Poliziamoderna

Cybercrime

1. Introduzione Come anticipato nell'articolo pubblicato nel numero precedente, questa seconda parte si occuperà dei più frequenti reati "comuni", commessi mediante il mezzo informatico: reati informatici e telematici "impropri". Si tratta di un gruppo assai eterogeneo composto da reati molto frequenti nella casistica. Compito dell'interprete, in questo caso, è soprattutto quello di verificare con attenzione la "compatibilità giuridica" di norme non "dedicate", in molti casi scritte ben prima dell'avvento del computer.

2. I delitti contro l'onore Ingiuria e diffamazione sono tra i reati più ricorrenti nel mondo telematico, probabilmente a causa delle enormi potenzialità del mezzo che, malauguratamente, favoriscono anche gli abusi. Com'è noto, in termini generali il discrimine tra le due fattispecie delittuose coincide con la presenza o meno dell'offeso. Ma come si può adattare il concetto di "presenza" a un mondo così particolare come quello di Internet ove le comunicazioni avvengono sempre e naturalmente a distanza? La soluzione si fonda sulla lettura del secondo comma dell'art. 594 cp il quale contempla l'uso di mezzi di comunicazione tra assenti equiparandoli ai fatti commessi tra presenti. Ma tra i mezzi ivi tassativamente elencati e definiti, non è certo possibile richiamare le comunicazioni telegrafiche o telefoniche. Pur riconoscendo che, sovente, con Internet possono condividere il vettore, ad esempio il cavo telefonico, ne è evidente la diversità, non soltanto tecnica, dalla Rete. È chiaro, a questo punto, che l'ingiuria può perfezionarsi con l'invio di scritti o disegni informatici, ad esempio un' email, o un'immagine digitale a condizione che, conformemente alla lettera della norma, siano "dirette" alla persona offesa. Passando alla diffamazione (art. 595 cp) essa consiste nell'offesa dell'altrui reputazione, come appena visto, mediante comunicazioni non dirette alla persona offesa. Si pensi a un messaggio destinato a più persone manualmente, vale a dire con l'inserimento di più destinatari da parte del mittente, oppure automaticamente, con l'invio a una mailing list (sempre che l'agente non intenda, con questo mezzo, offendere direttamente un soggetto iscritto a quella lista) ovvero a un newsgroup. La diffamazione, contrariamente all'ingiuria, non contempla mezzi tassativamente individuati, bensì un semplice "rapporto comunicativo" con terzi (due o più, anche non contemporaneamente) diversi dalla persona offesa. Discorso differente vale per il caso di offese perpetrate attraverso pagine web. In tale ipotesi, conformemente alla lettera dell'art. 595, sussiste sicuramente la comunicazione con più persone, anzi, verso un pubblico indeterminato. Il Web, con newsgroup, mailing list "aperte" e, comunque, servizi informativi accessibili da categorie indeterminate di utenti, rientra peraltro nei "mezzi di pubblicità" di cui all'aggravante del terzo comma dell'art. 595 cp Ma i punti di contatto con la stampa, soprattutto i comuni caratteri di pubblicità, hanno indotto taluni a ritenere il mondo Internet disciplinato dalle regole proprie dei media tradizionali, non soltanto quelli su carta ma anche quelli dell'etere. L'interprete, senza eccessivo lassismo o ingiustificato rigore, dovrà farsi guidare soltanto dai principi del diritto penale, tra i quali è sicuramente di primaria importanza quello che vieta il ricorso a ogni strumento analogico in malam partem. In gioco non vi sono soltanto le aggravanti relative alla stampa, ma soprattutto le responsabilità penali di soggetti diversi dall'autore del reato come quelle di cui agli artt. 57 e 57-bis cp. Sicché, ad esempio, se si applicassero le regole della stampa, un blogger dovrebbe essere inteso come direttore responsabile, passibile di sanzione penale per i commenti inseriti da terzi. In termini generali, sull'equazione Internet uguale stampa, buona parte della dottrina si è espressa negativamente soprattutto in relazione agli aspetti penali. Ciò, principalmente, in base alla definizione di stampa offerta dall'art. 1 della legge 47/48 chiaramente incompatibile con la telematica: "Sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici in qualsiasi modo destinate alla pubblicazione". Parimenti, si è esclusa l'applicabilità della disciplina del settore radiotelevisivo (in particolare, la c.d. "legge Mammì", l. 6 agosto 1990, n. 223). A parte lo specifico aspetto della registrabilità, oramai pacificamente ammessa, delle testate giornalistiche esclusivamente telematiche come nello storico caso "Interlex" (Tribunale di Roma, ordinanza 6 novembre 1997, in Interlex, http://interlex.it/testi/or061197.htm), in sede penale la giurisprudenza si è anch'essa prevalentemente espressa escludendo detta equiparabilità, la quale sussiste soltanto per le testate registrate (per tutte, Giudice dell'udienza preliminare presso il Tribunale di Oristano, 25 maggio 2000, in Penale.it, http://www.penale.it/giuris/meri_51.htm). Ciò, almeno, sino all'entrata in vigore della legge 7 marzo 2001, n. 62 che all'art. 1 così stabiliva e stabilisce tutt'ora: "Per «prodotto editoriale», ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografici o cinematografici". In tale definizione, una parte, pur minoritaria, della giurisprudenza ha scorto la possibilità di far rientrare le pubblicazioni telematiche nel concetto di

prodotto editoriale, con applicazione della disciplina propria della stampa (ad esempio, Giudice per le indagini preliminari presso il Tribunale di Latina, ordinanza 7 giugno 2001, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=605; più di recente, Tribunale di Firenze, Sezione I Penale in composizione monocratica, sentenza 13 febbraio 2009 - dep. 14 maggio 2009, n. 982/09, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=832). Ma, fortunatamente, a parte qualche episodio singolare (casi giurisprudenziali che sono divenuti casi di cronaca come Tribunale di Aosta, in composizione monocratica, sentenza 26 maggio 2006 - dep. 10 giugno 2006, n. 553/04, in Penale.it, http://www.penale.it/public/docs/Trib_Aosta_Sent_26_05_2006_10_6_2006.pdf e Tribunale di Modica, sentenza 8 maggio 2008 - dep. 6 agosto 2008, n. 194/08, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=692), la Corte di Cassazione ha chiarito, finalmente, che Internet non equivale necessariamente a stampa (Corte di Cassazione, sezione III penale, sentenza 11 dicembre 2008 - dep. 10 marzo 2009 n. 10535, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=762). Diversa, come anticipato, è l'ipotesi della diffamazione commessa per mezzo di testate giornalistiche telematiche registrate. È, infatti, fenomeno ormai piuttosto diffuso, pur dopo le cennate incertezze, la presenza, sul Web, di pubblicazioni regolarmente registrate ai sensi della l. 47/48 sulla stampa. Il panorama offre sia estensioni Internet di preesistenti presenze su carta, che testate esclusivamente telematiche (tra i siti giuridici si pensi ad Interlex, la prima in Italia registrata presso il Tribunale di Roma con l'ordinanza menzionata sopra). Considerato che le prime "replicano" sovente il materiale pubblicato su carta, a queste pare potersi applicare la disciplina sulla stampa. Il discorso è assai differente nel secondo caso. A fronte di queste evidenti realtà, pur volontariamente "regolarizzatesi", esistenti soltanto su Internet, ci si è interrogati soprattutto in ordine alle eventuali responsabilità penali dei rispetti direttori, editori e stampatori. La soluzione non è certo agevole, ma un tentativo può essere fatto ricordando sempre che il diritto penale vieta interventi analogici come quelli posti in essere dai giudici amministrativi che hanno dato via libera all'iscrizione di pubblicazioni telematiche pur in assenza di norme specifiche. Come osservato dal gup di Oristano nella sentenza citata, quando si è voluto estendere l'operatività della disciplina della stampa lo si è fatto espressamente. Si pensi all'informazione via etere regolata dalla "legge Mammì". In realtà, le decisioni favorevoli alla registrabilità delle pubblicazioni telematiche hanno generato confusione in materia, creando il terzo genere delle "pubblicazioni registrate volontariamente" cui dovrebbe conseguire, a rigor di logica, l'applicazione di tutta la disciplina sulla stampa, sia quella favorevole (che comporta vantaggi fiscali ed economici in genere) che quella potenzialmente sfavorevole (la responsabilità penale di soggetti diversi dall'autore e le aggravanti speciali). Ma, per i motivi anzidetti, il passo tra il diritto civile e quello amministrativo da un lato e quello penale dall'altro è molto lungo, riflettendosi anche sulla posizione dei soggetti che operano all'interno della testata telematica. Sicché la richiesta, pur liberamente proposta e, poi, accolta da un giudice, non può valere, di per sé, a fondare l'applicabilità dei riflessi (penali) di una legge che non c'è e che, invece, è stata "creata" , in sede amministrativa, mediante un procedimento analogico. È senz'altro vero che in tal modo si crea una sorta di doppio binario, per certi versi fonte di probabili imbarazzi per gli interpreti. Ma, ancora una volta, non si può fare a meno che prenderne atto, pur auspicando una regolamentazione che, adattandosi ai tempi, allontani, una volta per tutte, i pericoli di un trattamento penale non omogeneo del fenomeno.

3. Molestie telematiche e stalking Un altro reato che, secondo alcuni, può consumarsi via Internet, di solito con lo strumento della posta elettronica, è quello previsto dall'art. 660 cp. La norma, per la precisione, punisce "chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo". È chiaro, però, che contrariamente a un primo orientamento la telematica non può essere considerata luogo pubblico o aperto al pubblico, tanto meno "telefono", che va inteso come tecnologia, non come eventuale vettore. E ciò è confermato in una recentissima pronuncia della Suprema Corte (Corte di Cassazione, sezione I penale, sentenza 17 giugno 2010 - dep. 30 giugno 2010), n. 24510, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=865). Decisamente più calzante è il nuovo reato di atti persecutori di cui all'art. 612-bis cp (introdotto con il decreto legge 23 febbraio 2009, n. 11, successivamente convertito senza modifiche sul punto) secondo il quale "salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita". Si tratta del c.d. "stalking", che si concretizza in vere e proprie condotte persecutorie, sempre più sovente col mezzo telematico ed è chiaro che la formulazione delle norma incriminatrice (a differenza di quella dell'art. 660 cp) è in grado di colpire efficacemente quanto commesso via Internet (c.d. "cyberstalking"). **4. La pedopornografia nella Rete** Con l'introduzione dell'art. 600-ter cp, la legge 3 agosto 1998, n. 269 – norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù – ha, in un provvedimento di più ampia portata volto a combattere l'intero fenomeno della pedofilia, fatto fronte alla diffusione, anche telematica, di materiale pornografico riguardante i minori di anni diciotto, la c.d. "pedopornografia". La disposizione, leggermente modificata dalla legge 6 febbraio 2006, n. 38 consta di quattro commi dei quali il terzo evidenzia espressamente la rilevanza, tra gli altri mezzi, della telematica, sanzionando chiunque "distribuisce, divulga o pubblicizza" materiale pornografico

riguardante minori ovvero “distribuisce o divulga notizie o informazioni finalizzate all’adescamento o allo sfruttamento sessuale di minori”. La condotta più lieve è, invece, quella di cui al quarto comma che sanziona la semplice cessione (non importa se gratuita o verso corrispettivo) di materiale pedopornografico. Considerata la minore potenzialità lesiva, il legislatore ha previsto pene decisamente inferiori rispetto alle altre fattispecie di cui alla medesima norma. Ma i confini tra le fattispecie del terzo e quarto comma, specie se il fatto riguarda il mondo della telematica, non sono sempre apparsi del tutto chiari, così come emerge da una risalente pronuncia della Suprema Corte che ha investito l’aspetto tecnico delle chat via Irc. Nella fattispecie in esame viene contestato all’indagato di avere scambiato fotografie pedopornografiche, attraverso le reti Internet e mediante il programma Mirc di chat, nel canale con utilizzazione del nick. Il collegamento a tale canale è comunque accessibile a una indefinita pluralità di utenti e, successivamente, la comunicazione avviene esclusivamente con i soggetti presenti nell’area. Si configura, pertanto, divulgazione del materiale vietato, messo comunque a disposizione di un novero indefinito di destinatari” (Corte di Cassazione, sentenza 27 aprile 2000, n. 1762, in Penale.it, http://www.penale.it/giuris/cass_008.htm). Il caso affrontato dai giudici di legittimità riguardava proprio la distinzione tra le condotte di distribuzione, divulgazione e pubblicizzazione da un lato e la semplice cessione dall’altro. Il primo gruppo, come risulta ormai acquisito, si riferisce, pacificamente, a ipotesi di attività rivolte a un pubblico indefinito; il secondo riguarda, invece, cessioni occasionali a persone determinate. La Cassazione ha avallato tale impostazione, ma ha riconosciuto in Irc un veicolo nel quale lo scambio di materiali, più precisamente di immagini digitali, avverrebbe nei confronti di un pubblico indeterminato. Non v’è chi non veda quanto tale conclusione, che sostanzialmente confonde tutto il mondo della telematica, sia del tutto erronea nel ritenere che i file di un utente Irc siano a disposizione, indistintamente, di tutti gli utenti chat, come se si trattasse di un sito Internet di libero accesso. E infatti, la chat, cui può partecipare un’indefinita pluralità di utenti, è soltanto un luogo di discussione tra più persone ove, però, l’eventuale scambio di file avviene in modo mirato, non indistinto, sempre e comunque verso soggetti determinati scelti dal mittente. Ma anche se dovesse essere acclarata la diffusione di materiale illecito (usualmente, sono molto utilizzati i sistemi peer-to-peer o p2p), occorrerebbe pur sempre provare la consapevolezza di detta condotta, comunque del contenuto del file “monitorato”. Sotto il primo aspetto, infatti, non può darsi per scontato che l’incolpato disponga di cognizioni tecniche tali da consentirgli che, ad esempio, un determinato software mette in condivisione automaticamente quanto scaricato. Quanto alla seconda problematica, non va dimenticato il fenomeno, peraltro molto diffuso, dei fake, vale a dire file che pur avendo un contenuto illecito sono nominati in modo tale da nascondere detta illiceità (per un caso concreto, Tribunale ordinario di Brescia, sezione II penale, sentenza 22 aprile - dep. 24 maggio 2004, n. 1619 est. Mainardi, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=37). Una diversa norma applicabile alla telematica è quella di cui all’art. 600-quater cp che punisce, ovviamente al di fuori delle ipotesi dell’art. 600-ter, la mera detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori che ben può provenire dalla Rete. La norma, proprio perché punisce condotte da alcuni ritenute “di confine”, necessita di un’interpretazione molto rigorosa, specie sotto il profilo dell’elemento psicologico. È infatti possibile imbattersi involontariamente in siti illegali, semplice fatto che comporta la memorizzazione di file temporanei (nell’area c.d. di cache). Sarebbe, in questo caso, consentito sostenere la punibilità per la detenzione di tali prodotti oggettivamente illeciti? La risposta è, in linea di massima negativa soprattutto riguardo a utenti inesperti che, non conoscendo a fondo il funzionamento dei programmi utilizzati per la navigazione, non sarebbero in grado di cancellare i file indesiderati e, ancor prima, di rendersi conto di ciò che, almeno obiettivamente, è senza dubbio detenzione. Non resterà, allora, che procedere con estrema circospezione evitando conclusioni inique ed affrettate in assenza di elementi di riscontro a quella che potrebbe essere una detenzione inconsapevole, dunque non punibile (in proposito, Tribunale civile e penale di Perugia, ufficio del Giudice per le indagini preliminari, sentenza 8 luglio - dep. 30 dicembre 2003, n. 313, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=40). Per quanto riguarda gli aspetti investigativi, va osservata, all’art. 14 della legge, la previsione di particolari attività che possono essere compiute da agenti sotto copertura, gli undercover, caso assolutamente raro nel nostro ordinamento, quindi significativo del poderoso armamento, anche tecnologico, che il legislatore ha inteso mettere in campo per combattere il fenomeno. Si noti peraltro che la possibilità di realizzazione di “siti esca”, contemplata dal secondo comma, va ben al di là della “copertura”, legittimando anzi la figura dell’agente provocatore in altri ambiti non ricompreso nelle attività concesse alle forze di polizia. Nel 2006, inoltre, è stato costituito il Centro nazionale per il contrasto della pedopornografia sulla rete Internet (art. 14-bis l. 269/98). Sono stati imposti alcuni obblighi ai fornitori dei servizi della società dell’informazione, resi attraverso reti di comunicazione elettronica (art. 14-ter) e sono stati “codificati”, all’art. 14-quater, gli strumenti tecnici per impedire l’accesso ai siti illegali (mediante “inibizione”, evidentemente ove non possibile un vero e proprio sequestro).

5. Il diritto d’autore e il mondo digitale Nel mondo dell’informatica tutto è perfettamente riproducibile con la creazione di un nuovo originale, non semplicemente di una copia. Ma è proprio questa la “nuova debolezza” del prodotto digitale che rischia di condannare a morte il diritto d’autore e, comunque, lo indebolisce sensibilmente. Figlia quasi certa della consapevolezza di questa agonia tendenzialmente irreversibile, è la più organica riforma della legge sul diritto d’autore (l. 633/41, di seguito lda) entrata in vigore nel 2000 (l. 248/2000) la quale, lungi dal sapersi adattare alle nuove

travolgenti realtà, è riuscita soltanto a inasprire non poco le pene e a limitare i diritti dei singoli. Incidentalmente, va detto che, pur nella consapevolezza di quanto affermato nella relazione al ddl 2773, la quale colloca le violazioni in tema software (ma il discorso vale per tutte le opere digitali) tra i reati commessi sul computer, si è ritenuto di dover trattare la materia in questo articolo (e non in quello pubblicato nel numero precedente) spostando l'attenzione su informatica e telematica come possibili veicoli dell'illecito. Il nesso con la Rete discende dalla possibilità di "scaricare" programmi per elaboratore da siti specifici detti warez, per mezzo di accessi ftp anonimi, vale a dire aperti a tutti, o riservati ovvero più di rado avvalendosi della posta elettronica o di altri sistemi di corrispondenza (es. Irc e Icq). Ma certamente il mezzo oramai più "popolare" per la diffusione (anzi, un vero e proprio scambio) di opere digitali è il peer to peer, da Napster in poi. E non è un caso che, accanto alle condotte tradizionalmente sanzionate (principalmente dagli artt. 171-bis – per software e banche dati – e 171-ter lda – per audio e video) più di recente il legislatore abbia voluto colpire proprio questi traffici, sia se compiuti per lucro (art. 171-ter, comma 2, lett. a-bis) lda) che per scopi non lucrativi (art. 171, comma 1, lett. a-bis) lda). E proprio questo caso, tutt'altro che infrequente, merita qualche piccola riflessione in quanto la norma punisce "chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma (…) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa". Anzitutto, si comprende che la sanzione è destinata non soltanto al pur diffuso peer-to-peer, ma a qualsiasi immissione in Rete, come il semplice inserimento in un sito Internet. In secondo luogo, non può dirsi penalmente illecita l'attività di mero "scaricamento", il download di opere protette ad esempio mediante software di peer-to-peer in quanto, a ben vedere, la norma sanziona l'immissione, dunque il "caricamento" cioè l'upload. Certo è che, come già visto in tema di pedopornografia, molti programmi di peer-to-peer pongono automaticamente in condivisione, rendendo possibile l'upload, ciò che è stato scaricato e che, pertanto, pur in presenza del fatto obiettivo dell'immissione, non potrà darsi per scontata la volontarietà della condotta. A ogni modo, sempre per l'ipotesi di traffici compiuti senza fini di lucro, il legislatore ha comunque previsto una sorta di oblazione sui generis che comporta l'indubbio vantaggio dell'estinzione del reato: "chiunque commette la violazione di cui al primo comma, lettera a-bis, è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato" (art. 171, comma 2, lda). Tornando alle condotte già tradizionalmente sanzionate in principalità dagli art. 171-bis e 171-ter lda, vanno, infine, menzionati due recenti orientamenti giurisprudenziali. Il primo, relativo al solo software (art. 171-bis, comma 1, lda), ha escluso la rilevanza penale dell'uso (rectius: della detenzione) di programmi per elaboratore da parte di un professionista in quanto la norma sanziona esclusivamente la destinazione alla commercializzazione o l'uso da parte di un imprenditore (Corte di Cassazione, sezione III penale, sentenza 22 ottobre 2009 - dep. 22 dicembre 2009, n. 49385/09, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=829). Il secondo orientamento, di ben più ampia portata, è ancora più rivoluzionario. La Corte di Giustizia delle Comunità Europee ha, infatti, dichiarato l'illegittimità della vidimazione Siae, cioè del "bollino" posto sui supporti contenenti le opere (Corte di Giustizia delle Comunità Europee, terza sezione, sentenza 8 novembre 2007, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=492). Con conseguente inapplicabilità, almeno sino alla regolarizzazione da parte del nostro Paese, delle ipotesi delittuose incentrate sul predetto contrassegno come, per esempio, la detenzione (per tutte, Corte di Cassazione, sezione III penale, sentenza 12 febbraio 2008 - dep. 2 aprile 2008, n. 13810, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=602).

6. Carte di credito e di pagamento Con il dl 3 maggio 1991, n. 143 (convertito nella l. 5 luglio 1991, 197), il legislatore ha esordito nel diritto penale delle tecnologie regolando, sotto il profilo penale, i documenti "elettronici" distinti, in dottrina, dai documenti "informatici" nell'articolo precedente. Come è noto, infatti, le carte di credito, i mezzi di pagamento, una semplice Viacard o una carta di credito telefonica e i documenti per il prelievo di denaro contante, ad esempio il bancomat, sono normalmente supportati da strumenti telematici. Molto conosciuta, poi, è la realtà del commercio elettronico affiancato da sistemi di transazione online. L'art. 12 del decreto prevede tre distinte ipotesi coincidenti con il semplice uso indebito (del non titolare); la falsificazione o l'alterazione; il possesso, la cessione o l'acquisto di tali documenti di provenienza illecita o comunque falsificati o alterati. Si tratta, in sostanza, di condotte dette di carding. Pertanto, per quanto ci interessa di più, l'inserimento, da parte del non titolare, degli estremi di una carta di credito per effettuare una transazione online costituisce "uso" penalmente illecito a prescindere dalla detenzione della carta stessa.

7. Il "phishing" Fenomeno criminale relativamente recente, il phishing (dall'inglese storpiato "to phish", cioè pescare) consiste nella vera e propria "pesca" di credenziali normalmente per l'accesso a servizi bancari online. Si tratta di un caso di vera e propria ingegneria sociale che si dispiega, di regola, in più fasi. Anzitutto, il malintenzionato, detto phisher, si procura un certo numero, di solito molto elevato, di indirizzi di posta elettronica (spesso acquisiti illegalmente) predisponendo uno o più siti trappola, copie pressoché identiche di quelli realmente gestiti dagli istituti di credito. Utilizzando la predetta banca dati email, il phisher, così, invia messaggi che riproducono la grafica dei vari istituti di credito e, con una scusa (normalmente, si evidenzia la necessità di aggiornamento dei dati), invita i

destinatari a cliccare su un link che conduce al sito trappola per l'inserimento delle credenziali di accesso al servizio online (nome utente e password). Così, i dati inseriti dall'ignaro utente giungono in possesso del phisher il quale, eventualmente per interposta persona, li utilizza per accedere ai servizi online ed effettua operazioni a proprio favore (o di interposta persona che partecipa a questa fase di riciclaggio). In pratica, dunque, l'utente viene letteralmente truffato anche mediante quello che, pur in modo giuridicamente non corretto, viene chiamato "furto d'identità". Pur non esistendo, nel nostro Paese, una disciplina specifica, la giurisprudenza, sufficientemente consolidata, ha ravvisato in dette attività quanto meno i reati di truffa (art. 640 cp), sostituzione di persona (494 cp) e accesso abusivo a sistema informatico o telematico (art. 615-ter cp). Analogo al phishing è lo smishing, tecnica criminale che, come intuibile, viene veicolata tramite sms (in tema, Tribunale di Milano, ifficio Gip., sentenza 15 ottobre 2007 - dep. 7 novembre 2007, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=550). **8. I dati personali in Rete** Con la legge 31 dicembre 1996, n. 675, il legislatore italiano è finalmente intervenuto disciplinando positivamente il tema dei dati personali dopo una lunga gestazione dottrinale. Più tardi, si è definitivamente approdati a una legislazione più accurata e organica con l'entrata in vigore del decreto legislativo 30 giugno 2003, n. 196 (vero e proprio testo unico sui dati personali) contestualmente all'abrogazione della precedente l. 675/96. Tra le molteplici definizioni offerte dalla vigente disciplina, tre paiono essere di fondamentale importanza al fine di inquadrare meglio gli abusi riguardanti i dati personali. Trattamento è "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati". Dato personale corrisponde a "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Infine, l'interessato è "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali". Ciò premesso, è agevole concludere che uno degli illeciti più diffusi in Rete relativamente ai dati personali è il c.d. spamming. Con tale espressione, ancora una volta di origine anglosassone, si intende l'invio massivo di comunicazioni, eventualmente commerciali, non richieste. E in Rete ciò, ovviamente, avviene mediante la posta elettronica. Se, infatti, un indirizzo di posta elettronica è in grado di identificare la persona e la raccolta nonché l'utilizzo di esso costituisce "trattamento" secondo la definizione testé riportata, è chiaro che lo "spammer" può essere accusato, ricorrendone i presupposti, di trattamento illecito di dati personali, reato previsto e punito dall'art. 167 dlgs 196/2003. Questo il caso più frequente e tipico della Rete. Ma è chiaro che, vista anche l'ampiezza delle definizioni contenute nel testo unico (specie quella di trattamento), in alcuni casi la pubblicazione su Internet di dati personali può condurre alle sanzioni penali appena viste. Ma ciò, si badi bene, a condizione che il trattamento, oltre a essere illecito (normalmente senza il consenso validamente espresso), sia avvenuto a fini di profitto o di danno da parte dell'agente, e che comunque abbia cagionato un nocumento. In argomento, va riferita una controversa decisione con la quale la Suprema Corte ha stabilito l'irrilevanza penale della pubblicazione di dati presenti su elenchi pubblici (Corte di Cassazione, sezione III penale, sentenza 17 novembre 2004 - dep. 15 febbraio 2005, n. 5728, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=93). **9. Le regole per le indagini informatiche** Le indagini informatiche sono oramai centrali per l'accertamento di qualsiasi reato, non soltanto informatico o, comunque, collegato al mondo digitale. La cronaca parla da sé, in modo più che eloquente. È normale, dunque, che il legislatore si sia progressivamente interessato alla regolamentazione delle indagini informatiche e anche dell'informatica forense, computer forensic, vale a dire quella disciplina che, secondo la definizione data da Wikipedia, "studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici". Già con la l. 597/93 il legislatore aveva introdotto il preziosissimo strumento delle intercettazioni telematiche (artt. 266-bis e 268, comma 3-bis, cpp). Successivamente, in seno alla disciplina dei dati personali, precisamente all'art. 132 dlgs 196/2003, sono state poste regole peraltro più volte rimaneggiate, per l'acquisizione dei log, vale a dire dei tabulati relativi alle comunicazioni telematiche (con esclusione del contenuto). Ma l'intervento più mirato è fatto recente. La già menzionata l. 48/2008, di ratifica della convenzione di Budapest, si è, infatti, occupata proprio di quanto rilevante per l'informatica forense. Relativamente a ispezioni, perquisizioni e sequestri, anche di corrispondenza telematica, il legislatore ha voluto sottolineare la necessità che i dati informatici acquisiti siano conformi alla fonte e immodificabili. In proposito, appare emblematico il testo dell'art. 254-bis cpp, introdotto proprio dalla predetta legge: "Art. 254-bis. - (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). - 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali". Purtroppo, malgrado sia da apprezzare lo sforzo del legislatore, non si può nascondere che precetti come quello appena visto sono, in realtà, privi di sanzioni processuali espresse (ad esempio, l'inutilizzabilità). È,

però, ragionevole attendersi che, vista l'inequivoca volontà del legislatore in merito alla delicatezza della prova informatica, il giudice valuti con estremo rigore gli esiti delle indagini informatiche.

European Working Party on Information Technology La diffusione dei reati informatici ha determinato l'attivazione di fori specialistici in seno a tutte le più importanti organizzazioni per la cooperazione internazionale di polizia. Presso il Segretariato generale dell'Interpol, a Lione, è stato costituito, nel 1990, il Gruppo di lavoro europeo per la criminalità informatica (Ewpict), che lì si riunisce tre volte l'anno. L'Interpol è, infatti, attivamente coinvolto, da diversi anni, nel contrasto ai crimini legati alla tecnologia dell'informazione. Il Segretariato generale dell'organizzazione ha quindi ritenuto opportuno mettere a frutto la competenza dei membri nazionali, nel campo del crimine nella tecnologia dell'informazione (Itc), creando un gruppo di lavoro ad hoc, dove dagli esperti nazionali del settore potessero incontrarsi e mettere a fattore comune le esperienze maturate. Le principali finalità del gruppo sono l'approfondimento e lo scambio di informazioni sulle metodologie di contrasto alla criminalità informatica nonché la creazione di un manuale investigativo, riservato alle forze di polizia, che contiene, tra l'altro, la legislazione di contrasto ai crimini informatici vigente in ciascun Paese del mondo. Tra gli obiettivi del testo, vi è quello di rendere uniformi le procedure di perquisizione, sequestro e conservazione delle prove informatiche, così da poter dar vita, nei casi di crimini transnazionali, a una reale collaborazione tra le diverse forze di polizia. Altra attività di fondamentale importanza svolta dallo Ewpict è l'organizzazione di corsi di formazione ed aggiornamento, rivolti agli operatori delle forze di polizia, sulle tematiche di competenza del gruppo. *Mauro Valeri*

La risposta dell'Europol ai crimini informatici I crimini informatici ricadono esplicitamente tra quelli di competenza dell'Europol. Per questo nel 2002 è stato creato l'High tech crime center, Centro per il crimine informatico, all'interno del Dipartimento per i fenomeni criminali rilevanti. La capacità di reprimere il cybercrime è molto disomogenea negli Stati membri e differenti sono le metodologie e gli strumenti tecnologici di contrasto a disposizione di questi. Proprio per questo è fondamentale l'opera del Centro, la cui funzione è quella di combattere e reprimere i crimini informatici, offrendo agli Stati membri una piattaforma comune di strumenti e metodologie di contrasto ed un punto di riferimento unico nella lotta a questo tipo di criminalità. Per rendere la propria attività di coordinamento più incisiva e determinante l'Europol sta sviluppando tre progetti: Icros, Cyborg ed Iforex. Il cuore dell'Icros, Sistema di denunce online dei reati su Internet, sarà costituito da una piattaforma comune europea dove saranno contenute tutte le denunce per i reati perpetrati sulla rete Internet. Questo permetterà di evitare la duplicazione di indagini sullo stesso caso tra i diversi Stati membri e di conoscere, in tempo reale, le nuove tipologie di reato poste in essere. Il progetto Cyborg, Criminalità informatica organizzata, mira, principalmente, a creare una mappatura delle organizzazioni criminali in Europa che traggono, dai reati perpetrati sulla rete Internet, il proprio sostentamento. Iforex, Piattaforma per la conoscenza di Internet e dell'analisi forense, si baserà invece su un portale che offrirà, alle forze dell'ordine degli Stati membri, utilissimi consigli investigativi ed approfondimenti tecnici sulla rete Internet e sulla criminalità informatica. In avanzato stato di realizzazione è infine il progetto che prevede di dare vita, in collaborazione con alcuni prestigiosi atenei europei, a specifici master sul cybercrime. *Mauro Valeri*

Scarica l'inserto in formato PDF

01/12/2010