# I REATI INFORMATICI

Prof.ssa Annarita Ricci
Università degli Studi G. D'Annunzio Chieti – Pescara

annarita.ricci@unich.it

# IL QUADRO NORMATIVO

- Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica ("Convention on cybercrime") del 23 novembre 2001

- La Convenzione rappresenta il primo accordo internazionale riguardante i crimini commessi attraverso Internet o altre reti informatiche

- La Convenzione ha l'obiettivo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata, che consenta di combattere il crimine informatico in maniera coordinata

# IL QUADRO NORMATIVO (2)

- Legge 18 marzo 2008, n. 48, “Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno”

# IL QUADRO NORMATIVO (3)

- Parte I dedicata alle definizioni
  - “computer system”: qualsiasi apparecchiatura, o gruppo di apparecchiature interconnesse o collegate in base ad un programma, che compie l’elaborazione automatica di dati
  - “computer data”: qualsiasi presentazione di fatti, informazioni o concetti suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione (...)

# IL QUADRO NORMATIVO (4)

– “service provider”: qualsiasi soggetto pubblico o privato che fornisce agli utenti la possibilità di comunicare attraverso un sistema informatico, nonché qualsiasi altro soggetto che processa o archivia dati informatici per conto di tale servizio di comunicazione o per gli utenti di tale servizio

- “traffic data”: qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio

# IL QUADRO NORMATIVO (5)

- Parte II dedicata ai provvedimenti da adottare a livello nazionale, con la Sezione I dedicata alle fattispecie di reato, classificate in ordine all'oggetto

- Dai reati contro la riservatezza, la disponibilità e l'integrità dei dati ai reati relativi ai contenuti, quali la pornografia infantile, ai reati dove il sistema informatico è "parte offesa" (quali la falsificazione informatica e la frode informatica) fino ai reati contro la proprietà intellettuale e diritti collegati

# IL QUADRO NORMATIVO (6)

- Diversi inoltre sono stati i provvedimenti adottati dalla Commissione europea allo scopo di fornire un’efficace risposta alle problematiche conseguenti lo sviluppo telematico ed informatico, nonché derivanti dal dilagare dei reati informatici

- Fra gli altri, Comunicazione del 2001 della Commissione al Consiglio, al Parlamento Europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, denominata “Una strategia per una società dell'informazione sicura - Dialogo, partenariato e responsabilizzazione”

# IL QUADRO NORMATIVO (7)

- Commissione Europea 22 maggio 2007, “Comunicazione verso una politica generale di lotta contro la cibercriminalità”

- La cibercriminalità è definita come l’insieme degli atti criminali commessi contro reti di comunicazioni elettroniche e sistemi di informazione o avvalendosi di tali reti e sistemi

- Individuate tre categorie di reati: forme tradizionali di reati commessi attraverso le reti elettroniche; pubblicazione sul *web* di contenuti illegali; reati propri delle reti elettroniche, quali ad esempio la pirateria

# IL QUADRO NORMATIVO (8)

- Comunicazione del 28 marzo 2012 della Commissione Europea al Consiglio e al Parlamento Europeo, denominata “Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica”, finalizzata a rafforzare l’azione di contrasto dei reati informatici, nonché ad istituire un Centro per la lotta alla criminalità informatica a tutela dei cittadini e delle imprese europee

# I REATI INFORMATICI IN ITALIA

# IL QUADRO NORMATIVO INTERNO

- Fino al 1993 l'ordinamento giuridico italiano non prevede alcuna specifica disposizione in materia di reati informatici

- Con la legge del 23 dicembre 1993 n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", vengono introdotte le prime fattispecie di reato c.d. "informatico" anche per adeguare, ai fini della cooperazione internazionale, il sistema normativo a quello di altri ordinamenti

# LEGGE N. 547/1993

- Le nuove fattispecie di reato sono inserite nel codice penale

- La scelta è stata quindi quella di non considerare i reati informatici come “aggressivi” di beni giuridici nuovi rispetto a quelli tutelati dalle norme penali già esistenti

# LEGGE N. 547/1993 (2)

- I reati sono classificati in
  - reati perpetrati per mezzo sistemi informatici
  - reati perpetrati contro sistemi informatici

# LEGGE N. 547/1993 (3)

- Le (principali) nuove fattispecie di reato contemplate dalla legge n. 547 del 1993 sono:
  - falsità in documenti informatici
  - accesso abusivo ad un sistema informatico o telematico
  - la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
  - la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
  - la violazione della corrispondenza e delle comunicazioni informatiche e telematiche
  - il danneggiamento di sistemi informatici o telematici
  - la frode informatica
  - (...)

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO

- Art. 615 *ter* del codice penale

- Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO (2)

- La pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio (...) o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO (3)

- Reato di mera condotta
- Due le condotte vietate
  - l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza
  - il permanere nel medesimo sistema contro la volontà espressa o tacita di chi ha il diritto di escludere l'intrusione

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO (4)

- Nel primo caso è punita un'azione consistente nell'introdursi ed accedere alla memoria di un elaboratore per conoscere informazioni, dati e programmi, oppure per modificarli, alterarli o cancellarli

- Per la configurazione del reato occorre la presenza di misure di sicurezza e quindi misure tecniche, informatiche, organizzative e procedurali (riferite all'elaboratore e non ai locali dove esso è collocato) destinate ad escludere ovvero ad impedire l'accesso e la conoscenza delle informazioni a soggetti estranei, non autorizzati (ad esempio, le *password*)

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO (5)

- Nel secondo caso è punito il permanere nel sistema informatico nonostante il titolare del sistema abbia manifestato in modo espresso o tacito la volontà di esclusione

- Il bene giuridico è il domicilio informatico e di qui la collocazione della fattispecie di reato all'interno della Sezione V dei Delitti contro la persona dedicata ai Delitti contro la inviolabilità del domicilio

# ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO (6)

- Cass., 6 febbraio 2007, n. 11689: “l’accesso abusivo a un sistema telematico o informatico si configura con la mera intrusione e non richiede che la condotta comporti una lesione della riservatezza degli utenti né tantomeno che l’invasione sia compiuta con l’obiettivo di violare la loro privacy”

# L’ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA

- Cass. pen., Sez. Unite, 26 marzo 2015, n. 17325: “il luogo di consumazione del delitto coincide con quello in cui si trova l’utente che, tramite elaboratore elettronico o altro dispositivo per il trattamento automatico dei dati, digitando la parola chiave o altrimenti eseguendo la procedura di autenticazione, supera le misure di sicurezza apposte dal titolare per selezionare gli accessi e per tutelare la banca-dati memorizzata all'interno del sistema centrale ovvero vi si mantiene eccedendo i limiti dell'autorizzazione ricevuta”

# L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (2)

- Cass. pen., 31 ottobre 2014, n. 10083: "nel caso di soggetto autorizzato, quel che rileva è il dato oggettivo dell'accesso e del trattenimento nel sistema informatico violando i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema o ponendo in essere operazioni di natura ontologicamente diversa da quelle di cui egli sia incaricato e per le quali sia, pertanto, consentito l'accesso, con conseguente violazione del titolo legittimante l'accesso, mentre sono irrilevanti le finalità che lo abbiano motivato o che con esso siano perseguite" (...)

# L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (3)

- In questa fattispecie la Suprema Corte ha censurato la decisione con cui il giudice di appello aveva affermato la responsabilità dell'imputato - socio e consigliere di amministrazione di una società, ed in tale qualità in possesso delle credenziali di accesso alla banca dati aziendale - per avere copiato dei file senza dimostrare la violazione delle regole poste dalla società, le quali erano intese a interdire non già la copia o la duplicazione in sé, ma la copia e la duplicazione esulanti dalle competenze dell'operatore, il quale, peraltro, nel periodo in contestazione esercitava ancora attività lavorativa per detta società

# L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (4)

- Trib. Taranto, 6 ottobre 2014, non integra il reato di accesso abusivo ad un sistema informatico o telematico la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, si introducano nella banca dati interforze degli organi di polizia, trattandosi di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi ad una agenzia investigativa (condotta questa sanzionabile per altro e diverso titolo di reato)

# L’ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (5)

- Cass. pen., 24 aprile 2013, n. 22024: “integra il reato la condotta del pubblico dipendente, impiegato della Agenzia delle entrate, che effettui interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio”

# L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (6)

- Cass. pen., 8 maggio 2012, n. 42021: "è punibile l'ex-dipendente di una S.P.A. il quale, avendo lavorato per alcuni anni come responsabile dell'ufficio del personale, con mansioni di tecnico informatico ed essendo a conoscenza degli indirizzi e-mail degli impiegati, si introduca abusivamente nel *server* di posta elettronica della società, effettuando da postazione presso la sua abitazione molteplici tentativi di violazione di accesso a caselle postali *e-mail* di membri della società, alcuni dei quali giunti a buon fine, violando più *account* dei dipendenti e trasmettendo altresì *e-mail* destinate al servizio di posta elettronica interna mediante gli account violati

# L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO IN GIURISPRUDENZA (7)

- Cass. pen., 10 dicembre 2009, n. 2987: "commette il reato il lavoratore dipendente che, pur avendo titolo per accedere al sistema informatico della propria azienda, vi si introduce con la *password* di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell'archivio informatico; né, ai fini dell'integrazione del reato, si rende necessaria la distruzione dell'archivio informatico, risultando sufficiente la mera duplicazione, comportante una permanenza non autorizzata dell'utente

# DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI

- Art. 615 *quater* del codice penale

- Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno (dolo specifico), abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164

# DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (2)

- La norma punisce chiunque si impossessi o diffonda i codici di accesso riservati (*password*, PIN) necessari per accedere ad un sistema informatico o telematico, nonché chi diffonda istruzioni tecniche su come eludere ovvero ottenere i menzionati codici di accesso

- Nella fattispecie rientrano condotte quali la clonazione degli apparecchi di telefonia mobile, l'acquisizione di codici correnti a conti bancari (...)

# DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (3)

- Trib. Trapani, 22 dicembre 2005: “La creazione e l’utilizzo di *smart card* pirata atte all’accesso ai programmi trasmessi da un sistema satellitare non integrano il reato di cui all’art. 615 *quater* del codice penale, atteso che tali condotte sono volte a procurarsi gratuitamente dei servizi e non anche a violare il c.d. domicilio informatico, alla cui protezione si rivolge la norma citata e il cui presupposto sostanziale è l'abusivo accesso ad un sistema che consenta uno scambio biunivoco di dati (in senso conforme anche Cass. pen., 16 aprile 2003, n. 22319)

# DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (4)

- Trib. L'Aquila, 10 giugno 2005: "Sono integrati i reati di accesso abusivo ad un sistema informatico e di abusiva acquisizione e detenzione dei codici di accesso nel caso in cui un soggetto si colleghi illegittimamente agli archivi di posta elettronica riservati agli studenti di una Università, trattandosi di sistema informatico di interesse pubblico"

# DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (5)

- Cass. pen., 17 gennaio 2003, n. 36288: “Rientra nelle previsioni di reato di cui all’art. 615 *quater* c.p. la condotta consistente nell’attivazione di un telefono cellulare “clonato” su numero intestato ad altro utente, essendo essa possibile solo a condizione che l’agente si sia procurato abusivamente il c.d. “seriale”, cioè il numero riservato che, abbinato con il numero di utenza, consente la connessione con la rete di telefonia mobile, la quale costituisce un sistema telematico non solo per la sua funzione di trasmissione delle comunicazioni ma anche per quella di memorizzazione e trattamento con tecnologia informatica dei dati esterni alle conversazioni”

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO

- Art. 615 *quinquies* del codice penale

- Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (2)

- La fattispecie di reato colpisce un sistema informatico generalmente attraverso un programma infetto

- *Malware* è espressione idonea a racchiudere i programmi informatici realizzati al solo fine di recare danni al computer su cui vengono “scaricati”

- All’interno della nozione sono riconducibili anche i virus informatici, tra le cui principali caratteristiche oltre alla semplicità vi è la riproducibilità

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (3)

- Altro tipo di *malware* è il *worm* che viene eseguito ogni volta che si avvia l'*hardware* e rimane attivo fino a che il computer non viene spento o il processo corrispondente non è arrestato

- Lo strumento più utilizzato per diffondere il *worm* è la posta elettronica

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (4)

- Attraverso la posta elettronica il programma ricerca indirizzi *e-mail* memorizzati nel computer ospite ed invia una copia di sé stesso alla stregua di un file allegato a tutti o parte degli indirizzi raccolti

- I messaggi che contengono i *worm* generalmente adottano tecniche di *social engineering* così da indurre destinatari ad aprire l'allegato

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (5)

- Altro tipo di *malware* è il *trojan horse*

- La denominazione si giustifica considerando che le sue funzionalità sono nascoste all'interno di un programma principale apparentemente utile

- L'installazione del programma da parte dell'utente comporta anche l'inconsapevole installazione del *trojan*

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (6)

- Gli *spyware* raccolgono informazioni sulle attività *on-line* degli utenti senza il loro consenso, per poi inviarle a soggetti che li utilizzano per scopi di lucro

- A differenza di virus e *worm* non riescono a diffondersi autonomamente, richiedendo per l'installazione l'intervento dell'utente

- È il caso dei programmi che hanno la funzione di modificare la pagina iniziale o la lista dei preferiti del *browser* o di "dirottare" su falsi siti di *e-commerce*

# DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO (7)

- Il *rootkit* è un programma creato per ottenere il controllo su un sistema senza la necessità dell' autorizzazione da parte dell'utente o dell'amministratore

- (...)

# I PROGRAMMI INFORMATICI MALIGNI IN GIURISPRUDENZA

- Trib. Bologna, 22 dicembre 2005: il reato si configura nel caso in cui l'imputato diffonda un programma informatico di sua creazione avente per effetto l'alterazione del funzionamento di sistemi informatici (c.d. virus), previa abusiva introduzione in un sistema informatico altrui

# INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

- Art. 617 *quater* del codice penale

- Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni
- La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni

# INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (2)

- Il bene giuridico tutelato è la riservatezza delle comunicazioni
- Integra la condotta di “intercettazione” la condotta di colui che utilizza apparecchiature idonee a copiare i codici alfanumerici di accesso degli utenti, mediante applicazione ai terminali automatici delle banche
- La digitazione del codice di accesso costituisce, invero, la prima comunicazione dell’utente con il sistema informatico, con la conseguenza che la copiatura di detti codici rientra nel concetto di intercettazione di comunicazioni telematiche preso in considerazione dalla citata disposizione normativa(Cass. pen., 9 novembre 2007, n. 45207)

# INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (3)

- Cass. pen., 6 luglio 2007, n. 31135: “Commette il reato il responsabile del centro elaborazione dati di una società che, pur investito della connessa posizione di amministratore di sistema, avvalendosi di mezzi atti a eludere i meccanismi di sicurezza volti a impedire l'accesso di estranei alle comunicazioni (*password*, firewall, criptazione od altri analoghi strumenti), intercetti le comunicazioni di posta elettronica indirizzate ai singoli amministratori e dipendenti”

# DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI

- Art. 635 *bis* del codice penale

- Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni

- Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni

# DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (2)

- Cass. pen., 18 novembre 2011, n. 8555: “Commette il reato di danneggiamento il dipendente che cancella un numero rilevante di dati dal computer affidatogli dal datore di lavoro per motivi lavorativi, anche se i *files* sono stati poi recuperati grazie all'intervento di un tecnico informatico specializzato”

- Sotto il profilo civilistico, l’eventuale licenziamento intimato dal datore di lavoro al lavoratore responsabile di aver cancellato tutti i documenti di lavoro dal suo computer ivi compresa la corrispondenza elettronica è qualificato “di giusta causa”

# FRODE INFORMATICA

- Art. 640 *ter* del codice penale

- 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

# FRODE INFORMATICA (2)

- Cass. pen., 13 ottobre 2015, n. 50140: “Integra il delitto di frode informatica la condotta di colui che, servendosi di un codice di accesso fraudolentemente captato, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, al fine di trarne profitto per sé o per altri”

- App. Napoli, 2 luglio 2013: “è imputabile per il reato di frode informatica chi intervenendo senza diritto su dati, informazioni o programmi contenuti nel sistema informatico o telematico dell'istituto di credito, procurava a sé l'ingiusto profitto rappresentato dall'accredito sul c/c a lui intestato, della somma di denaro di oltre 3.000,00 euro

# FRODE INFORMATICA (3)

- Il reato di frode informatica si differenzia dal reato di truffa in quanto l'attività fraudolenta dell'agente investe non la persona, ovvero il soggetto passivo, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema, fermo restando l'elemento dell'ingiusto profitto, costitutivo di entrambe le ipotesi criminose

# FRODE INFORMATICA (4)

- Cass. pen., 10 aprile 2013, n. 18909: “Integra il reato di frode informatica 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, trattandosi dell'attivazione di un diverso programma con alterazione del funzionamento di un sistema informatico”

# INFINE: I SUGGERIMENTI DI LETTURA

- Oltre ai capitoli a ciò dedicati in *Diritto dell'informatica*, Delfini – Finocchiaro, Utet, Torino, 2014

- Mangiamelli – Amato Mangiamelli, *I reati informatici: elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2015

- Piccinni – Vagiago (a cura di), *Computer crimes: casi pratici e metodologie investigative dei reati informatici*, Moretti Honegger, Bergamo, 2008

# GRAZIE DELL'ATTENZIONE

annarita.ricci@unich.it