Cominciamo con le presentazioni...

- Vicepresidente

- Auditor Iso 27001:2013
- Auditor Iso 20000:2011

Avv. Emiliano Vitelli
Civilista e Penalista

Il codice penale

La sistemazione dei reati secondo il bene interesse tutelato

Titolo I - Dei delitti contro la personalità dello Stato (artt. 241-313)
Titolo II - Dei delitti contro la Pubblica amministrazione (artt. 314-360)
Titolo III - Dei delitti contro l'amministrazione della giustizia (artt. 361-401)
Titolo V - Dei delitti contro l'ordine pubblico (artt. 414-421)
Titolo VII - Dei delitti contro la fede pubblica (artt. 453-498)
Titolo VIII - Dei delitti contro l'economia pubblica (artt. 499-518)
Titolo XI - Dei delitti contro la famiglia (artt. 556-574bis)
Titolo XII - Dei delitti contro la persona (artt. 575-623bis)
Titolo XIII - Dei delitti contro il patrimonio (artt. 624-649

I reati monoffensivi e plurioffensivi.

I reati informatici «tipici» (1)

- Esercizio arbitrario delle proprie ragioni con violenza su un bene informatico (III comma, art. 392 c.p.)
- Falsità in documenti informatici (art.491 bis c.p.)
- Accesso abusivo ad un sistema informatico e telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

I reati informatici «tipici» (2)

- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Frode informatica (art. 640-ter c.p.)
- Danneggiamento di sistemi informatici e telematici (art. 635-bis c.p.)
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-sexies c.p.)

Dove sono i reati informatici? (1)

- Il legislatore ha ritenuto di non varare un corpus unitario di (nuove) norme repressive, ma ha scelto di prevedere le "nuove condotte criminali distribuendole negli habitat normativi che sono sembrati —di volta in volta— più opportuni.
- L'idea di base è stata appunto che non vi erano nuovi bene interessi da tutelare.
- Ma, si dee aggiungere, è stata una scelta obbligata perché si è reso conto che non ce l'avrebbe fatta a stare al passo con i tempi.

Dove sono i reati informatici? (2)

La creazione di nuove figure criminose (da parte della legislazione nazionale, ma ormai soprattutto, se non esclusivamente, da quella europea) non deve ingannare: sono nuove le condotte (determinate dal medium), non i beni aggrediti, protetti.

La definizione di reati informatici

In realtà non esiste una definizione precisa. Tanto che la giurisprudenza si è dedicata soprattutto alla definizione di sistema informatico.

La Suprema Corte di Cassazione, Sez. VI penale, ed in particolare alla sentenza 4 ottobre 1999, n. 3067, ha definito un sistema informatico come tutte quelle "apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche in parte) di tecnologie informatiche".

Ancora sulla definizione di reati informatici

- Normalmente si distingue tra:
  - Computer crimes in senso stretto
  - Computer crimes in senso lato

I reati informatici in senso lato

- Tutte quelle fattispecie di reato "comune" che, per le particolari modalità con cui viene posto in essere si presta ad implicazioni di carattere informatico, ma in maniera del tutto accidentale e assolutamente non caratterizzante.
- Esempio sono:

  - diffamazione e stalking on line, truffe via web, pedopornografia on line, estorsione, associazione a delinquere e…

Che cosa succede in Italia?

Nel 2014 è prevista una forte ascesa dei crimini informatici rispetto al 2012.

Le tecniche preferite dai cyber-criminali includono:

- attacchi DDoS;
- cracking di account;
- Advanced Persistent Threat (APT)

Che cosa succede in Italia?

Sustima che la maggior parte delle minacce informatiche che viaggiano in Rete siano dovute a malware (81 per cento).

Per quanto riguarda le vittime, invece, il settore governativo è un bersaglio sempre più popolare (+7,5 per cento nel 2013) e **un vero e proprio boom di attacchi verso gli istituti bancari (+83 per cento) che passano dal 5 al 9 per cento del totale**.

Il reato di sostituzione di persona art. 494 codice penale

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino a un anno.

Art. 640-ter.
Frode informatica.

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

Art. 640-ter.
Frode informatica.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante

La questione

- C'è evidentemente un problema di coordinazione normativa e di relazione tra il dato normativo e la fattispecie concreta
- Si vede chiaramente comparando le previsioni del codice
- Qual è, nel furto di identità il bene interesse tutelato?

Il furto di identità ed il reato di sostituzione di persona

- Ma siamo sicuri?
- Ma il furto di identità è un reato?
- E' il giusto approccio interpretativo?

O forse sarebbe meglio cominciare a parlare di identity theft related crimes

I reati informatici collegati con quello di sostituzione di persona

- Accesso abusivo ad un sistema informatico o telematico 615 ter c.p.
- Detenzione abusiva di codici di accesso a sistemi informatici o telematici 615 quater c.p.
- Violazione di domicilio 614 c.p.
- Frode informatica 640 ter
- …ma ricordiamoci anche Associazione a delinquere 416 c.p.; c.p. Truffa 640 c.p.;

Cos'è allora il furto di identità? (1)

La sostituzione di persona è diventato il grimaldello per perpetrare ben altri e più gravi reati.

- Nonostante l'ultimo intervento del Legislatore in realtà l'attuale quadro normativo continua ad essere inadeguato;

- Si pongo vari problemi giuridici primo fra tutti quello di come e se applicare le ipotesi di concorso tra reati.

Una possibile definizione normativa

L'art. 30 bis del dlgs 64/2011 definisce il furto di identità distinguendo tra impersonificazione totale e parziale.

Occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto anche deceduto (p.e. carta di identità inalterata di altra persona, oppure in ambito digitale l'utilizzo di user id e password sottratte ad altro utente)

La giurisprudenza. Un caso pratico (1)

La sentenza della quinta sezione penale della Corte di Cassazione del 29 aprile 2013, n. 18826

L'imputata era accusata di aver partecipato a una chat erotica utilizzando un nome di fantasia, ma in qualche modo riconducibile alla sua datrice di lavoro e fornendo il cellulare della donna. Quest'ultima riceveva numerose comunicazioni offensive e moleste da parte di altri utenti della chat evidentemente tratti in errore sulla disponibilità delle vittima.

La giurisprudenza Un caso pratico (2)

Come a deciso la Corte di Cassazione?

L'inserimento, in una chat di incontri personali, del numero di telefono cellulare di un'altra persona, ignara, in associazione a uno pseudonimo (il telematico "nickname") al fine di danneggiare la stessa persona facendola apparire sessualmente disponibile, integra il reato di sostituzione di persona di cui all'articolo 494 del c.p., nella modalità dell'attribuzione di un falso nome.

La giurisprudenza Un caso pratico (3)

Il bene interesse tutelato dalla norma incriminatrice è la sfera privata o la fede pubblica?

La Suprema Corte con un esplicita *excusatio non petita* ha ammesso di aver dovuto operare una interpretazione estensiva e considerare il 494 c.p. come un reato plurioffensivo.

Come analizzare il fenomeno del furto di identità?

È vero, c'è un forte problema di ignoranza dell'utente nel dribblare tutte le insidie che nell'arco anche di una sola giornata può incorrere distribuendo i dati sulla propria identità a destra ed a sinistra.

Ma il problema che non viene mai affrontato è quale reazione i soggetti che operativamente hanno gli strumenti per mitigare il rischio dei furti di identità possono mettere in essere proprio per diminuire al minimo i furti di identità

Come reagire

- E' imprescindibile:

  - capire cosa e come è stato realmente fatto;

  - operare nel modo più rapido possibile.

- E quindi per esempio:

  - richiesta di sequestro (conti correnti, beni acquistati in leasing, ecc.);

  - richiesta di accesso alle informazioni e/o ai dati di traffico;

  - richiesta di accesso alla documentazione bancaria;

  - attività di computer forensics (anche sui propri device e computer, ecc.)

Quali strumenti utilizzare?

Le investigazioni difensive:

- gli artt. 391 bis c.p.p. e segg.

- l'art 132 del Dlgs 196/2003

Nozioni di procedura

- Le indagini preliminari. Come funzionano?
- Perché è importante conoscerne i meccanismi: è necessario supportare il difensore nella sua attività di indagine.
- Il p.m. è il dominus di questa fase del procedimento penale ma…

….ma deve avere le esatte competenze oppure avere, a suo supporto, degli specialisti del mestiere.

- Per il difensore, e soprattutto per quello della persona offesa, le cose sono ben diverse.

Nozioni di investigazioni difensive (1)

TIPOLOGIA DELLE ATTIVITÀ CONSENTITE PER RICERCARE ED INDIVIDUARE ELEMENTI DI PROVA A FAVORE DELLA PERSONA ASSISTITA
Colloquio non documentato con la persona in grado di riferire circostanze utili ai fini dell'attività investigativa
Ricezione di dichiarazione scritta dalla persona in grado di riferire circostanze utili ai fini dell'attività investigativa
Assunzione di informazioni dalla persona in grado di riferire circostanze utili ai fini dell'attività
Richiesta di documentazione alla pubblica amministrazione
Accesso ai luoghi pubblici o aperti al pubblico per prenderne visione, per procedere alla loro descrizione o per eseguire rilievi
Accesso ai luoghi privati o non aperti al pubblico per prenderne visione, per procedere alla loro descrizione o per eseguire rilievi
Esame delle cose sequestrate
Intervento del consulente tecnico alle ispezioni ed esame delle cose sequestrate od oggetto delle ispezioni

Nozioni di investigazioni difensive (2)

- L'attività difensiva del difensore può essere svolta in ogni stato e grado del procedimento (e anche prima…)

- La persona sottoposta all'interrogatorio ha **il diritto di avvalersi della facoltà di non rispondere o di non rendere la dichiarazione**; in tal caso il difensore può chiedere al giudice che si proceda con incidente probatorio all'assunzione della testimonianza o all'esame della persona o chiedere al pubblico ministero di procedere all'audizione della persona

- **Se non vi è il consenso della persona che ha la disponibilità del luogo**, l'accesso è consentito solo se autorizzato dal giudice. Nei luoghi di abitazione e loro pertinenze l'accesso è consentito solo se sia necessario per accertare le tracce e gli altri effetti materiali del reato.

- **L'intervento del consulente tecnico** deve essere autorizzato dal giudice o, nella fase delle indagini preliminari, dal pubblico ministero.

Dlgs 196/2003 (1)

- **Art. 7 (Diritto di accesso ai dati personali)**

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

- **Art. 8 (Esercizio dei diritti)**

I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati

[…]

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive

Dlgs 196/2003 (2)

- **Art. 24 Casi nei quali può essere effettuato il trattamento senza consenso**

  1. **Il consenso non è richiesto**, oltre che nei casi previsti nella Parte II, **quando il trattamento**:

  […]

  f) con esclusione della diffusione, **è necessario ai fini dello svolgimento delle investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

  […]

Dlgs 196/2003 (3)

- **Art. 132 Conservazione di dati di traffico per altre finalità**

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al **traffico telefonico**, sono conservati dal fornitore per **ventiquattro mesi** dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al **traffico telematico**, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per **dodici mesi** dalla data della comunicazione.

Dlgs 196/2003 (4)

Come si acquisiscono i dati di traffico? Chi può acquisirli?

…e la persona offesa?

- Qui entra in gioco l'abilità del difensore e l'ausilio dei tecnici di cui si avvale.
- L'avvocato non può e non deve fare tutto da solo. Le indicazioni che gli devono essere fornite dagli specialisti sono essenziali per una efficacie impostazione della linea difensiva.
- Sotto questo profilo risulterà essenziale anche la collaborazione con il pubblico ministero.

Un caso pratico di furto di identità (1)

- Un giorno il Sig. Tizio non riesce ad accedere al suo conto corrente on line. La password non funziona.
- Chiama la banca e dopo una serie si operazioni riesce ad entrare nel conto.

Il Sig. Tizio scopre che tutti i suoi risparmi non ci sono più.
Il conto è stato svuotato per mezzo di bonifici eseguiti in favore di un conto sempre a nome del Sig. Tizio, presso un altro istituto bancario, ma che lui non ha mai aperto

Un caso pratico di furto di identità (2)

L'operazione criminale

- Clonazione della carta di identità della vittima
- Sottrazione delle credenziali di accesso al conto corrente on-line
- Falsa ~~denuncia~~/dichiarazione di smarrimento della SIM il cui numero è collegato al conto
- Apertura di un conto corrente presso una nuova banca
- Sostituzione dei conti correnti con cui dialoga quello del Sig. Tizio immettendo quello appena acceso
- Spostamento del denaro dal primo al secondo conto e da quest'ultimo ad altri.

Un caso pratico di furto di identità (2)

- Cosa si può fare per tutelare la persona offesa?
- Quale il ruolo dell'avvocato?
- Quale il ruolo del tecnico?

La qualificazione del fatto-reato

- Frode informatica ex art. 640 ter c.p.
- Sostituzione di persona ex art. 494 c.p.
- Associazione a delinquere ……
- Concorso di reati o più reati distinti?
- Continuazione ex art. 81 c.p.?
- Un solo reato che contiene anche l'altro?

La redazione della querela

- **Non si deve tralasciare nulla**
- L'avvocato meno esperto in questa materia deve necessariamente farsi aiutare da un tecnico.
- Anche l'indicazione del o delle url, il sistema operativo utilizzato dall'utente, la rete telematica cui è allacciato (compreso il proprio ip), i programmi utilizzati soprattutto quelli relativi alla sicurezza, se utilizza un fisso o un mobile, se utilizza device anche per accedere al proprio conto.
- Tutte le eventuali anomalie o difformità che la persona offesa potrebbe avere riscontrato quando è acceduto al sito web
- Ovviamente anche tutte le informazioni relative al conto.
- Per far ciò sono necessari più di un incontro con la persona offesa.

Le indagini difensive (1)

- mentre il pubblico ministero fa il suo lavoro….
- …anche il difensore coadiuvato dal tecnico può dire la sua e fare la sua parte.
- Occorre innanzitutto individuare i soggetti coinvolti, anche a loro insaputa (ed a prescindere dalle loro responsabilità):
- I due istituti bancari
- Il gestore della rete telematica
- Il gestore della rete telefonica
- Altri soggetti terzi comunque coinvolti (altri furti di identità)

Le indagini difensive (2)

- Consideriamo che in questa fase teoricamente l'imputato potrebbe non sapere nulla delle indagini a meno che, una volta individuato (sempre se ci si riesce), il pubblico ministero compia uno dei c.d. atti garantiti.

- D'altra parte invece la persona offesa essendo stato quello che ha attivato la macchina giudiziaria sa bene quello che sta accadendo.

Le indagini difensive (3)

- Il difensore, codice alla mano, può tentare di richiedere ai soggetti coinvolti nella vicenda tutta una serie di informazioni.

Otterrà qualcosa?

Normalmente no…, soprattutto se chi deve rispondere sono le banche.

Le indagini difensive (4)

Oppure…

- Si può andare direttamente dal pubblico ministero. Qui li problema è duplice:

  1) si bypassa il dato normativo, saltando un passaggio;

Ma soprattutto…

  2) ci si deve trovare di fronte un pubblico ministero collaborativo

- La richiesta va sempre costantemente ed attentamente motivata e giustificata dalle esigenze difensive (civilistiche) e circoscritta temporalmente

Le indagini difensive (5)

Cosa è possibile chiedere?

Diamo spazio alla fantasia….

- Richiesta di accesso ai dati di traffico telematico degli istituti bancari coinvolti
- Ricevuta la risposta dovremmo essere a conoscenza quando mento del gestore telematico
- Quindi si può chiedere l'autorizzazione ad acquisire i dati di traffico relativi agli Ip pubblici.
- In particolare l'elenco di tutti i CGI e gli intestatari IMSI riconducibili a tali dati
- In tal modo si potrebbe riuscire a determinare il luogo di provenienza degli accessi

Le indagini difensive (6)

- Contattare il gestore telefonico per chiedere tutte i dati riferibili al titolare della sim.
- Nel nostro caso abbiamo riscontrato che era stata attivata una nuova sim che tuttavia la persona offesa non riconosceva come propria.
- Dal gestore si deve cercare di ottenere tutta la documentazione relativa alle anomalie riscontrate e, anche qui, delle due l'una:

  1) o il gestore collabora;

  2) oppure si deve tentare di passare per l'autorizzazione del pubblico ministero

La relazione tecnica

Come redigerla?

Il punto di partenza: i dati raccolti durante le investigazioni.

Questi però devono essere supportati da un percorso argomentativo forte.

Ciò significa che tutto ciò che si sostiene nella relazione deve avere seri e noti riscontri scientifici (tecnici e normativi).

La relazione tecnica

La relazione tecnica redatta in favore di una persona (imputato, indagato o parte offesa/civile che sia) è un elaborato **necessariamente e volutamente** parziale.

L'abilità del consulente tecnico sarà nell'evidenziare i pro e minimizzare i contro.

Grazie!