

278

30 1/2

UFFICIO AA.GG. e PERS.

- 9 GEN. 2007

MICHELE GUERNELLI - IGOR SECCO

RELAZIONE SULL' INCONTRO DI STUDI "FORME DI MANIFESTAZIONE E STRATEGIE DI CONTRASTO DELLA CRIMINALITA' SU INTERNET" - TREVIRI 4-9.12.2006

PREMESSA

L'incontro, organizzato dal Ministero della Giustizia bavarese e aperto alla partecipazione di giudici e pubblici ministeri della Germania e di altri Paesi europei, si è svolto in otto sessioni antimeridiane e pomeridiane, di tre ore circa ciascuna e ripartite nell'arco di quattro giornate, con approfondimenti della tematica sia dal punto di vista teorico che pratico.

Lo svolgimento si è articolato con relazioni (tutte supportate da slides e dirette proiezioni da videate di computer), aperte alle domande e agli interventi dei partecipanti.

Dal punto di vista strettamente giuridico l'analisi ha riguardato sia il diritto sostanziale sia gli aspetti processuali nel diritto tedesco, con particolare riferimento alla giurisprudenza e agli aspetti critici derivanti dalla particolarità del mezzo tecnico in questione (i dati e i sistemi informatici e internet come oggetto materiale, oggetto giuridico e strumento della nuova criminalità) e dalla conseguente necessità di inquadramento, adattamento, razionalizzazione ed armonizzazione a livello interno, comunitario ed internazionale. Le relazioni su questi aspetti sono state svolte da giudici e docenti universitari.

Dal punto di vista pratico sono state analizzate le principali forme di manifestazione della criminalità informatica attualmente incontrate nella casistica tedesca (peraltro del tutto simile a quella italiana e "globale"), in connessione con le spiegazioni tecniche e di aggiornamento necessarie per comprendere lo stato attuale dell'"arte" (progresso, connessioni, frazionamento e potenzialità dei sistemi informatici), e le possibilità di contrasto sia preventivo (impedimento attraverso tecnologia di sicurezza) che repressivo (accertamento del fatto e individuazione del responsabile). Le relazioni su questi aspetti sono state svolte da responsabili per la sicurezza di Deutsche Telekom e da funzionari di polizia.

SINTESI DELLE RELAZIONI

1. "Diritto penale sostanziale, applicazione del diritto penale tedesco alla criminalità informatica, problemi della prassi delle Procure" (C. Weiß, giudice del Tribunale di Monaco di Baviera).

L'analisi ha esaminato i caratteri delle singole fattispecie (Tatbestandsmerkmale) del codice penale tedesco inerenti la criminalità informatica, e quindi:

- § 202.a StGB: "Procacciamento di dati" ("(1) Chiunque indebitamente procura a sé o ad altri dati a lui non destinati e protetti contro l'accesso illegittimo è punito... (2) Dati ai sensi del comma 1 sono solo quelli che vengono memorizzati o trasmessi elettronicamente, magneticamente o in altro modo non immediatamente percepibile"), che tutela il domicilio informatico ("violazione di domicilio elettronico", "elektronischer Hausfriedensbruch") ovvero la disponibilità dei legittimati contro l'accesso abusivo. I dati come sopra definiti non costituiscono necessariamente segreti né sono necessariamente personali; è indispensabile la violazione di misure di sicurezza ma non sufficiente, occorrendo (a differenza che nel nostro 615 ter c.p.) il "furto di dati"; viceversa il mero impiego illegittimo

di dati di cui si ha la legittima disponibilità non è punito ai sensi di questa norma, subordinata alla querela e con tentativo non punibile. E' possibile un concorso formale o apparente con il § 17.2 UWG (legge sulla concorrenza sleale del 2004), caratterizzato dalla posizione del soggetto attivo, ad esempio il collaboratore di una impresa che copia dati da consegnare a un concorrente è punibile anche se non riesce nell'intento ed è legittimato all'accesso.

- § 303.a StGB: "Mutamento di dati" ("Chiunque illegittimamente cancella, sopprime, rende inservibili o immuta dati, è punito...");
- § 303.b StGB: "Sabotaggio informatico" ("Chiunque danneggia una elaborazione di dati di interesse essenziale per una altrui impresa, azienda o una Autorità in modo tale da: 1. integrare un fatto ai sensi del § 303.a oppure / 2. distrugge, danneggia, rende inservibile, elimina o immuta un impianto di elaborazione o un supporto di dati, è punito..."); si tratta di fattispecie perseguibili su querela o istanza e con tentativo punibile (ad es. l'installazione del programma finalizzato al danneggiamento), che tutelano la prima l'utilizzabilità delle informazioni contenute nei dati memorizzati, e la seconda l'interesse del sistema economico e della amministrazione al corretto funzionamento dell'elaborazione dei dati. Non è necessario forzare misure di sicurezza; l'ultima parte della seconda disposizione si riferisce all'hardware o ai supporti materiali.
- § 263.a StGB: "Frode informatica" ("Chiunque, con l'intento di procurare a sé o a un terzo un vantaggio patrimoniale anti-giuridico, danneggia il patrimonio altrui influenzando sul risultato di un procedimento di elaborazione di dati tramite una errata impostazione del programma, l'impiego di dati inesatti o incompleti, l'utilizzazione non autorizzata di dati, o altrimenti tramite un indebito intervento sul procedimento, è punito..."). Come per la truffa semplice (§ 263 StGB) l'interesse tutelato è il patrimonio individuale. Tuttavia non è necessario l'inganno di una persona fisica bensì l'intervento su un sistema informatico e la sua manipolazione (apparecchi "non puramente meccanici"); l'intervento deve condurre a una disposizione rilevante dal punto di vista patrimoniale e quindi sul risultato di elaborazione di dati concernenti questo aspetto (evidenti le assonanze con l'art. 640 ter c.p. italiano; la disposizione tedesca assorbe tuttavia anche il nostro art. 12 L. 197/91 e l'uso indebito di banche dati). L'intervento può essere su un programma, o attuato con l'inserimento di dati, o semplicemente usando dei dati interni al sistema. E' astrattamente ipotizzabile un concorso con la truffa semplice, quando con i comportamenti inerenti la frode informatica si provochi un inganno e una disposizione patrimoniale della persona legittimata ad operare nel sistema; tuttavia la frode informatica dovrebbe avere carattere sussidiario. Può costituire un antecedente del delitto di riciclaggio (Geldwäsche), ad es. nel caso di programmi manipolativi "dialer" (in cui i proventi della connessione Internet a tariffa speciale vengono divisi fra più soggetti non sempre identificabili), ma non è semplice verificare nel caso singolo la consapevolezza e la responsabilità del provider e di chi offre la pagina Internet.
- § 269 StGB: "Falsità in dati probatori rilevanti" ("Chi, a fine di inganno nella circolazione dei beni giuridici, memorizza o immuta dati in modo tale che dalla loro considerazione consegue la formazione di un documento falso o non autentico, o usa i dati in tal modo memorizzati o cambiati, è punito..."); la fattispecie tutela la sicurezza e affidabilità dei dati come prova ("als Beweis") e diritto, in parallelo con il concetto analogo della falsità documentale ordinaria (§ 267 StGB); può riferirsi alle codifiche di carte di credito o delle pay tv; aspetti problematici (simili al diritto italiano) si rinvergono nelle falsificazioni delle e-mail (hanno efficacia probatoria "Beweiserheblichkeit" - ? sono documenti falsificabili anche se non muniti di firma elettronica ?) sia con riguardo al loro contenuto sia al nome del

mittente. Sembra preferibile la soluzione positiva, specialmente quanto alla casistica del "phishing" (quando si inviano falsi ordini di pagamento), qualora le e-mail contengano informazioni su cui si debba fare affidamento. Ciò sembra confermato dal § 270 StGB, che equipara la falsificazione vera e propria all'"influenzare falsamente" un procedimento di elaborazione di dati. E' poi circostanza aggravante, come per il falso "semplice", l'aver agito professionalmente o quale membro di una associazione, al fine di commettere truffe (§ 269.3 in relazione al § 267.3 StGB).

Quanto alle *forme di manifestazione e ai casi esemplificativi*, sembra evidente come i "hacking" rientri nel § 202.a, nella maggior parte dei casi derivando dall'accesso abusivo, di per sé non punibile, la disponibilità di dati altrui che appaiono sullo schermo dell' intruso.

La password altrui può essere captata attraverso programmi che utilizzano la "forza bruta", ovvero ("guessing password") attraverso e-mail fraudolente, o anche con metodi convenzionali non informatici ("social engineering"), che di per sé non rientrano nel § 202.a. L'introduzione di virus ("Computerviren") può rientrare nei § 303.a e 303.b nelle diverse e note forme di manifestazione ("Wurm", "Trojan Pferd", "destruktive Viren" come le "Logik-Bomben"); biglietti augurali via e-mail con backdoors; attacchi DOS- denial of service, anche a cascata, spam ed e-mail bombing).

Sono stati ottenuti ordini di perquisizione nel domicilio di presunti responsabili di attacchi informatici, a seguito di indagini volte ad individuare il computer sorgente, per acquisire i computer nella disponibilità degli stessi. Nel 2002 un attacco contro almeno 231 ignari utenti di cellulari attraverso l' inserimento nel sito Mini.de della BMW portò all' invio indesiderato di circa 51.000 messaggi SMS contenenti il Mini logo BMW non richiesto; introdotte misure di sicurezza furono respinti almeno altrettanti messaggi di disturbo, senza tuttavia che si potesse risalire ai responsabili (procedimento solo contro ignoti), per l'impossibilità di risalire agli indirizzi IP pertinenti, verosimilmente per il troppo breve periodo nel quale il provider è obbligato alla conservazione dei dati di connessione (80 giorni). Ancora nel 2003 un attacco spam proveniente dall'indirizzo "skol.de" (attivo per solo 2 giorni) bloccò il sito del giornale "Südkurier"; fu quindi emanato un ordine di comunicare i dati di connessione come specificamente previsto dal § 100 g/h del codice di procedura penale tedesco (StPO).

Altri casi concreti sono stati esposti attraverso copia di provvedimenti ("Beschlüsse") di perquisizione ("Durchsuchung") e sequestro ("Beschlagnahme") con gli addebiti ipotizzati dalla pubblica accusa per i reati di procacciamento di dati e mutamento di dati.

Infine, quanto ai "dialer" in rapporto alla frode informatica, si ripropone (come per il diritto italiano), una suddivisione a seconda che sulla pagina web siano spiegate le condizioni contrattuali e il meccanismo di adesione - poi rispettati - , con download e installazione chiaramente collegati all' assenso dell' utente (nessuna punibilità), ovvero alcuni aspetti siano lasciati e/o il programma venga installato in tutto o in parte senza o contro la volontà dell' utente (punibilità per frode informatica, mutamento di dati o sabotaggio).

Un esempio esposto di frode informatica ha riguardato accrediti fraudolenti sui conti dei responsabili anziché su quelli dei titolari di carte di credito commesso da impiegati della Loyalty Partner GmbH in circa 3000 casi nel corso del 2003, con un danno per la società di circa 115.000 Euro; ancora la Corte di Cassazione tedesca (BGH) ha con due decisioni stabilito che la ricarica abusiva di carte telefoniche con appositi apparecchi costituisce falsità rilevante ex § 269 StGB in quanto il chip di memoria delle stesse contiene dati rilevanti dal punto di vista

probatorio (decisione 13.5.2003); che l'utilizzo illecito di SIM card da parte del titolare non costituisce né truffa semplice né frode informatica (decisione 31.3.2004).

2. "Attività e responsabilità dei provider in Internet; aspetti di danno sulle reti di trasmissione di dati e misure di difesa" (Ing. P. Quick e Mich. W. Reinert, direzione Deutsche Telekom)

Sono state deliberate la cronistoria e l'attuale dimensione del fenomeno Internet, da rete universitaria - militare a rete aperta, multilaterale e non più bilaterale, con una molteplicità di sistemi autonomi e di "snodi", per consentirne il funzionamento anche in caso di interruzione locale, e quindi "insicura per natura", cosicché i nemici sono "interni" e gli utenti "devono difendersi da soli".

Si è rilevato come, dal punto di vista economico, secondo un resoconto del 2005 il giro di affari su Internet ha superato i 1000 miliardi di dollari, così come gli utenti della rete, diretti o indiretti, hanno superato la soglia del miliardo di persone; che negli ultimi due anni possono stimarsi in diversi milioni i sistemi informatici infettati da virus solo nell'ambito dei servizi D.L.

Le forme di danno ("Schadensformen") riscontrabili su Internet riguardano un uso "diverso da quello normale" o addirittura illegale, come l'incasso di somme di denaro senza consegna della merce, gli attacchi alla borsa elettronica, le violazioni del diritto di autore, la truffa con le carte di credito, le lotterie e il gioco d'azzardo anche come strumento di riciclaggio di denaro, l'uso di programmi di remote-control, ecc.

Sugli autori e i motivi delle condotte abusive o illecite si sono suddivisi gli operatori interni (ad es. collaboratori delle imprese) da quelli esterni, ecc.

Le possibilità di accesso abusivo (hacking) sono state moltiplicate dalla diffusione e dalla semplicità ed economicità della tecnologia utilizzabile, ormai alla portata di non esperti, e con hardware e software ampiamente disponibili anche nella rete stessa.

Difficilmente l'hacking è fine a se stesso, ma comporta finalità ulteriori delle condotte, quali l'estorsione ("hacking als Geschäft", come affare), la vendita di informazioni acquisite, la truffa con carte di credito, lo spionaggio o il sabotaggio industriale (anche con "web defacement"). Da notare anche la possibilità di inserire "attacchi automatizzati" o che si riproducono all'infinito.

Ulteriori possibilità sono state offerte dalla diffusione delle reti WLAN (*wireless local area network*), a loro volta connesse esternamente ad Internet, e nelle quali è possibile introdursi assai agevolmente anche con tecniche (ed "antenne") rudimentali, captando dati e utilizzando la connessione del computer attaccato per navigare (surfering, programma "wardriver") in rete a spese della vittima. Vi sono programmi che permettono una sufficiente difesa da questi attacchi e in ogni caso sono consigliabili modalità di gestione WLAN "chiuso" o con crittografia.

Quanto al phishing, si è puntualizzato che esso si concretizza in un furto di identità elettronica ("Identitätsdiebstahl") attuato con le già citate social engineering, e-mail fraudolente, worms o backdoors; gli indizi di riconoscibilità essendo costituiti dalla falsità del mittente del messaggio, dalla impersonalità dell'interpello (es. "a tutti i clienti"), dalla prospettazione nei messaggi di conseguenze in caso di mancata comunicazione di dati o risposta.

Sulla attività e responsabilità del provider si è evidenziato il critico problema dello scarso periodo di conservazione dei dati di traffico ai fini di una qualunque efficacia nelle indagini e della impossibilità di controllo dei contenuti messi a disposizione dai provider.

3. "Sabotaggio di computer, Internet - hacking, programmi dialer, procacciamento di dati, frode informatica" (J. Müller, Commissario capo di polizia criminale, Monaco di Baviera).
4. "Indagini preliminari su Internet, indagini sulla pedopornografia in collegamento con indagini internazionali, E - Boy" (A. Betschelsrieder, Direttore dell' Ufficio criminale statale, Monaco di Baviera).

Oltre agli aspetti evidenziati in precedenti relazioni, e a numerosi esempi concreti esposti di pagine web che prospettano comportamenti illeciti anche di rilevante gravità (costruzione di ordigni, istigazione a comportamenti violenti, pornografia ecc.), si sono enumerati i principali servizi oggi disponibili su Internet, quali il WWW, FTP (file transfer protocol), la posta elettronica, usenoi (newsgroup), l'Internet relay (dialogo chat), il Telnet (controllo a distanza dell'elaboratore), la realizzazione e gestione di pagine Internet.

Sugli "scenari di attacco" si è aggiunto che questi possono riguardare anche il domain name service (accaparramento o copia di nomi a dominio, riproduzione fraudolenta di siti con il cd. phishing); si è accennato alle trasmissioni illecite occultate tramite steganografia.

Si è prospettato il problema che la delocalizzazione delle condotte (ad. es. nel trasferimento di denaro in varie parti del mondo con Western Union) pone, di allineamento dei procedimenti sia a livello interno (fra i singoli Länder) che internazionale, evidenziando la attuale assenza di un coordinamento federale in Germania, come presente per la criminalità organizzata o il terrorismo.

Ne consegue la sempre più pressante necessità di cooperazione giudiziaria (ad. es. rete Eurojust) che però non riesce spesso a coprire l'area extracuropea, o comunque non in tempi utili.

Si è calcolato che circa il 5% dei contenuti di Internet vanno considerati attualmente illeciti, pur essendovi una ampia "zona grigia", contrari ad. es. alle norme interne sulla pornografia, sulle armi, sui farmaci, sul diritto di autore, sulla protezione della gioventù, ecc.

Si è ribadito come le reti di trasmissione di dati costituiscono o possono costituire lo strumento materiale dei reati (ad. es. con le truffe tramite le case d'asta).

5. "Assicurazione e valutazione dei dati all'interno e all'estero, modalità di estrazione e risalita alla fonte di dati" (R. Richard, Commissario capo della polizia criminale di Monaco di Baviera)

La relazione ha preso in esame e classificato i diversi supporti di dati suddividendoli rispetto alla possibilità di protezione dalla riscrittura (hard disk, floppy e MOD, CD ROM e DVD) e trattando la struttura in settori del disco fisso, nonché quanto avviene in caso di cancellazione (che conserva traccia dei dati cancellati).

Fondamento della assicurazione dei dati è la possibilità di renderli gli stessi immutabili; tale possibilità con il disco rigido si ottiene con la cosiddetta "Image- Sicherung", essendo

impossibile agire sull'originale se ne ottiene una copia unica ("clone") attraverso i boot-diskette/CD, senza interagire con il sistema hardware esaminato, e mediante determinati programmi di assicurazione dei dati ("forensische software") fra cui *Encase*. Con questi programmi è possibile verificare e risalire all'inserimento dei dati, all'ultimo cambiamento, e ai dati precedenti.

Non è invece semplice risalire al computer che ha inviato determinati messaggi via Internet. Infatti il browser (software per la navigazione in WWW) non consente di risalire al server inizialmente utilizzato e quindi all'IP - address assegnato dal provider, ma solo al "proxy server" (al suo numero IP), che appare negli headers dell'e-mail.

Esistono poi su Internet provider che offrono programmi e "servizi di anonimato" (JAP, rewebber, an.on.surf ecc.), in modo da rendere impossibile o estremamente difficoltoso risalire al computer che ha immesso determinati contenuti in rete attraverso l'occultamento degli headers (mittente, ricevente, data, lunghezza ecc.) o la crittografia dei contenuti; è comunque possibile ottenere anche nei confronti di questi providers provvedimenti di controllo e registrazione dei dati di traffico ai sensi del § 100.a StPO (caso dei dati trafugati ad Allianz Assicurazioni a fini estorsivi), dati comunque che gli stessi hanno l'obbligo di fornire in caso di commissione di reati anche ai sensi del § 113 TKG (Telekommunikationsgesetz del 2004); i dati rilevanti del traffico possono comunque essere conservati per un termine non superiore a sei mesi secondo il § 6 comma 7 TDDStG (Telemediendatenschutzgesetz, legge per la protezione dei dati dei servizi di telecomunicazione del 1997), e che attualmente in concreto varia da operatore ad operatore a seconda delle finalità e delle condizioni contrattuali. Il problema si pone per gli utenti "flatrate" (con tariffa a forfait), i cui dati di traffico devono essere secondo la giurisprudenza immediatamente cancellati dopo la comunicazione stessa, e comunque non ne è consentita la memorizzazione captandoli on line (BGH, sentenza del 26.10.06).

Tuttavia una direttiva europea da recepire nel corso del 2007 imporrà di conservare i dati rilevanti del traffico per almeno sei mesi (2005/182/COD).

Pur essendo l'intercettazione dei dati telematici in linea di massima possibile, resta critica l'individuazione del provider di cui l'intercettato è cliente; altro elemento critico è costituito dal VOIP (voice over Internet protocol), poiché la comunicazione vocale via computer non è necessariamente collegata a servizi fissi forniti da un provider, ma un software individuale può di volta in volta essere usato allo scopo, senza che si possa individuare nemmeno se i computer in comunicazione siano fissi o in movimento. *Skype* permette addirittura di collegare computer a telefoni, e più apparecchi fra loro contemporaneamente; permette di immagazzinare conversazioni come un normale e-mailbox e la normale funzione chat; non vi è un server centrale, ma può essere utilizzata la memoria di un computer collegato; le classiche intercettazioni telefoniche non sono in questo caso praticabili.

I fondamenti normativi delle intercettazioni si individuano nei § 100.a/b StPO (ordine solo del giudice, o del PM in caso di pericolo nel ritardo, da convalidare entro tre giorni, durata massima tre mesi); della comunicazione dei dati di traffico nei già menzionati § 100.g/h; nel § 100.i per quanto riguarda la telefonia mobile e le reti WLAN (durata massima 6 mesi), nei § 112 e 113 TKG quanto ai dati automatizzati o manuali da fornire da parte dei fornitori di servizi di telecomunicazione.

Sono state quindi esaminate le modalità tecniche delle intercettazioni (celle di trasmissione della telefonia mobile, localizzazione geografica, intercettazioni di SMS, SMS "silenziosi", ecc.) e i concetti connessi (SEM card, IMEI, IMSI con documentazione in una perizia sul punto

del Tribunale di Monaco, per le reti WLAN il corrispondente MAC - multimedia address control).

6. "Attuali questioni giuridiche inerenti l'assicurazione e la valutazione dei dati FDD (EDP-electronic data processing) nel diritto interno e all'estero"

7. "Attuali questioni giuridiche inerenti le indagini nelle reti di trasmissione di dati e attuali sviluppi della legislazione e della giurisprudenza nella assicurazione della prova FDD" (di W. Bär, giudice della Corte di Appello di Bayreuth)

Promossa la necessità che il legislatore consideri attentamente lo sviluppo tecnologico del settore e la rapida crescita degli illeciti in materia (Corte Costituzionale federale, BVerfG, decisione del 12.4.05), si è inizialmente osservato come importanti norme processuali risalgano ancora al secolo scorso (§ 94.102 StPO sulla assicurazione delle fonti di prova), mentre gli attuali problemi emergenti sono costituiti dalla scarsità dei precedenti giurisprudenziali, dalla carenza di comprensione tecnica da parte degli operatori, dal pericolo di dispersione di dati probatori rilevanti in brevissimo arco di tempo.

Limiti costituzionali sono presenti non nell'art. 103.2 Cost. (GG) in quanto il divieto di analogia vale solo per il diritto penale sostanziale, ma nell'art. 20.3 GG per il quale la legislazione si deve ispirare al principio costituzionale per il quale il potere esecutivo e giudiziario si conformano alla legge e al diritto, da cui consegue il divieto di estendere le disposizioni invasive oltre il tenore letterale delle medesime (es. intercettazioni ambientali e confronto vocale).

L'intervento sulle telecomunicazioni presuppone un inquadramento delimitativo dei dati di telecomunicazione, da suddividere in: dati sulla consistenza (Bestandsdaten, §3 n. 3 TKG del 2004, nome e altri dati contrattuali dell'utente, numero IP non dinamico, nomi relativi all'e-mail), del traffico o del collegamento (§ 3 r. 30 TKG, mittente, destinatario, durata localizzazione, IP address "dinamico"); vi è discussione se possano essere acquisiti su decreto del giudice ex StPO o provvedimento del PM o di polizia ex § 113 TKG), relativi all'indirizzo (solo per servizi televisivi e di altri media, § 6 TDDStG, § 19 MDSIV), relativi al contenuto della comunicazione (§ 3 r. 22 TKG), all'accesso (password, PIN, PUK ecc.; non ricadono nella salvaguardia dell'art. 10 GG relativo alla corrispondenza se non vi è in concreto una comunicazione).

L'identificazione degli utenti della rete si consegue con l'indirizzo IP, che però non è fisso per i privati, ma concesso, in quanto in numero limitato, per la sola durata della comunicazione (indirizzo dinamico), e quindi dipende, per la sua individuazione, dalla collaborazione del provider, considerati inoltre i limiti temporali di memorizzazione di cui si è detto e la problematica della clientela "fluttuante".

L'intercettazione delle telecomunicazioni comprende ogni forma di mezzo e contenuto (dati, suoni, immagini, segnali ecc.); il dovere di collaborazione degli operatori in caso di provvedimento dell'autorità è sancito dal § 100.b comma 3 StPO. Questioni si pongono per le reti interne e per l'acquisizione delle videate (valgono le norme generali su perquisizioni e sequestri).

Fra i reati che consentono le intercettazioni (§ 100.a StPO), pur in via di mutamento (inserita la pedopornografia), non sono ancora tuttavia compresi quelli inerenti la criminalità economica e informatica, ma vi è una clausola generale di chiusura che comprende i reati di "rilevante significato". Gli "interessati" dal provvedimento sono l'indagato, chi è in

comunicazione con lui, e chi gestisce il collegamento; il provvedimento scritto deve contenere il numero interessato ovvero altri dati identificativi del collegamento, le modalità, l'inizio, la durata (3+3 mesi - § 100.b c. 2 StPO).

Questioni particolari concernono la localizzazione dei cellulari in stand-by (che siano "pronti alla ricezione", consentita e al di fuori dell'art. 10 GG, BVerfG 22.8.06), l'IMEI (International Mobile Equipment Identity) comunque incluso nel § 100.b StPO, non ancora possibile con tutti i gestori), il roaming (l'appoggio presso altri gestori), la comunicazione via e-mail (che include il passaggio fra il server del mittente e quello del destinatario, e la memorizzazione su entrambi, ascrivibile anche al § 94 e ss. StPO, come da giurisprudenza costituzionale; la conclusione non cambia con la cd. web-mail), il VOIP e il cd. collegamento peer-to-peer (difficoltà tecniche e specifica proposta di legge), l'IMSI (International Mobile Subscriber Identity, numero di chiamata identificativo dell'utente, la cui captazione serve per localizzare utente o apparecchio, ovvero identificare apparecchio e carta SIM).

La sanzione per l'acquisizione fuori dai limiti di legge è la inutilizzabilità (giurisprudenza costante BGH). Non vi è divieto di utilizzazione per le parti della intercettazione illegittimamente acquisite se è impossibile effettuare cancellazioni selettive (Trib. Francoforte, 2005).

Più specifiche disposizioni sono dettate dal regolamento sulle intercettazioni nelle telecomunicazioni (TKÜV), novellato nel 2005, che prevede la possibilità di intercettare reti intere sopra i 1000 utenti, e all'estero ove ivi sia il destinatario, e all'interno vi sia il terminale di partenza.

I dati del collegamento devono essere forniti ai sensi del § 100 g StPO per fatti determinati e "di rilevante significato", e nel caso che collegamento vi sia (non a cellulare spento), sia per comunicazioni pregresse che future, e con termine e certezza degli interessati analogo a quello delle intercettazioni; vi è contrasto in ordine all'ascrivibilità rispetto ai dati relativi al pedaggio autostradale.

La competenza territoriale si radica nel luogo della sede regionale del fornitore di servizi che detiene i dati (BGH, 2003). Il provvedimento deve contenere nome e recapito dell'indagato, numero identificativo ecc. o altri dati conosciuti se a carico di ignoti (anche solo indirizzo IP dinamico, Trib. Ulm, 15.10.2003).

Per il § 100.h StPO in caso di reato di "rilevante significato" basta definire nel tempo e nello spazio la comunicazione della quale si richiedono i dati, quando ulteriori specificazioni ostacolerebbero o impedirebbero la ricerca; vi è contrasto nella giurisprudenza di merito in ordine alla necessità di una previa verifica dell'esistenza o dell'avvenuta comunicazione.

L'indagine non può aver corso in caso di diritto di astenersi dal deporre (parlamentari, difensori dell'indagato, religiosi - §100.h), e i risultati possono essere utilizzati solo in altri procedimenti contemplati nel § 100.g comma 1 (100.a c. 1) StPO.

I dati di collegamento presenti sulla memoria di un cellulare che ricadono nell'art. 10 GG (inviolabilità della corrispondenza) sono acquisibili previo sequestro solo ai sensi del § 100.g/h StPO (BVerfG, 4.2.05); la tutela cessa quando l'informazione è consentita dal destinatario (BVerfG, 2.3.06).

Quanto ai dati "statici" relativi al rapporto (nome, recapito dell'utente ecc. - "Bestandsdaten") le questioni di delimitazione fra StPO e § 111 e ss. TKG riguardano le password e gli indirizzi IP dinamici.

E' intercettazione qualunque controllo statale all'insaputa di entrambi i partner della comunicazione (BVerfG); pertanto è possibile il libero ascolto di comunicazioni con l'assenso di uno dei soggetti, e se un soggetto è la polizia (BGH).

In ordine alla *perquisizione (Durchsuchung)*, personale o locale, consentita sul sospettato e altre persone ai sensi dei §§ 102 e 103 StPO, e ai fini del sequestro, si pongono questioni di superamento di programmi di protezione (firewall, password ecc.), di accesso a dati protetti (anche dal diritto di autore, consentiti ai sensi del § 45 UrhG) o segreti, e soprattutto qualora i dati siano conservati e vadano attinti in luogo diverso da quello in cui si trovano gli spazi perquisiti: in questo caso, se si è all'interno del territorio nazionale, o si ottiene un provvedimento dell'autorità territorialmente competente, ovvero si procede ugualmente se vi è pericolo nel ritardo (§ 105 StPO, BVerfG, 20.2.2001).

Se i dati sono conservati all'estero, si pongono problemi di giurisdizione e cooperazione giudiziaria, previsti dalla convenzione 23.11.2001 sul Cyber Crime (art. 19 per lo spazio interno, 29, 32 per quello dei paesi contraenti).

Secondo il Tribunale di Stoccarda (2002) non è sufficiente un sospetto di inizio di reato per la perquisizione di un Host provider che non possa essere ritenuto responsabile ai sensi delle disposizioni del TDG (Telemediengesetz, legge sui servizi di telecomunicazione), come novellata per il recepimento della direttiva 2000/31/CE (§ 8 e ss.), secondo una differenziazione di responsabilità conforme al d.lg. 70/03 italiano fra Access (§ 9), Host-Service (§ 10), Content (§ 11) Providers.

Secondo il Tribunale di Francoforte (21.10.03, caso anOn) non è possibile una perquisizione presso un terzo al fine di sequestro di dati di collegamento.

L'ispezione di documenti (§ 110 StPO) possibile da parte del PM e di suoi incaricati (o della sola PG su assenso dell'ispezionato), comprende anche "documenti tecnici" quali supporti di dati e computer (BGH, 1988). Non vi sono divieti di utilizzabilità in caso di violazione del § 110 (Trib. Magdeburg: 12.10.2000).

E' possibile bloccare dati o conversazioni nel corso della perquisizione, anche se vi è il rischio di perdere mezzi di prova; sono necessarie particolari procedure tecniche e cautele nel procedere alla perquisizione e sequestro inerenti sistemi informatici.

Il sequestro (Beschlagnahme, § 94 StPO) comprende oggetti da assicurare quali pezzi di prova; tali possono considerarsi nel loro insieme gli impianti EDP, i supporti di dati, il computer, il disco fisso dello stesso, non anche le videate (si potrà fotografarle); l'estrazione di copia di sicurezza è compresa.

I divieti di sequestro sono quelli che riguardano la facoltà di astenersi dal deporre, e si riferiscono a comunicazioni scritte, estensibili ai sistemi informatici in quanto indipendenti dal supporto che le contiene; in un caso concreto inerente perquisizione e sequestro presso una società fra avvocati, si è stabilito che non possono essere acquisiti e devono essere cancellati i dati non inerenti lo scopo della perquisizione; mezzo che peraltro non deve essere utilizzato

qualora siano disponibili altri sistemi meno invasivi di acquisizione della prova (BVerfG, 12.4.2005).

La norma sul *sequestro di corrispondenza* (§ 99 StPO) che cita anche i "servizi di telecomunicazione", non è applicabile al telefax, in custodia (Gewahrsam) del diretto interessato, ma ai controlli delle e-mail (Trib. Ravensburg 2003), che possono essere considerati "invio di posta".

Il dovere di *testimonianza* (§ 161.a - § 48 StPO) comprende quello di rivelare i dispositivi di sicurezza e di funzionamento dei sistemi informatici; la produzione di tabulati non è un supporto scritto alla testimonianza e non costituisce deposizione scritta.

Il dovere di *esibizione*, previsto dal § 95 StPO, non si estende al dovere di rendere leggibili o intelligibili gli oggetti dell'obbligo come invece previsto in materia civile dal § 261 HGB (codice di commercio).

L'accesso ai dati crittografati (si calcola, il 10% dei dati trasmessi) e il dovere di renderli intelligibili è specificamente previsto dal § 8.3 TKJV (v. anche §§ 95 e 110.a StPO).

Le indagini sulle reti di trasmissione di dati pongono i problemi già rilevati in ordine alla acquisizione e conservazione dei dati. Esistono ormai uffici specializzati di polizia, che ad es. fanno ricorso in determinate situazioni alla creazione di fittizie identità elettroniche per agire in rete quali "agenti provocatori". Strumenti processuali o metodi di indagine adottati sono il cd. "preservation order" al provider (di non cancellare e conservare determinati dati di collegamento o contenuto); l'invio di SMS "coperti" al cellulare dell'indagato per carpire determinati dati; l'installazione di programmi "keylogger", "trojan horse" o di "sniffing" sui sistemi informatici oggetto di indagine.

8. *"La Convenzione del Consiglio d'Europa sul Cyber-Crime, significato e portata per l'UE e gli Stati nazionali. Problemi attuali del diritto d'autore nell'ambito di Internet"* (dr. M. Gercke, avvocato, docente di diritto dei Media all'Università di Colonia)

I problemi posti nel campo del diritto di autore dallo sviluppo di Internet sono quelli della possibile condivisione dei files ("Dateien") - cd. file sharing, e quindi della incontrollabilità della riproduzione di opere o banche dati protette (- geschützten Werke, caso Napster) tramite up e downloading files. Tali punti critici sono ingigantiti dalla possibilità per i singoli utenti di offrire direttamente ad altri i servizi di file-sharing.

Anche la legislazione tedesca (come quella italiana) ha subito nel campo molti cambiamenti a seguito di convenzioni e disposizioni internazionali e comunitarie. Le norme di tutela sono contenute nella legge sul diritto di autore (UrhG) del 1965, novellata sino al 2003, ai § 3, 4, 16 (contenuto, diritto di sfruttamento economico), 19.a (di diffusione secondo la propria intenzione), 53.a (liceità di riproduzione per scopi e uso privato da parte di una persona fisica), 106 (divieto di riproduzione e diffusione abusiva, in cui dovrebbe essere introdotta la esimente del "modesto profitto", "geringe Zahl").

Quanto alla Convenzione sul Cyber-Crime del 2001, entrata in vigore, sottoscritta ma non ancora ratificata dalla Repubblica Federale, si tratta di un testo la cui genesi trae origine da una ricerca intrapresa dal Consiglio d'Europa sin dal 1995, e siglata nel 2001 dopo la relazione di circa una ventina di bozze.

Si suddivide in una prima parte riguardante i concetti e le definizioni generali, una seconda che riguarda il diritto sostanziale e processuale, una terza riguardante la cooperazione giudiziaria internazionale, una quarta contenente le disposizioni finali.

Gli scopi sono quelli dell'armonizzazione del diritto penale sostanziale e della difesa, attraverso questo strumento, di determinati beni giuridici, nonché dello sviluppo di strumenti unitari di indagine.

Le definizioni iniziali riguardano il sistema informatico, i dati informatici, e i fornitori di servizi.

Le norme sul diritto penale sostanziale incideranno sul sistema tedesco, prevedendosi la punibilità del semplice accesso abusivo, oggi esclusa, la punibilità del danneggiamento informatico (Computersabotage) anche ai sistemi privati, l'estensione del divieto di abuso di dispositivi o di produzione e diffusione di programmi virus al di fuori dell'ambito specialistico dei fornitori di servizi o del diritto di autore; per la pornografia minorile viene allargato l'ambito del materiale vietato e innalzata l'età dei soggetti tutelati rispetto al § 184.b StGB (che prevede ora solo i materiali "scritti" e i soggetti infraquattordicenni).

Dal punto di vista processuale, vengono allargati e potenziati gli specifici strumenti di indagine utilizzabili (art. 16 e ss.), fra cui la possibilità d'impedire la cancellazione e ordinare la conservazione di dati su ordine dell'autorità, per impedire la volatilità degli stessi, oggi solo con difficoltà ricavabile dalle disposizioni del StPO; gli art. 20 e 21 obbligano gli Stati aderenti a rendere possibile nel diritto interno la raccolta, l'intercettazione e l'ostensibilità dei dati in tempo reale a fini di indagine.

Tutte le disposizioni della convenzione andranno coordinate con la decisione quadro 24.2.2005 della U.E. sugli attacchi contro i sistemi di informazione (2005/222/KAT), che prevede, oltre a una conforme parte definitoria e di diritto penale sostanziale relativa all'accesso illecito e alla interferenza illecita in sistemi o dati, anche la responsabilità delle persone giuridiche per tali fattispecie, già prevista dall'ordinamento tedesco sotto forma di confisca (Einziehung) e prelievo del vantaggio (Verfall), oltreché con sanzioni pecuniarie (Geldbuße) dai §§ 30 e 130 OWiG, ma che diventa anche in forza della decisione quadro, potenzialmente suscettibile di "allargamento" al diritto penale vero e proprio.

CONCLUSIONI

Le problematiche affrontate hanno continui punti di contatto con quelle presenti nell'ordinamento italiano, in evidente connessione con la particolare natura tecnica e "globale" delle questioni, la ubiquità dei fenomeni riscontrati, la caduta delle barriere spaziotemporali, la possibilità di anonimato ("to pretend to be some else"), la necessità di adattamento dei tradizionali concetti giuridici, la tecnica novellistica, stratificata e spesso frammentaria delle legislazioni con la relativa molteplicità delle fonti, l'essenzialità di coordinamento non solo interno, e anche in tempo reale, se è vero, come ha rilevato l'ultimo relatore, che il 90% dei casi di criminalità in Internet sono internazionali.