigazione ovvero di rafforzamento dell'altrui proposito delittuoso nell'ipotesi di concorso eventuale di persone".*

Quanto all'elemento soggettivo, la sentenza che si commenta si riporta in maniera condivisibile alla giurisprudenza maggioritaria, affermando come in tema di ricettazione "*la prova del dolo può essere desunta da qualsiasi elemento, anche indiretto, e la stessa mancata o non attendibile giustificazione del possesso di una cosa proveniente da delitto costituisce prova della conoscenza dell'illecita provenienza del bene*"[13]. L'affermazione della responsabilità per il delitto di ricettazione non richiede pertanto l'accertamento giudiziale del delitto che ne costituisce il presupposto (ossia il *phishing*), né dei suoi autori, né dell'esatta tipologia del reato, potendo il giudice affermarne l'esistenza attraverso prove logiche[14].

Sempre secondo il consolidato orientamento giurisprudenziale, occorre poi infine ricordare come il dolo di ricettazione (da accertarsi caso per caso) non può essere integrato né dal dubbio né dal mero sospetto, ma può dirsi sussistente solo quando, sulla base di precisi elementi di fatto, si possa affermare che colui che ha ricevuto il denaro si sia seriamente rappresentato l'eventualità della provenienza delittuosa dello stesso e, nondimeno, si sia comunque determinato a riceverlo (ed, eventualmente, a ritrasferirlo successivamente) con le modalità indicate dall'autore del reato presupposto[15].

In sostanza, perché possa ravvisarsi il dolo eventuale si richiede "*più di un semplice motivo di sospetto, rispetto al quale l'agente potrebbe avere un atteggiamento psicologico di disattenzione, di noncuranza o di mero disinteresse; è necessaria una situazione fattuale di significato inequivoco, che impone all'agente una scelta consapevole tra l'agire, accettando l'eventualità di commettere una ricettazione, e il non agire*"[16].

4. Le due ipotesi a confronto.

Dalla lettura delle due sentenze è possibile ipotizzare che la scelta di optare per l'una o l'altra ipotesi accusatoria derivi, di fatto, dal materiale probatorio raccolto durante le indagini.

Ciò premesso, occorre infine sottolineare come la scelta dell'una o dell'altra qualificazione giuridica comporti differenze non di poco momento anche da altri punti di vista, sostanziali e processuali.

Sotto il profilo penale-sostanziale, i reati di frode informatica e accesso abusivo ad un sistema informatico o telematico sono puniti con la pena, rispettivamente, della reclusione da sei mesi a tre anni e con la multa da euro 51,00 a euro 1.032,00 e con la reclusione fino a tre anni; il reato di ricettazione la reclusione da due ad otto anni e con

[13] Cfr. Cass., Sez. II, 27 febbraio 1997, n. 2436, in *C.E.D. Cass.,* n. 207313.
[14] Cfr. Cass., Sez. II, 5 luglio 2011, n. 29685, in *C.E.D. Cass*., n. 251028.
[15] Cfr. Cass., Sez. II, 17 giugno 2011, n. 25960 *in questa Rivista,* 9 settembre 2011.
[16] *Ibidem.*

la multa da euro 516,00 a euro 10.329,00[17]. Tutto ciò incide, di conseguenza e salve le ipotesi di interruzione o sospensione previste dal c.p., anche sui termini di prescrizione *ex* art. 157 c.p.: sei anni per i primi, otto anni per il reato di ricettazione.

Sotto il profilo penal-processuale, i reati di frode informatica e accesso abusivo ad un sistema informatico o telematico sono procedibili a querela della persona offesa, salva la configurabilità delle aggravanti di cui al comma 2 e 3 degli art. 615-*ter* e 640-*ter* c.p., mentre il reato di ricettazione è sempre procedibile d'ufficio.

Quanto alla competenza territoriale, occorre premettere che solo per i primi due reati vale la competenza distrettuale cosi come previsto dall'art. 11 della legge n. 48 del 2008.

Bisogna *in primis* considerare che il reato di accesso abusivo si consuma nel luogo in cui viene effettivamente superata la protezione informatica e vi è l'introduzione nel sistema e, quindi, là dove è materialmente situato il sistema informatico (*server*) violato, l'elaboratore che controlla le credenziali di autenticazione del cliente.

Precisamente, è nel luogo in cui si trova il sistema violato che si perfeziona la condotta del reo, sia che essa consista nel superare le barriere logiche che, in un sistema che deve essere protetto da misure di sicurezza, impediscono l'accesso ai dati contenuti nella sua memoria interna, sia che invece si esaurisca nell'intrattenersi all'interno del sistema senza esserne autorizzato, dopo esservi entrato in modo legittimo perché in possesso delle credenziali necessarie[18].

La frode informatica si consuma invece nel luogo in cui si verifica l'arricchimento dell'agente, ovvero nel luogo in cui si procura l'ingiusto profitto, essendo in questo caso irrilevante il luogo in cui è stata posta in essere la condotta[19].

Pertanto, se si conclude per la tesi del concorso nei reati presupposti, occorrerà individuare la competenza territoriale – alla luce dei richiamati criteri – individuando il reato più grave tra i due sopra indicati, alla luce della disposizione di cui all'art. 16 c.p.p.

Se si conclude, invece, per la tesi della qualificazione giuridica di ricettazione, tale reato si consuma nel luogo e nel tempo in cui il denaro o la *res* di provenienza delittuosa è acquistata o ricevuta dall'autore del reato[20]: essa deve pertanto individuarsi nel luogo ove il ricettatore riceve le somme provento di *phishing*. Trattandosi di carte ricaricabili prive di un conto corrente collegato, il luogo di consumazione sarà quindi quello del luogo dell'ufficio postale o dello sportello ATM

---

[17] La *ratio* della maggiore severità del trattamento sanzionatorio del reato di ricettazione dipende dalla necessità di evitare il pericolo di un consolidamento o di un aggravamento del danno patrimoniale generalmente subito dalla vittima del delitto-presupposto, e anche di impedire ulteriori incrementi patrimoniali da parte di altri soggetti, diversi dagli autori del reato, non ostacolando l'attività giudiziaria nell'accertamento e nella punizione dei colpevoli e prevenire la commissione dei di reati: cfr. MANTOVANI F., *Diritto penale. Parte speciale*, II, *Delitti contro il patrimonio*, Padova, 2009, pp. 240 e ss.

[18] Cfr. Cass., Sez. I, 27 settembre 2013, n. 40303, in *Penale.it*.

[19] Cfr. Cass, Sez. VI, 14 dicembre 1999, n. 3065, in *Cass. pen*, 1, 2001, pp. 481 e ss.

[20] Cfr. Cass., Sez. I, 24 febbraio 2004, n. 24934, in *C.E.D. Cass*. n. 228778.

presso cui l'imputato preleva le somme, vale a dire dove acquisisce la disponibilità materiale del denaro.

Infine, per quanto attiene alle modalità concrete di esercizio dell'azione penale, nel caso di concorso nei reati presupposti di accesso abusivo e frode informatica si potrebbero configurare in concreto due ipotesi.

La prima attiene proprio al caso di cui alla sentenza n. 2507/13 del Tribunale di Milano, vale a dire la fattispecie di accesso abusivo aggravato dalla circostanza (ad effetto speciale) del sistema di "pubblica utilità/pubblico interesse" *ex* art. 615 –*ter* comma 3 c.p., in concorso con il reato di frode informatica: essendo il primo il reato più grave, perché punito con la reclusione da uno a cinque anni, si procederà con la richiesta di emissione del decreto che dispone il giudizio (con celebrazione quindi dell'udienza preliminare). Analoga soluzione, anche se di difficile verificazione nell'esperienza pratica del passato[21], in caso di ipotesi di frode informatica aggravata (in concorso con il reato di accesso abusivo).

Nella diversa ipotesi di fattispecie non aggravate di accesso abusivo e frode informatica, si procederà invece con decreto di citazione diretta a giudizio, essendo entrambi reati non punibili con la pena superiore nel massimo a quattro anni.

Nel caso di ricettazione, per l'esplicita previsione contenuta nell'art. 550 comma 2 lett. g) c.p.p. si procede sempre con decreto di citazione diretta a giudizio (senza celebrazione dell'udienza preliminare).

[21] Discorso diverso dovrà essere invece fatto alla luce della nuova formulazione dell'art. 640-*ter* comma 3 c.p.: cfr. CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, cit.