CORSO DI AGGIORNAMENTO FORENSE 2019

PATRONATO PIO X - Sala "Emmaus"

Via Borgo Treviso n. 74 - Cittadella (PD)

Data: **VENERDI' 24 MAGGIO 2019 dalle ore 14.30 alle ore 18.30**

Area disciplinare: DIRITTO PENALE – DIRITTO DELL'INFORMATICA

Titolo: **CYBERBULLISMO E REATI "DIGITALI" - ASPETTI GIURIDICI, PSICOLOGICI E TECNICI**

FENOMENO DELLA DATAFICATION («Big data»; «datalizzazione»)

- Mayer-Schönberger e Cukier (2013);
- trasformazione in dati elaborabili di tutto ciò che facciamo, pensiamo, preferiamo o detestiamo e di tutte le relazioni che intratteniamo con privati e con istituzioni e compagnie
- - e-commerce;
- - e-government;
- - house banking;
- - trading on-line;

ALFABETIZZAZIONE DELL'UTENZA

DATA RETENTION: - indirizzo IP
- file log
- conservazione dei dati

Cyberspazio

- luogo di interazione tra uomo e macchina all'interno del quale vengono in rilievo «flussi di informazioni digitali, che, spostandosi attraverso reti tra loro collegate, **sfuggono alla ordinaria qualificazione delle cose** e a una netta distinzione tra una dimensione soggettiva e una dimensione oggettiva»

Hacker/cracker

- **Hacker** è colui che tramite il proprio personal computer trova collegamenti o cerca accessi non autorizzati a informazioni o banche dati: «si tratta in genere di soggetti caratterizzati da un elevato tasso di conoscenze tecniche e che talvolta sono animati da motivazioni di carattere politico o ideologiche

- Cracker: dopo l'accesso carpisce o distrugge informazioni e dati.

Entrambi sono punibili secondo la legge italiana

Identità Digitale

- *il legislatore, con d.l. n. 93/2013 (convertito dalla l. n. 119/2013 su c.d. violenza di genere) ha introdotto, per la prima volta, nel codice penale, il concetto di "identità digitale" (comma 3 dell'art. 640-ter)*

- *"rappresentazione informatica della corrispondenza biunivoca tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale".*

(c.d. Decreto SPID - Decreto Pres. CdM 24 ottobre 2014, art. 1, lett. o)

https://www.gazzettaufficiale.it/eli/id/2014/12/09/14A09376/sg)

Art. 15 Costituzione

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili

Art. 21 Costituzione

Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di comunicazione

Art. 8 Cedu

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

Interventi normativi

- Legge n. 191/1978 (introduzione art. 420 c.p. – «*attentato a impianti di elaborazione dati*», sostituito da L. 547/1993)
- Legge n. 121/1981 (prima forma di tutela di dati archiviati in sistema informatico)
- Legge n. 197/1991 (art. 12: utilizzo indebito di carte di credito);
- Legge n. 518/1992 (art. 10: «pirateria informatica»)

L.23 dicembre 1993, n. 547

- *- «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica».*

- - Repressione dei c.d.

COMPUTER CRIMES

Definizione di «reati informatici»

- Vengono definiti reati informatici tutti quei crimini commessi grazie all'utilizzo di tecnologie informatiche o telematiche. In Italia, sono disciplinati dalla legge 547 del 1993 che ha integrato le norme del codice penale e del codice di procedura penale relative alla criminalità informatica

1) REATI INFORMATICI

- – la **frode informatica**, prevista dall'articolo 640 ter del codice penale che consiste nell'alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto;
- – l'**accesso abusivo ad un sistema informatico o telematico** (615 ter del codice penale);
- – la **detenzione e diffusione abusiva di codici di accesso** a sistemi informatici e telematici (615 quater del codice penale);
- – la **diffusione** di apparecchiature, dispositivi o programmi informatici diretti a **danneggiare o interrompere** un sistema informatico o telematico (615 quinquies del codice penale).

Titolo XIII, Capo I- Dei delitti contro il patrimonio mediante violenza alle cose o alle persone

2) Crimini diretti contro il **computer** (c.d.: crimini informatici **PROPRI**)

- SABOTAGGIO: art. 635bis c.p.
- VANDALISMO: art. 635 ter c.p.
- DANNEGGIAMENTO INFORMATICO: art. 635 quater c.p.
- ATTENTATO a PUBBLICA UTILITA': art. 635 quinquies c.p.

3) Crimini correlati all'**uso** del computer (c.d.: crimini informatici **IMPROPRI**)

- I reati informatici impropri sembrerebbero in aumento pertanto lo studio della fenomenologia ha consentito di elaborare una vera e propria diversificazione di casistiche.
- coincide invece con un complesso eterogeneo di reati comuni, previsti da codice penale, da leggi speciali e, pure, dalla legge citata.
- In pratica i reati informatici propri sono quelli commessi su Internet, mentre i reati informatici impropri sono quelli commessi tramite Internet.

Competenza territoriale reati informatici

- **Sezioni Unite della Corte di Cassazione** (Sent. 26 marzo 2015, n. 17325): **il luogo di consumazione è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente**, e non già il luogo nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente. La regola della competenza radicata nel luogo dove si trova **il client** non trova eccezioni per le forme aggravate del reato di introduzione abusiva ad un sistema informatico.
- Invece, nelle ipotesi meramente residuali in cui non risulta rintracciabile la piattaforma su cui ha operato il client, trovano applicazione i criteri tracciati dall'**articolo 9 c.p.p. (regole supplettive)**

Titolo XIII, Capo II - Dei delitti contro il patrimonio mediante frode

1)Crimini con finalità di **profitto**

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*

Titolo XIII, Capo II - Dei delitti contro il patrimonio mediante frode

1)Crimini con finalità di **profitto**

Art. 640 ter: frode informatica

- Trarre in inganno un elaboratore elettronico;
- Fine di profitto;
- Danno

- Da 1 a 5 anni
- Da 2 a 6 anni se furto/indebito utilizzo identità digitale

1)Crimini con finalità di **profitto**
Art. 640 ter: frode informatica

A) c.d. phishing (bonifico/ricarica disconosciuta)

l'illecita acquisizione di codici di accesso a conti correnti bancari e postali ed il loro successivo utilizzo per effettuare prelievi e bonifici on line non autorizzati **(c.d. phishing)** è inquadrabile ai sensi degli artt. 640-*ter*, 615-*quater* e 615-*quinquies* (*Trib. Milano 28 luglio 2006*, in *Dir. Internet*, 2007, 1, 62 nota di **VACIAGO,GIORDANO**)

1)Crimini con finalità di **profitto**
Art. 640 ter: frode informatica

A) c.d. phishing (bonifico/ricarica disconosciuta)

«Acquisizione per scopi illegali di dati personali di clienti di banche e organizzazioni finanziarie attraverso una finestra apribile da una e-mail»

- Invio di mail simile a quella che sarebbe inviata da istituto/provider;
- Indicazione di problemi tecnici che invitano a cliccare sul ink per aggiornare i dati personali;
- Il link porta ad un sito falso che capterà i dati personali dell'utente.

1)Crimini con finalità di **profitto**
Art. 640 ter: frode informatica

A) c.d. phishing (bonifico/ricarica disconosciuta)

ABI (Associazione Bancaria Italiana)

Come proteggersi dal phishing – Decalogo per i clienti

https://www.abi.it/DOC_Mercati/Analisi/Innovazione-ricerca/Innovazione--Ricerca/tmp1120233228212_2Phishing.pdf

1)Crimini con finalità di **profitto**
Art. 640 ter: frode informatica

A) c.d. phishing (bonifico/ricarica disconosciuta)

- Cassazione Civile: è **responsabilità dell'istituto bancario** dimostrare di avere adottato tutte le misure idonee a garantire la sicurezza del servizio telematico a disposizione del cliente

"***anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (cioè che rappresenta interesse degli stessi operatori), appare del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore di servizi di pagamento**, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici da parte di terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo*".

Corte di Cassazione - Sezione Prima Civile, Sentenza 3 febbraio 2017, n. 2950

1)Crimini con finalità di **profitto**

Frode informatica (art. 640ter c.p.).

B) Sistema della «doppia scheda»

Integra il reato di frode informatica, previsto dall'art. 640-*ter* c.p., l'introduzione, in apparecchi elettronici per il gioco di intrattenimento senza vincite, di una seconda scheda, attivabile a distanza, che li abilita all'esercizio del gioco d'azzardo (cosiddette «slot machine»), trattandosi della attivazione di un diverso programma con alterazione del funzionamento di un sistema informatico (*Cass. V, n. 27135/2010*).

Il principio e' stato recentemente ribadito negli stessi termini (*Cass. II, n. 54715/2016*).

1)Crimini con finalità di **profitto**
Frode informatica (art. 640ter c.p.).
C) Utilizzo del Dialer

- Numerazioni a valore aggiunto;
- L'utente navigando da rete fissa, scarica programmi autoistallanti che **disconnettono** il modem e lo **ricollegano** a **numeri a valore aggiunto** (899) e codici satellitari ed internazionali (00), comportando costi molto elevati per la chiamata (fonte: *Pool reati informatici della Procura di Milano*)
- Prevenzione:
  - disabilitazione chiamate a numeri speciali/internazionali;
  - installazione di software («stop dialer»);
  - linea telefonica a fibra.

1)Crimini con finalità di **profitto**

Frode informatica (art. 640ter c.p.)

vs

art. 55, comma 9, D. Lgs. n. 231/2007

Utilizzo di carte di credito clonate nel circuito informatico bancario

- Integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, **penetri abusivamente** nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua (*Cass. II, n. 41777/2015*). Il caso concreto riguardava un soggetto che, introdottosi nel sistema informatico di una società di gestione dei servizi finanziari, utilizzava senza diritto i dati relativi a carte di credito appartenenti a cittadini stranieri ed **effettuava**, così, **transazioni commerciali**, conseguendo un ingiusto profitto.
- integra il reato di **indebita utilizzazione di carte di credito** di cui all ' art. 55, comma 9, d.lgs. 21 novembre 2007 n. 231 e non quello di frode informatica di cui all ' art. 640-*ter*, il reiterato prelievo di denaro contante presso lo sportello bancomat di un istituto bancario mediante utilizzazione di un **supporto magnetico clonato**, in quanto il ripetuto ritiro di somme per mezzo di una **carta bancomat illecitamente duplicata** configura l ' utilizzo indebito di uno strumento di prelievo sanzionato dal predetto art. 55 (*Cass. VI, n. 1333/2015*).

1)Crimini con finalità di **profitto**

Frode informatica (art. 640ter c.p.)

Intervento senza diritto su dati e informazioni contenuti in un sistema informatico

Integra il reato di frode informatica, nelle forme dell'intervento senza diritto su dati e informazioni contenuti in un sistema informatico, oltre che quello di accesso abusivo ad un sistema informatico, la condotta del **dipendente dell'Agenzia delle Entrate** che, utilizzando la «password» in dotazione, manomette la posizione di un contribuente, effettuando sgravi non dovuti e non giustificati dalle evidenze in possesso dell'ufficio (*Cass. II, n. 13475/2013*).

Titolo XIII, Capo I- Dei delitti contro il patrimonio mediante violenza alle cose o alle persone

2) Crimini diretti contro il **computer** (c.d.: crimini informatici **PROPRI**)

- SABOTAGGIO: art. 635bis c.p.
- VANDALISMO: art. 635 ter c.p.
- DANNEGGIAMENTO INFORMATICO: art. 635 quater c.p.
- ATTENTATO a PUBBLICA UTILITA': art. 635 quinquies c.p.

2) Crimini diretti contro il **computer** (c.d.: crimini informatici **PROPRI**)

SABOTAGGIO: art. 635bis c.p.

Danneggiamento di informazioni, dati e programmi informatici

- Modificato con L. n. 48/2008 di ratifica della Convenzione di Budapest del 23 novembre 2001 («Convenzione del Consiglio di Europa sulla Criminalità Informatica»);
- Tutela integrità del patrimonio informatico;
- Dati *immagazzinati* e dati *in transito*;
- **CANCELLAZIONE**: in via provvisoria/definitiva
- **Backup: *E' quella cosa a cui nessuno pensa prima che sia troppo tardi***

2) Crimini diretti contro il **computer**
(c.d.: crimini informatici **PROPRI**)
SABOTAGGIO: art. 635bis c.p.

Recuperabilità dei dati informatici danneggiati o cancellati

- Caso di file cancellati dopo lo svuotamento del c.d. «cestino» -

*«è integrato anche quando la manomissione ed alterazione dello stato di un computer siano **rimediabili** soltanto attraverso un intervento recuperatorio postumo comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro. Nel caso concreto si era trattato della cancellazione, mediante l'apposito comando e dunque senza determinare la definitiva rimozione dei dati, di un rilevante numero di file, che poi erano stati recuperati grazie all'intervento di un tecnico informatico specializzato (Cass. V, n. 8555/2011).*

2) Crimini diretti contro il **computer**
(c.d.: crimini informatici **PROPRI**)

VANDALISMO: art. 635 ter c.p.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

- Delitto di attentato
- Informazioni o programmi di pubblica utilità

2) Crimini diretti contro il **computer** (c.d.: crimini informatici **PROPRI**)

DANNEGGIAMENTO INFORMATICO
art. 635 quater c.p.

Danneggiamento di sistemi informatici o telematici

- clonazione di carte di credito accompagnata dalla acquisizione, tramite videoripresa, dei codici PIN all'atto della loro digitazione, con acquisizione dei codici di accesso al sistema informatico della Banca.

2) Crimini diretti contro il **computer** (c.d.: crimini informatici **PROPRI**)

Attentato a impianti di pubblica utilità
Art. 635 quinquies c.p.

Danneggiamento di sistemi informatici o telematici di pubblica utilità

- Già in art. 420 c.p. (attentato a impianti di pubblica utilità);

3) Crimini correlati all'**uso** del computer (c.d.: crimini informatici **IMPROPRI**)

- I reati informatici impropri sembrerebbero in aumento pertanto lo studio della fenomenologia ha consentito di elaborare una vera e propria diversificazione di casistiche.
- coincide invece con un complesso eterogeneo di reati comuni, previsti da codice penale, da leggi speciali e, pure, dalla legge citata.
- In pratica i reati informatici propri sono quelli commessi su Internet, mentre i reati informatici impropri sono quelli commessi tramite Internet.

3) Crimini correlati all'uso del computer (c.d.: crimini informatici IMPROPRI) Casistica

- PEDOFILIA E PEDOPORNOGRAFIA
- FURTO DI IDENTITÀ SEMPLICE (art. 494 c.p.)
- DIFFAMAZIONE ON LINE (art. 595, comma 3 c.p.)
- VIOLAZIONE DI ACCOUNT (art. 494, 615-terc.p.)
- ACCESSO ABUSIVO A E-MAIL (art. 615-ter c.p.)
- TRUFFA E-BAY O SU ALTRE PIATTAFORME E-COMMERCE (art. 640 c.p.)
- RICICLAGGIO ELETTRONICO PROVENTI ILLECITI (CYBER LAUNDERING) (art. 648, 648bis c.p.)

Furto di identità semplice (art 494 c.p.)

- Pur non corrispondendo “materialmente” ad una **sostituzione della persona**, in mancanza di una fattispecie incriminatrice specifica, il **furto di identità in rete** viene **ricondotto dalla giurisprudenza** di legittimità **nell'ambito del reato di cui all'art. 494 c.p., relativo alla “sostituzione di persona”,** secondo il quale “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".
- sul punto, la Cassazione si è pronunciata più volte ritenendo che **la condotta di chi crea ed utilizzi account o caselle di posta elettronica** servendosi dei dati anagrafici di un terzo soggetto, *inconsapevole*, **è in grado di indurre in errore,** non il fornitore del servizio, bensì **l'intera platea di utenti**, i quali, convinti di interloquire con un soggetto, si troveranno ad interagire, invece, con una persona diversa da quella che a loro viene fatta credere, integrando così la fattispecie di reato prevista dalla norma (Cass. Pen. n. 46674/2007).
- La Cassazione ha confermato il suddetto orientamento, riconoscendo **l'applicabilità dell'art. 494 c.p.** in una fattispecie in cui è stata ravvisata la **sostituzione di persona mediante chat line.** Anche in tal caso, la condanna del soggetto agente, è stata il risultato dell'interpretazione “estensiva” che la S.C. ha riconosciuto alla norma in esame (Cass. Pen. n. 18826/2013).

Identità digitale

- il legislatore, con **d.l. n. 93/2014** (convertito dalla l. n. 119/2014) ha introdotto, per la prima volta, nel codice penale, **il concetto di "identità digitale".**
- infatti, l'art. 9 del citato decreto, rubricato:"Frode informatica commessa con sostituzione di identità digitale" ha modificato l'art. **640-ter c.p.**, con l'inserimento di un **terzo comma**, ove il legislatore ha previsto la pena della reclusione da due e sei anni e la multa da 600,00 euro a 3.000,00 euro nel caso in cui il **fatto sia commesso mediante furto o indebito utilizzo dell'identità digitale** in danno di uno o più soggetti; trattasi di un delitto per il quale è prevista la querela della persona offesa salvo che ricorra l'ipotesi di cui al 2° o 3° comma dell'art. 640-ter ovvero altra circostanza aggravante
- **Con l'istituzione del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID) le pubbliche amministrazioni potranno consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi. Il termine entro il quale la disposizione entrerà in vigore sarà stabilito con il decreto attuativo. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.**
- Il 7 ottobre 2016 è stata pubblicata la Determinazione 239/2016 che consente anche ai privati di accedere al sistema SPID in qualità di fornitori di servizi.

Cyberlaundering: riciclaggio 3.0

- I capitali ottenuti da attività criminali, come lo spaccio di sostanze stupefacenti, la prostituzione e le frodi, vengono 'ripuliti' in modo tale che nessuno possa capire da dove essi provengano; se ne impedisce, insomma, la 'tracciabilità delle origini', fino al cosiddetto '**Commingling**', cioè fino a riuscire a confondere fondi illeciti con fondi leciti.
- minaccia gravissima per la sicurezza delle transazioni monetarie telematiche se si considera il fatto che esse sono sempre più difficili da individuare in Internet, a causa della frammentazione degli scambi e della molteplicità degli itinerari percorsi dal denaro veicolato. Esistono, tuttavia, progetti, ancora in fase sperimentale, finalizzati a contrastare il fenomeno. Tra i più importanti: quello del '**CNTO**' ('Cyberpayment Network Targeting Order'), un localizzatore telematico di ordini di cyberpagamento; e il sistema '**F.A.I.S.**' ('FinCen Artificial Intelligence System'), attualmente adoperato per analizzare le transazioni monetarie sospette, entrambi progettati negli Stati Uniti ed ancora a vaglio degli esperti.
- I cybercriminali (spesso stranieri) 'adescano' gli internauti più ignari e sprovveduti con false **offerte lavorative,** pubblicate sui social network o inviate via e-mail, in cui propongono di diventare **'financial manager'** di fantomatiche società internazionali, leader in investimenti offshore; richiedendo un limitato impegno lavorativo, anche in termini di ore, e la disponibilità di un conto corrente.

Cyberlaundering: riciclaggio 3.0 prestaconto nelle operazioni di phishing

- *Di cosa risponde il soggetto che assume il ruolo di prestaconto nelle operazioni di phishing che conducono ad appropriarsi di somme di denaro delle persone offese? Si tratta di riciclaggio, ai sensi dell'art.648 bis c.p., ovvero di frode informatica nella forma del phishing, ai sensi dell'art.640 ter c.p.?*
- La Cassazione non ha dubbi: si tratta di riciclaggio, non potendosi configurare l'assorbimento di tale fattispecie criminosa nella sfera del phishing. *(Cass. 10060/2017)*.

Diffamazione on line (art 595 comma 3 c.p.)

- definizione di social network: *"un servizio di rete sociale, basato su una piattaforma software scritta in vari linguaggi di programmazione, che offre servizi di messaggistica privata ed instaura una* ***trama di relazioni*** *tra più persone all'interno dello stesso sistema*" (Corte di Cassazione, sez. V penale, sentenza n. 4873/2017).
- Corte di Cassazione (sentenza n. 50/2017), secondo cui "*la diffusione di un messaggio diffamatorio attraverso l'uso di una* ***bacheca "Facebook"*** *integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595 terzo comma del codice penale, poiché trattasi di condotta potenzialmente capace di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone; l'aggravante dell'uso di un mezzo di pubblicità, nel reato di diffamazione, trova, infatti, la sua ratio nell'idoneità del mezzo utilizzato a coinvolgere e raggiungere una* ***vasta platea di soggetti****, ampliando – e aggravando – in tal modo la capacità diffusiva del messaggio lesivo della reputazione della persona offesa, come si verifica ordinariamente attraverso le bacheche del social network, destinate per comune esperienza ad essere consultate da un* ***numero potenzialmente indeterminato di persone****, secondo la logica e la funzione propria dello strumento di comunicazione e condivisione telematica*".

ART. 491bis c.p. – Documenti informatici

- «*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*»
- La norma estende la portata oggettiva, sotto il profilo degli atti suscettibili di essere falsificati, delle fattispecie di reato di falso contemplate nel capo III "della Falsità in atti" aventi ad oggetto gli **atti pubblici**, disponendo che quando la falsità ivi previste riguardano un documento informatico pubblico avente efficacia probatoria si applicano le disposizioni del capo stesso concernenti gli atti pubblici. L'art. 491-*bis* è stato recentemente oggetto di modifica ad opera dell'art. 2 comma 1 lett. e) **d.lgs. 15 gennaio 2016, n. 7** recante «Disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'art. 2 comma 3 l. 28 aprile 2014, n. 67» che *ha eliminato il riferimento ai **documenti informatici privati** e alle disposizioni concernenti le scritture private, a seguito dell'abrogazione del reato di falso in scrittura privata di cui all'art. 485.*

ART. 491bis c.p. – Documenti informatici

- l'art. 3 l. 18 marzo 2008, n. 48 ha soppresso la seconda parte dell'art. 491 *bis* comma 1, eliminando al contempo la definizione penalistica di documento informatico e disponendo un rinvio implicito alla nozione fissata nell'ordinamento *extrapenale* e, in particolare, all'art. 1 lett. *p* d.lgs. 7 marzo 2005, n. 82, come modificato prima dal d.lgs. 4 aprile 2006, n. 159, e poi dal d.lgs. 26 agosto 2016, n.179 , ai sensi del quale il documento informatico è la «**il documento elettronico che contiene rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti**». L'attuale definizione prescinde, dunque, dall'incorporazione dei dati in un oggetto materiale, e, di conseguenza, rilevano penalmente anche i falsi che hanno ad oggetto informazioni anche non registrate su alcun supporto materiale.

ART. 491bis c.p. – Documenti informatici

- documento informatico inteso **in senso lato** (cioè al documento formato dall'elaboratore su supporto cartaceo mediante i propri organi di output: c.d. "tabulato")
- documento informatico inteso **in senso stretto**, quello cioè formato e memorizzato esclusivamente in forma digitale e, come tale, privo di quelle essenziali caratteristiche (espressione in forma scritta, contenuto intelligibile di pensiero, riconoscibilità dell'autore) che sono considerate tipiche del documento inteso in senso tradizionale (Borgogno, 2013, 605).

ART. 491bis c.p. – Documenti informatici

- Nello specifico il d.lgs. n. 82/2005, come modificato dal d.lgs. n. 179/2016, ed il Regolamento (UE) n. 910/2014, individuano **quattro categorie** di documenti informatici, aventi un diverso valore probatorio:
- 1) il documento sottoscritto con firma elettronica **non altrimenti qualificata** (art. 3 n. 10 Regolamento (UE) n. 910/2014), che, ai sensi dell'art. 21 comma 1 è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità;
- 2) il documento sottoscritto con firma elettronica **qualificata** (art. 3 n.12 Regolamento (UE) n. 910/2014);
- 3) il documento sottoscritto con firma elettronica **avanzata** (art. 3 n.11 Regolamento (UE) n. 910/2014);
- 4) il documento sottoscritto con firma elettronica **digitale** (art. 1, lett. *s* d.lgs. n. 82/2005).

ART. 491bis c.p. – Documenti informatici Casistica

- Integra il reato di falsità materiale in atto pubblico (artt. 476 e 491 *bis*):
- **a)** la falsificazione di atti contenuti nei supporti del sistema informatico di un ente pubblico anche quando gli stessi siano documentati in forma cartacea (*Cass. VI, n. 7752/2009*, in un caso di alterazione nel sistema informatico di un ospedale del contenuto di un referto medico);
- **b)** l'inserimento operato dal pubblico dipendente nell'archivio informatico dell'Albo nazionale dei costruttori di dati non corrispondenti alle **delibere** adottate dai competenti organi deliberativi del predetto Albo (*Cass. V, n. 11915/2003*);
- **c)** l'alterazione di documenti informatici pubblici relativi alla predisposizione di verbali di accertamento di violazioni delle norme del codice della strada da parte del pubblico ufficiale in qualità di addetto al servizio di inserimento dati nel sistema di verbalizzazione informatica (*Cass. V, n. 45313/2005*).

ART. 491bis c.p. – Documenti informatici Casistica

- Integra il reato di cui agli artt. 483 e *491 bis*:
- **a)** la falsificazione della richiesta del rilascio di firma digitale poiché si tratta di attività diretta alla Pubblica Amministrazione ed assimilabile alla richiesta di un certificato o autorizzazione amministrativa (*Cass. V, n. 10200/2010*);
- **b)** l'inserimento di dati relativi al superamento di **esami mai sostenuti** su un supporto informatico, che abbia funzione vicaria dell'archivio dell'Università e, pertanto, destinazione potenzialmente probatoria, quanto meno provvisoria (*Cass. V, n. 15535/2008*).

Titolo XII, Capo III, Sez IV- Dei delitti contro l'inviolabilità del domicilio

Art. 615 *ter* c.p.
accesso abusivo a sistema informatico o telematico

consiste, alternativamente, nell'introdursi abusivamente, e cioè senza il consenso del titolare dello *jus excludendi* (*rectius* Titolare/Responsabile del trattamento dei dati), in un sistema protetto, ovvero nel permanervi *invito domino* ma per finalità estranee da quelle consentite.

Vale la pena precisare che *"**non hanno rilievo**, […] per la configurazione del reato, **gli scopi e le finalità** che soggettivamente hanno motivato l'ingresso al sistema"* (Cass. S.U., 27 ottobre 2011, n. 4694).

Il reato di accesso abusivo a sistemi informatici **ed il reato di illecito trattamento dei dati**, benché quest'ultimo preveda una clausola di riserva espressa in apertura della norma, possono pacificamente concorrere (cfr. Cass. Pen. Sez. V, 05/12/2016, n. 11994).

(Titolo XII, Capo III, Sez. IV – delitti contro inviolabilità domicilio)

art. 615ter c.p.

Accesso abusivo ad un sistema informatico o telematico

Domicilio informatico

- ***Sezioni Unite della Corte di Cassazione** nella sentenza n. 17325/2015*

- il **bene giuridico tutelato**: **Raccomandazione del Consiglio di Europa del 1989** per assicurare una protezione all'ambiente informatico o telematico che contiene **dati personali** che devono rimanere riservati e conservati al riparo da ingerenze ed intrusioni altrui e rappresenta **un luogo inviolabile**, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche.
- Per questo la fattispecie è stata inserita nella Sezione IV del Capo III del Titolo XII del Libro II del codice penale, dedicata ai delitti contro la **inviolabilità del domicilio, che deve essere inteso come luogo, anche virtuale, dove l'individuo esplica liberamente la sua personalità in tutte le sue dimensioni e manifestazioni.**

Art. 615 ter c.p.

Accesso abusivo ad un sistema informatico o telematico

Pubblico ufficiale o incaricato di pubblico servizio

- **Cass. S.U., n. 41210 dell'8 settembre 2017**
- E' stata depositata la sentenza **n. 41210 dell'8 settembre 2017**, con la quale le Sezioni Unite, chiamate a stabilire se il delitto previsto dall'art. 615-*ter*, comma 2, n. 1, c.p. sia integrato anche nell'ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative, hanno affermato il seguente principio di diritto:
- *<<Integra il delitto previsto dall'art. 615-*ter*, comma 2, n. 1, c.p., la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso (nella specie, **Registro delle notizie di reato:** Re. Ge.), acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita>> (Cass. S.U., n. 41210/2017).*

Art. 615 ter c.p.

Accesso abusivo ad un sistema informatico o telematico

Dipendenti infedeli

- Nella **casistica giurisprudenziale** numerosi sono i casi in cui è stata affermata la responsabilità di **dipendenti infedeli**, che, pur se abilitati, dopo essere legittimamente entrati nel sistema informatico dell'amministrazione o della società di appartenenza, avevano:
- - effettuato interrogazioni sul sistema centrale dell'**anagrafe tributaria** sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio (*Cass. V, n. 22024/2013*);
- - manomesso la posizione di un contribuente, effettuando **sgravi non dovuti** e non giustificati dalle evidenze in possesso dell'ufficio (*Cass. II, n. 13475/ 2013*);
- - compiuto una interrogazione al **CED** — banca dati del Ministero dell'Interno — relativa ad una vettura, usando la propria «password» con l'artifizio della richiesta di un organo di Polizia in realtà inesistente, necessario per accedere a tale informazione (*Cass. V, n. 39620/2010*);
- - acquisito indebitamente notizie riservate tratte dalla banca dati del sistema telematico di informazione interforze del Ministero dell'Interno, per l'utilizzo in attività di investigazione privata (*Cass. V, n. 18006/ 2009*);
- - alterato i dati contenuti nel sistema in modo tale da fare apparire insussistente il credito tributario dell'Erario nei confronti di numerosi contribuenti (*Cass. V, n. 1727/2009*).

Art. 615 ter c.p.

Accesso abusivo ad un sistema informatico o telematico

Cancelliere del Tribunale

- Da ultimo è stato ritenuto (*Cass V n. 44403/2015*) che integra il delitto previsto dall'art. 615-*ter*, la condotta di accesso o di mantenimento nel sistema informatico da parte di un soggetto, che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. (Fattispecie in cui la Corte ha ritenuto configurarsi il reato nei confronti di un cancelliere del tribunale, che, utilizzando un codice di accesso ad efficacia limitata nel tempo, fornitogli anni addietro per la trasmigrazione di dati informatici, si era abusivamente introdotto nel sistema informatico RE.GE. in dotazione alla Procura della Repubblica, al diverso fine di visionare l'iscrizione di un procedimento penale a carico di un suo conoscente).

Art. 615 ter c.p.

Accesso abusivo ad un sistema informatico o telematico

CONCORSO CON Art. 640-ter c.p.

si tratta di reati diversi: la frode informatica postula necessariamente la **manipolazione del sistema**, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica. (*Cass. V n. 2672/2004*; *Cass. V. n. 1727/2009*)

- Caso di un **dipendente dell'Agenzia delle entrate** che, agendo in concorso con altri dipendenti nonché con commercialisti e consulenti tributari, si era **abusivamente introdotto** nel sistema informatico dell'amministrazione, inserendovi provvedimenti di sgravio fiscale illegittimi perché mai adottati, in relazione a tributi già iscritti a ruolo per la riscossione coattiva, così **alterando i dati** contenuti nel sistema in modo tale da fare apparire insussistente il credito tributario dell'Erario nei confronti di numerosi contribuenti)

(Titolo XII, Sez. IV – delitti contro inviolabilità domicilio)

Art. 615 – quater c.p.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

- **Tutela anticipata** del domicilio informatico (reato di pericolo);
- Abusiva condotta di procacciamento/riproduzione/diffusione/comunicazione/consegna di **password, carte magnetiche, chiavi**, altri mezzi di **accesso** a sistemi protetti
- Condotta che fornisca **indicazioni/istruzioni** idonee in tal senso

Art. 615 – quater c.p.
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Numero seriale di un apparecchio telefonico cellulare

- Integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici di cui all'art. 615 *quater*, la condotta di colui che si procuri abusivamente **il numero seriale di un apparecchio telefonico cellulare** appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta **clonazione**) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce **un sistema telematico protetto**, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche.
- Ne consegue che **l'acquisto** consapevole a fini di profitto di un telefono cellulare predisposto per l'accesso alla rete di telefonia mediante i codici di altro utente («clonato») configura il delitto di **ricettazione**, di cui costituisce reato presupposto quello *ex* art. 615 *quater* c.p.(*Cass. II, n. 5688/2005*; *Cass. II, n. 36288/2003*).

Art. 615 – quater c.p.
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Codici di carte di credito

Integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici e telematici (art. 615 *quater*) e non quello di ricettazione **la condotta di chi riceve i codici di carte di credito abusivamente scaricati dal sistema informatico**, ad opera di terzi e li inserisce in **carte di credito clonate** poi utilizzate per il prelievo di denaro contante attraverso il sistema bancomat (*Cass. II n. 47021/2013*).

art. 615 *quater* c.p.
vs
trattamento illecito di dati (art. 167 d. lgs. 196/2003)

Qualora, invece, si dovesse verificare una **fuga di informazioni protette**, o siano state poste in essere azioni tali da configurarne il pericolo, sempre che tali condotte siano volte all'ottenimento di un profitto (in senso ampio), si avrà nella violazione dell'**art. 167 D.Lgs. 30 giugno 2003, n. 196** (trattamento illecito dei dati).

(Titolo XII, Sez. IV – delitti contro inviolabilità domicilio)
art. 615quinquies c.p.
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

La messa a disposizione di un software pericoloso

- — In altri casi vengono punite condotte che si sostanziano nella consapevole "*messa a disposizione di terzi*" di un programma informatico pericoloso. Si pensi, a titolo esemplificativo, ai fatti che consistono nel « *mettere a disposizione* » o anche nel « *procurare ad altri* » uno specifico *software*, nel « *comunicare* » o, meglio, nel « *rendere accessibile* » ovvero nel « *cedere* » ad un numero determinato di persone un dispositivo idoneo a commettere un reato. Il soggetto agente agevola così con la sua condotta la commissione di un reato da parte di un terzo mediante quell'oggetto, lasciando a lui la scelta se utilizzarlo per scopi illeciti.
- Il « *mettere a disposizione* » o il « *diffondere* » un *malware* in rete presenta un livello di pericolosità maggiore rispetto al consegnarlo o comunicarlo ad un numero limitato di persone. Data la facilità con la quale è possibile duplicare o auto-eseguire i *software*, una volta che vengono immessi in rete potrebbero essere scaricati e utilizzati da un numero elevato ed indeterminato di persone e potrebbero difficilmente essere ritirati dal "mercato".

(Titolo XII, Sez. IV – delitti contro inviolabilità domicilio)
art. 615quinquies c.p.
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

La messa a disposizione di un software pericoloso NON è punibile se….solo tentata

Non sempre l'agente è a conoscenza del fatto che il software che mette a disposizione di altri verrà effettivamente impiegato per commettere un reato.

Si pensi, ad es., ai casi in cui un **malware** venga caricato su una pagina web **liberamente accessibile** da un numero indeterminato di utenti e dalla quale è possibile scaricarlo gratuitamente.

Qualora l'agente ceda il malware a chi lo vuole impiegare per perpetrare un reato, ma quest'ultimo per diversi motivi decida di non compiere quel reato, si sarebbe di fronte ad un tentativo di concorso, o meglio ad un tentativo di partecipazione non punibile, nel nostro ordinamento,

in forza dell'**art. 115 c.p**

art. 615quinquies c.p.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

c.d. phishing (bonifico/ricarica disconosciuta)

È stato ritenuto che l'illecita acquisizione di codici di accesso a conti correnti bancari e postali ed il loro successivo utilizzo per effettuare prelievi e bonifici on line non autorizzati **(c.d. phishing)** è inquadrabile ai sensi degli artt. 640-*ter*, 615-*quater* e 615-*quinquies* (*Trib. Milano 28 luglio 2006*, in *Dir. Internet*, 2007, 1, 62 nota di **VACIAGO**,**GIORDANO**)

art. 615quinquies c.p.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

vs

art. 6 D. Lgs. n. 373/2000

detenzione di pics-card

- **La giurisprudenza** in un primo tempo ha applicato la norma in esame anche alla detenzione o diffusione abusiva **delle *pics-cards*** ovvero di schede informatiche che consentono di vedere **programmi televisivi criptati** attraverso la decodifica di segnali trasmessi secondo modalità tecniche di carattere telematico,

- **per poi escludere** che il reato possa essere integrato dal possesso di un decodificatore di segnali satellitari e di schede per la ricezione degli stessi (c.d. *pic-card* o *smart-card*) in quanto con tali strumenti non si viola o mette in pericolo alcun domicilio informatico, protetto da misure di sicurezza, ma si utilizzano irregolarmente servizi di trasmissione o comunicazione ad accesso condizionato, contravvenendo in tal modo alle **disposizioni sul diritto d'autore** di cui all'art. 6 d.lgs. n. 373/2000, sanzionato solo in via amministrativa prima dell'entrata in vigore della l. n. 38/2003 (*Cass. V, n. 22319/200*).

(Titolo XII, Sez. V – Dei delitti contro inviolabilità dei segreti)

Art. 617-bis c.p.

Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche

Art. 617-ter c.p.

Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche

Art. 617- quater c.p.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Art. 617- quinquies c.p.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Art. 617- sexies c.p.

Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

Art. 617- quater c.p.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

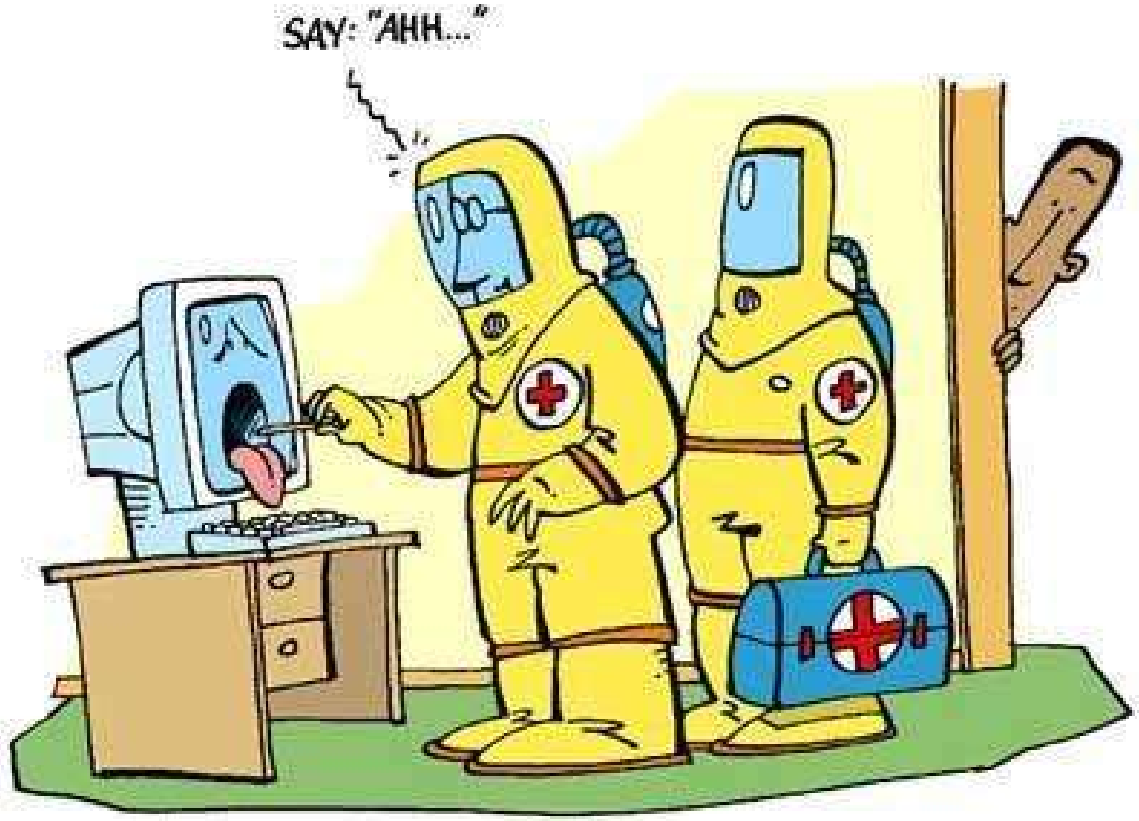
Utilizzo pos

Secondo la giurisprudenza integra il reato di cui all'art. 617 *quater* la condotta del titolare di un esercizio commerciale che utilizza, mediante un terminale **Pos** in sua dotazione, una **carta di credito contraffatta**, atteso che il titolare dell'esercizio commerciale è ben legittimato ad usare il terminale **Pos** e l'accesso abusivo genera un flusso di informazioni ai danni del titolare della carta contraffatta diretto all'addebito sul suo conto della spesa fittiziamente effettuata. In particolare nella condotta del titolare di esercizio commerciale il quale, d'intesa con il possessore di una carta di credito contraffatta, **utilizza tale documento mediante il terminale Pos** in dotazione, sono ravvisabili sia il reato di cui all'art. 615 *ter* (accesso abusivo ad un sistema informatico o telematico) sia quello di cui all'art. 617 *quater*(intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche):

- il primo perché l'uso di una chiave contraffatta rende abusivo l'accesso al Pos;
- il secondo perché, con l'uso di una carta di credito contraffatta, si genera un flusso di informazioni relativo alla posizione del vero titolare di essa diretto all'addebito sul suo conto della spesa fittiziamente effettuata, per cui vi è fraudolenta intercettazione di comunicazioni (*Cass. V, 44362/2003*).

25 MAGGIO 2018: GDPR
Regolamento Generale sulla Protezione dei Dati

- http://www.garanteprivacy.it/regolamentoue
- Con l'introduzione del nuovo Regolamento, gli avvocati **non avranno gli stessi obblighi** delle imprese e degli enti pubblici: in particolare, non sarà necessario per i legali fare la **valutazione di impatto privacy** e considerare i rischi a lungo termine e su larga scala.
- Gli avvocati saranno comunque obbligati a sottoporre **l'informativa ai clienti** e a garantire il **rispetto delle misure di sicurezza di base** necessarie per la tutela dei dati e delle informazioni personali.
- Adeguamento informativa privacy: http://www.altalex.com/documents/news/2016/10/25/informativa-privacy-e-regolamento-europeo


SAY: "AHH..."

Buona sicurezza a tutti!