I REATI INFORMATICI

AVV. ELISA MARINI
LOSENGO SOLIANI STUDIO LEGALE ASSOCIATO
20122 MILANO – CORSO ITALIA, 49
elisamarini@losengosoliani.com
www.losengosoliani.com

Corso di formazione tecnica e deontologica

dell'avvocato penalista

Camera Penale di Novara

12 maggio 2017

SEZIONE I
I REATI INFORMATICI
PARTE SOSTANZIALE

- Definizione di reato informatico e rilevanza internazionale del fenomeno del *cyber crime*
- Le normativa comunitaria e nazionale
- Diritto penale dell'informatica: elementi comuni
- Le principali fattispecie di reati informatici
- Giurisprudenza

I reati informatici: definizione e rilevanza del fenomeno

I **REATI INFORMATICI** (*cyber crimes*) rappresentano un fenomeno criminale caratterizzato dall'uso illecito della tecnologia informatica o telematica.

La diffusione di tale tipologia di reati ha condotto, a livello internazionale, ad una implementazione della legislazione in materia, che è stata recepita a livello nazionale con l'introduzione di nuove fattispecie di reato, o la modifica di altre fattispecie già esistenti.

Tali fattispecie sono dislocate in varie sezioni del codice penale: nell'ambito dei delitti contro la persona, nonché nel novero dei delitti contro il patrimonio, o ancora fra i delitti contro la fede pubblica.

Occorre, inoltre, distinguere i reati propriamente informatici dai reati che vengono commessi con il mezzo informatico.

Le principali fonti normative

- **Codice penale**
- **Legge 23 dicembre 1993, n°547**

  «Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.»
- **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.»
- **Legge 15 febbraio 2012, n°12**

  «Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica.»

La collocazione sistematica dei reati informatici all'interno del codice penale

- Delitti contro la persona
- Delitti contro il patrimonio
- Delitto contro la fede pubblica

Diritto penale dell'informatica: definizioni generali

Il **SISTEMA INFORMATICO** è il complesso di apparecchi organizzati per mezzo di specifici programmi al fine di acquisire ed elaborare in modo automatico le informazioni.

Il **SISTEMA TELEMATICO** è un mezzo per collegare tra loro più elaboratori tramite una rete telefonica al fine di consentire un utilizzo decentrato dei dati.

Diritto penale dell'informatica: definizioni generali

- **Reati propriamente informatici**

(es.: accesso abusivo a sistema informatico, frode informatica, danneggiamento informatico, ecc.)

- **Reati che possono essere commessi con il mezzo informatico**

(es.: diffamazione, esercizio arbitrario delle proprie ragioni con violenza sulle cose, rivelazione di segreti professionali, scientifici e industriali, reati pedopornografici, ecc.)

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

«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.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore di sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) 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.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.»

Art. 615 ter c.p. analisi del reato

La norma punisce la condotta di chi **abusivamente si introduce** in un **sistema informatico o telematico**, purché sia **protetto**, **ovvero la condotta di chi vi permane contro la volontà - espressa o tacita - di chi ha il diritto di escluderlo**.

Viene tutelato il **domicilio informatico** inteso come spazio ideale di pertinenza della persona (difatti, la fattispecie si colloca nell'ambito dei delitti contro la persona).

Il Legislatore ha inteso reprimere **qualsiasi introduzione o trattenimento in un sistema informatico che avvenga contro la volontà dell'avente diritto**, e per rendere penalmente apprezzabile tale volontà è da ritenersi sufficiente qualsiasi mezzo di protezione.

Si tratta di un delitto comune di pericolo, a dolo generico, che si consuma nel momento dell'accesso, e che prevede altresì, al secondo comma, tre circostanze aggravanti speciali.

Art. 615 ter c.p. giurisprudenza

NOZIONI DI INTRUSIONE E ACCESSO ABUSIVO

Cass. Sez. Un., 27 ottobre 2011, n°4694

«Integra il delitto previsto dall'art. 615 ter c.p. colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema.»

Art. 615 ter c.p. giurisprudenza

NOZIONI DI INTRUSIONE E ACCESSO ABUSIVO

CONTRASTO PRECEDENTE ALLE SEZIONI UNITE:

- 1° ORIENTAMENTO (respinto):

il reato non è configurabile allorché il soggetto che abbia titolo per accedere al sistema se ne avvalga per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente ravvisabili, ove tali finalità vengano poi effettivamente realizzate (*ex multis*, Cass. V, 8 ottobre 2008, n°39290; Cass. V, 20 dicembre 2007, n°2534);

- 2° ORIENTAMENTO (accolto):

perché il reato sia configurabile, basta la semplice condotta del soggetto che, pur abilitato ad accedere al sistema informatico o telematico, vi si introduca con la *password* di servizio per raccogliere dati protetti per fini estranei alle ragioni di istituto e agli scopi insiti nella protezione dell'archivio informatico, utilizzando il sistema per obiettivi diversi da quelli consentiti, poiché ad essere punita non è solo l'abusiva introduzione, ma anche l'abusiva permanenza (*ex multis*, Cass. V, 10 dicembre 2009, n°2987; Cass. V, 16 febbraio 2010, n°19463).

Art. 615 ter c.p. giurisprudenza

NOZIONI DI INTRUSIONE E ACCESSO ABUSIVO

Revirement della giurisprudenza

- Cass. V, 19 aprile 2016, n°35127
- Cass. V, 9 febbraio 2016, n°27883

QUESTIONE NUOVAMENTE RIMESSA ALLE SEZIONI UNITE

Cass. V, ord. 14 marzo 2017, n°12264:

«Si chiede al supremo Consesso riunito se il delitto previsto dall'art. 615 ter, comma 2, n. 1 cod. pen. sia integrato anche dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur 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, e se, quindi, detta condotta, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative, possa integrare l'abuso dei poteri o la violazione dei doveri previsti dall'art. 615 ter, comma secondo, n. 1 cod. pen.».

Art. 615 ter c.p. giurisprudenza

CONSUMAZIONE

*«Il **luogo di consumazione** del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 ter c.p., è **quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente**.»*

(Cass. Sez. Un., 26 marzo 2015, n°17325)

RAPPORTO CON ALTRI REATI

*«(…) **Né può dubitarsi che i reati di accesso abusivo ad un sistema informatico e la frode informatica possano concorrere**: trattasi di delitti diversi, il secondo dei quali postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del primo; d'altro canto l'accesso abusivo può essere commesso solo con riferimento a sistemi protetti, requisito non postulato per la frode informatica.»*

(Cass. V, 27 gennaio 2004, n°2672)

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

«Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno ingiusto, 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 a un anno e con la multa sino a € 5.164.

La pena è della reclusione da uno a due anni e della multa da € 5.164 a € 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.»

Art. 615 quater c.p. analisi del reato

Per «**procurarsi i mezzi di accesso**» di un sistema informatico o telematico si intende la condotta di chi si appropria della chiave meccanica o della scheda magnetica, oppure individua i codici di accesso attraverso procedimenti logici tipici del computer.

Per «**riprodurre**» si intende la condotta di chi realizza una copia abusiva di un codice di accesso, idonea all'uso.

La «**divulgazione**» a terzi è integrata mediante la diffusione, la comunicazione, la consegna, o condotte che possano concorrere con il mero procacciamento.

L'ultima parte della norma punisce anche chi **sveli particolari tecnici tali da consentire ad altri di procurarsi l'accesso**.

Il reato si consuma nel momento e nel luogo in cui il soggetto pone in essere una delle condotte previste dalla fattispecie, ed è caratterizzato dal dolo specifico che consiste nel procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

Art. 615 quater c.p. giurisprudenza

CASISTICA PREVALENTE: CLONAZIONE DI TELEFONINI

«Integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici di cui all'art. 615 quater c.p. 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.»

(Cass. II, 17 dicembre 2004, n°5688)

ALTRI CASI

«In tema di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, la detenzione di una scheda contraffatta (pic card) per la decrittazione delle trasmissioni a pagamento (pay tv) configura il reato di cui all'art. 615 quater c.p., ma non rientra nella previsione di cui all'art. 171 octies l. n. 248 del 2000, che concerne la tutela del diritto d'autore, con la conseguenza che tra le due previsioni non sussiste alcun rapporto di specialità.» (Cass. V, 29 maggio 2002, n°24847)

Art. 615 quinquies c.p.
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o a interrompere un sistema informatico o telematico

«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 € 10.329.»

Art. 615 quinquies c.p. analisi del reato

La norma, nella sua formulazione originaria, prevedeva tre condotte alternative (**diffusione**, **comunicazione** e **consegna**), in parte sovrapponibili, allo scopo di punire ogni forma di distribuzione o circolazione dei programmi nocivi.

Dopo l'entrata in vigore della **Convenzione di Budapest**, la fattispecie è stata modificata e sono state aggiunte, allo scopo di anticipare la soglia della punibilità, le condotte del **procurarsi, produrre, riprodurre, importare e mettere a disposizione**.

Ai **programmi informatici** sono state aggiunte le **apparecchiature** ed i **dispositivi**, anche se è scomparso ogni riferimento al carattere dannoso degli stessi.

La nuova fattispecie considera, dunque, anche condotte perfettamente lecite, ed anzi usuali nell'attività degli operatori, nelle quali **solo il dolo specifico dell'illecito danneggiamento rende il fatto penalmente rilevante**.

Trattasi di reato di pericolo, non essendo necessario, per la sua consumazione, l'effettivo danneggiamento del sistema, dei dati e delle informazioni.

Art. 616 c.p. Violazione, sottrazione e soppressione di corrispondenza

«Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da € 30 a € 516.

Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a 3 anni.

Il delitto è punibile a querela della persona offesa.

Agli effetti delle disposizioni di questa sezione, per "corrispondenza" s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.»

Art. 616 c.p. analisi del reato

La norma prevede, al primo comma, tre distinte ipotesi di reato che consistono rispettivamente nella:

- **presa di cognizione**
- **sottrazione e distrazione**
- **distruzione e soppressione**

della corrispondenza, **anche informatica o telematica**.

Il secondo comma punisce la **rivelazione** della corrispondenza **senza giusta causa**, intendendosi, con tale formula, l'assenza di ragioni che rendano inevitabile la commissione del reato.

È altresì necessario che dalla rivelazione derivi un **nocumento** al soggetto passivo, ovvero un pregiudizio giuridicamente rilevante, morale o materiale, sia per il mittente che per il destinatario.

Il bene giuridico tutelato è la segretezza e l'inviolabilità della corrispondenza, interesse garantito dall'art. 15 della Costituzione.

Le problematiche più rilevanti sotto il profilo informatico in ambito aziendale attengono, principalmente, alla **cognizione della posta elettronica aziendale** contenuta nel computer del dipendente da parte del datore di lavoro.

Art. 616 c.p. giurisprudenza

ELEMENTO OGGETTIVO

«Non si configura la fattispecie prevista dal comma 1 dell'art. 616 c.p., relativa alla cognizione, sottrazione o distrazione di una corrispondenza online, nei casi in cui la cognizione della posta elettronica venga fatta nell'ambito di un medesimo contesto lavorativo, non potendo equipararsi, tale cognizione, a quella della corrispondenza cartacea chiusa. Ove il sistema telematico sia protetto da una password, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che, legittimamente, dispongano della chiave informatica di accesso.»

(Trib. Cagliari, 22 gennaio 2015, n°8)

GIUSTA CAUSA

«In materia di violazione, sottrazione e soppressione di corrispondenza, la nozione di giusta causa, alla cui assenza l'art. 616 c.p., comma 2, subordina la punibilità della rivelazione del contenuto della corrispondenza, non è fornita dal legislatore ed è dunque affidata al concetto generico di giustizia, che la locuzione stessa presuppone, e che il giudice deve pertanto determinare di volta in volta con riguardo alla liceità - sotto il profilo etico e sociale - dei motivi che determinano il soggetto ad un certo atto o comportamento.»

(Cass. V, 15 dicembre 2014, n°52075)

Art. 616 c.p. giurisprudenza

CORRISPONDENZA «CHIUSA» E «APERTA»

«***Deve ritenersi che la corrispondenza informatica o telematica possa essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi***. *Infatti, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite. Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. E* ***quando in particolare il sistema telematico sia protetto da una password, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso***. *Anche quando la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso.*»

(Cass. V, 11 dicembre 2007, n°47096)

Art. 616 c.p. giurisprudenza

ACCESSO ALLA POSTA ELETTRONICA AZIENDALE

«Nel caso in cui il datore di lavoro, in forza del regolamento aziendale, sia legittimamente a conoscenza della password atta a proteggere il sistema informatico, la corrispondenza informatica o telematica del singolo dipendente non può essere qualificata come chiusa, pertanto non è ravvisabile una violazione dell'art. 616 c.p. nell'ipotesi in cui il superiore gerarchico prenda cognizione del contenuto della posta elettronica del lavoratore assente.»

(Cass. V, 11 dicembre 2007, n°47096)

Tale orientamento è stato recentemente – seppur indirettamente – confermato anche a livello comunitario, dalla sentenza CEDU *Barbulescu vs Romania* ECHR 013 del 12 gennaio 2016, che ha legittimato il licenziamento di un dipendente che aveva utilizzato la posta elettronica aziendale per fini personali.

A livello di **Codice della privacy** (D. Lgs. 196/2003), rivestono un rilievo specifico le ***policy* aziendali** sull'utilizzo della posta elettronica.

Art. 617 quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

«Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena di applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno ad un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore di sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.»

Art. 617 quater c.p. analisi del reato

Tale disposizione estende anche alla **comunicazione informatica o telematica** la tutela prevista dall'art. 617 c.p. in favore della **segretezza** e della **genuinità delle conversazioni o delle trasmissioni**.

Il **mezzo fraudolento** è richiesto **solo per** l'ipotesi di **intercettazione**, mentre **l'impedimento o l'interruzione** possono determinarsi **con qualunque mezzo**.

Per intercettazione si intende un'attività volta a rappresentare al sistema stesso in via automatica, o al gestore del sistema, una situazione non corrispondente al vero quanto all'identità del soggetto autorizzato, o alle caratteristiche del sistema intercomunicante, o dell'impianto ricevente, o alle particolari modalità richieste per la connessione o la ricezione di dati particolari.

Il dolo è generico e il reato si consuma nel momento e nel luogo in cui è compiuta una delle condotte previste dalla fattispecie.

Art. 617 quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

«Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617 quater.»

Art. 617 quinquies c.p. analisi del reato

La norma estende alle comunicazioni informatiche e telematiche la tutela prevista dall'art. 617 bis c.p. per le comunicazioni telefoniche o telegrafiche.

Il bene giuridico tutelato dalla norma è quello della sicurezza informatica e telematica.

Il reato si consuma nel momento e nel luogo in cui è compiuta l'installazione delle apparecchiature, anche qualora, per ragioni non concernenti l'idoneità assoluta, non abbiano funzionato.

Art. 617 sexies c.p. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

«Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617 quater.»

Art. 617 sexies c.p. analisi del reato

La norma estende alle comunicazioni informatiche e telematiche la tutela prevista dall'art. 617 ter c.p. per le comunicazioni telefoniche o telegrafiche.

Il bene giuridico tutelato è quello della sicurezza informatica e telematica.

La condotta consiste nella comunicazione distorta di ciò che è stato volontariamente o casualmente intercettato.

È irrilevante il modo in cui il reo sia venuto a conoscenza delle comunicazioni, e l'uso va considerato come elemento essenziale del reato, e non come condizione obiettiva di punibilità.

Art. 635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici

«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.»

Art. 635 bis c.p. analisi del reato

Il delitto in esame tutela i beni informatici.

Prima dell'entrata in vigore della L. n°547/93, la condotta consistente nella cancellazione di dati dalla memoria di un computer configurava un'ipotesi classica di danneggiamento, ai sensi dell'art. 635 c.p. (prima della modifica ai sensi del D.Lgs. 15 gennaio 2016, n° 7).

Le condotte di **cancellazione**, **alterazione** e **soppressione** previste dalla Convenzione di Budapest sono state previste in ragione del particolare oggetto materiale della condotta (le informazioni, i dati e i programmi informatici), ossia il *software* e le informazioni memorizzate in un elaboratore, difficilmente riconducibili al concetto di "cosa", a meno che la condotta non abbia ad oggetto anche il supporto magnetico che li contiene (*hardware*).

Il secondo comma prevede **due aggravanti**, ovvero quella relativa al fatto commesso con **abuso della qualità di operatore del sistema**, e quella relativa alla commissione del fatto con **violenza alla persona o minaccia**.

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

«Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque, di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto 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 aumentata.»

Art. 635 ter c.p. analisi del reato

La fattispecie ricalca la previsione dell'art. 635 bis c.p., diversificandosi per l'oggetto materiale, che attiene all'**ambito pubblico o di pubblica utilità**.

Sul piano oggettivo si distinguono due ipotesi di reato: la prima, costruita come delitto di attentato, garantisce un grado di tutela anticipata rispetto alla previsione generale.

La seconda ipotesi punisce la realizzazione dell'evento di danno.

Le circostanze aggravanti sono le medesime previste dall'art. 635 bis c.p.

Art. 635 quater c.p. Danneggiamento di sistemi informatici o telematici

«Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque 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 aumentata.»

Art. 635 quater c.p. analisi del reato

L'introduzione della autonoma fattispecie di danneggiamento al sistema informatico o telematico risponde ad una esigenza di simmetria rispetto alla sistematica della **Convenzione di Budapest,** che **distingue il danneggiamento dell'integrità dei dati** (art. 4, a cui corrisponde l'art. **635 bis c.p.**) dal **danneggiamento dell'integrità del sistema** (art. 5), che comprende i danneggiamenti realizzabili mediante programmi virus o altre tipologie di *malware*, anche attraverso internet.

Particolarmente importante è la previsione dell'ipotesi di ostruzione grave del funzionamento del sistema informatico o telematico, sia per la rilevanza pratica, sia per l'avere, la fattispecie, colmato un vuoto normativo relativo alla alterazione funzionale del sistema.

Trattasi di reato di evento, che prevede le stesse circostanze aggravanti dell'art. 635 bis c.p.

La procedibilità d'ufficio, non prevista per l'ipotesi di cui all'art. 635 bis c.p. (se non nell'ipotesi aggravata di cui al comma II) implica che il Legislatore abbia attribuito a tale fattispecie un coefficiente maggiore di gravità rispetto all'ipotesi di danneggiamento dei dati, nell'ambito della quale era ricompresa prima dell'entrata in vigore della L. 48/08.

Art. 635 quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità

«Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto 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 aumentata.»

Art. 635 quinquies c.p. analisi del reato

Per l'analisi delle principali questioni giuridiche che attengono a tale fattispecie si rimanda al commento sub art. 635 ter c.p.

L'unica differenza attiene al riferimento esclusivo alla "pubblica utilità", e non anche alla utilizzazione da parte dello Stato o di altro ente pubblico, anche se ciò non implica una significativa differenza a livello di applicazione pratica.

Art. 640 ter c.p.
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 € 51 ad € 1.032.

La pena è della reclusione da uno a cinque anni e della multa da € 309 ad € 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

La pena della reclusione da due a sei anni e della multa da € 600 ad € 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.»

Art. 640 ter c.p. analisi del reato

La norma prevede due condotte differenti, seppur sanzionate con la medesima pena:

1) **l'alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o telematico**: le condotte delineate consistono in un'alterazione estrinseca del sistema, volta ad indurlo a compiere operazioni diverse da quelle per cui è programmato, per trarne profitto ai danni del titolare;

2) **l'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti**: la condotta contempla, al contrario, le modifiche intrinseche al sistema operativo, dirette ad alterare, oltre che i dati, gli esiti delle elaborazioni, con inserimento di informazioni e delle correlazioni logiche del programma.

Art. 640 ter c.p. giurisprudenza

CONDOTTA INCRIMINATA E NATURA DEL REATO

«È un hacker anche chi detiene ed utilizza carte di credito clonate ed è chiamato, pertanto, a rispondere del reato di frode informatica di cui all'art. 640 ter.

La condotta che integra la figura criminosa, infatti, è duplice: da un lato, si persegue chi "alteri", in qualsiasi modo, il funzionamento di un sistema informatico o telematico; dall'altro, si persegue chi interviene senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti nel sistema, così da realizzare l'ingiusto profitto con correlativo altrui danno. L'utilizzazione di carte falsificate e la previa artificiosa captazione dei codici segreti di accesso (PIN) integra questa seconda ipotesi perché permette all'agente di penetrare abusivamente e, dunque, senza diritto, all'interno dei vari sistemi bancari, alterando i relativi dati contabili, mediante ordini (abusivi) di operazioni bancarie di trasferimento fondi: tale essendo, evidentemente, anche l'operazione di prelievo di contanti, attraverso i servizi di cassa continua.»

(Cass. II, 15 aprile 2011, n°17748)

Art. 640 ter c.p. giurisprudenza

RAPPORTO CON ALTRI REATI

«***Il delitto di accesso abusivo ad un sistema informatico può concorrere con quello di frode informatica***, *diversi essendo i beni giuridici tutelati e le condotte sanzionate, in quanto il primo tutela il domicilio informatico sotto il profilo dello "ius excludendi alios", anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, mentre il secondo contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto.*»

(Cass. V, 30 settembre 2008, n°1727)

«***Il reato di frode informatica si differenzia dal reato di truffa*** *perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.*»

(Cass. II, 20 novembre 2009, n°44720)

Art. 640 ter c.p. giurisprudenza

CONSUMAZIONE

«Il reato di frode informatica, previsto dall'art. 640 ter c.p., si consuma – non diversamente dal comune reato di truffa – nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo danno altrui.»

(Cass. VI, 4 ottobre 1999, n°3065)

CONFISCA

«In forza del rinvio indifferenziato dell'art. 640 quater c.p. alle disposizioni contenute nell'art. 322 ter c.p., la confisca di beni per un valore equivalente al profitto del reato può essere disposta anche nel caso di condanna per uno dei delitti previsti dagli artt. 640 comma 2 n. 1, 640 bis e 640 ter c.p.»

(Cass. Sez. Un. 25 ottobre 2005, n°41936)

Art. 640 quater c.p. Applicabilità dell'articolo 322 ter c.p. Confisca per equivalente

«Nei casi di cui agli articoli 640, secondo comma, numero 1, 640 bis e 640 ter, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'art. 322 ter.»

Art. 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

«Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 €.»

Art. 491 bis 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.»

Art. 491 bis c.p. analisi del reato

La norma individua l'ipotesi del cosiddetto "**falso informatico**", che consiste nella falsificazione di documenti informatici, ed è stata introdotta a seguito della ratifica della Convenzione di Budapest allo scopo di tutelare la pubblica fiducia riposta nella genuinità e nella veridicità di essi.

L'obiettivo del Legislatore era quello di attribuire alla firma digitale l'idoneità ad identificare univocamente l'autore del documento, in modo da consentire l'attribuzione al documento informatico della stessa natura di un atto originale, e dunque della piena efficacia giuridica sostanziale e processuale.

Art. 495 bis c.p.
Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri

«Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino a un anno.»

Art. 495 bis c.p. analisi del reato

La norma in esame e le condotte illecite dalla stessa previste sono formulate sulla scorta dell'art. 495 c.p. ("*Falsa attestazione o dichiarazione ad un pubblico ufficiale sulla identità o su qualità personali proprie e altrui*").

Per la concreta operatività di tale disposizione occorre far riferimento al Codice dell'amministrazione digitale (D.Lgs. 82/2005), che disciplina le dichiarazioni e le attestazioni che devono essere rese al certificatore qualificato competente a rilasciare il certificato elettronico necessario per l'ottenimento della firma elettronica qualificata o della firma digitale.

SEZIONE II:
I REATI INFORMATICI
PARTE PROCESSUALE

Con l'entrata in vigore della **L. 18 marzo 2008, n°48**, il Legislatore, ratificando la Convenzione di Budapest del Consiglio d'Europa del 23 novembre 2001, ha "aggiornato" parte delle disposizioni in tema di **mezzi di ricerca della prova** attraverso il riferimento ai sistemi informatici e telematici, e prevedendo – in parallelo – che tali operazioni assicurino la conservazione dei dati originali e la non alterabilità degli stessi.

Le disposizioni in tema di intercettazioni delle comunicazioni informatiche e telematiche erano già entrate in vigore con la **L. 23 dicembre 1993, n°547**, con cui sono state introdotte, sul piano sostanziale, le principali fattispecie incriminatrici relative all'ambito del *cyber crime*.

Le indagini preliminari: i mezzi di ricerca della prova

I principi della "***digital forensics***":

- acquisizione della prova senza alterazione o danneggiamento dei dispositivi originali
- autenticazione del reperto acquisito
- garanzia della ripetibilità dell'accertamento
- analisi senza modificazione dei dati originali
- imparzialità nell'agire tecnico

Art. 244 c.p.p.
Casi e forme delle ispezioni

«L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. ***L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione****.»*

Art. 247 c.p.p.
Casi e forme delle perquisizioni

"Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione **(comma 1 bis).**

La perquisizione è disposta con decreto motivato.

L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto."

Art. 248 c.p.p.
Richiesta di consegna

"Se attraverso la perquisizione si ricerca una cosa determinata, l`autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.

Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione."

Art. 253 c.p.p.
Il sequestro probatorio

“L'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti.

Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo.

Al sequestro procede personalmente l'autorità giudiziaria ovvero un ufficiale di polizia giudiziaria delegato con lo stesso decreto.

Copia del decreto di sequestro è consegnata all'interessato, se presente.”

Art. 256 c.p.p.
Dovere di esibizione e segreti

*"**Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.***

Quando la dichiarazione concerne un segreto di ufficio o professionale, l'autorità giudiziaria se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti i documenti o le cose indicati nel comma 1 provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro.

Quando la dichiarazione concerne un segreto di Stato l'autorità giudiziaria ne informa il Presidente del Consiglio dei Ministri chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato. Qualora entro sessanta giorni dalla notificazione della richiesta il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.

(...)"

Art. 259 c.p.p.
Custodia delle cose sequestrate

«Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso determinandone il modo e nominando un altro custode idoneo a norma dell'articolo 120.

All'atto della consegna il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. ***Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.***

(…)"

Art. 260 c.p.p.
Apposizione di sigilli alle cose sequestrate.
Cose deperibili.
Distruzione di cose sequestrate

"Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia.

L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti disponendo, quanto alle cose, in conformità dell'articolo 259. ***Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.***

(...)"

Art. 266 bis c.p.p. Intercettazioni di comunicazioni informatiche o telematiche

«Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.»

Art. 353 c.p.p. Acquisizione di plichi o di corrispondenza

“Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l’ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.

Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l‘apertura immediata e l'accertamento del contenuto.

Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati”.

Art. 354 c.p.p. Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.

"Gli ufficiali e gli agenti di polizia giudiziaria curano che e tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.

Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. ***In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.*** *Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.*

Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi alle persone diversi dalla ispezione personale".

SEZIONE III
I REATI INFORMATICI E LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

Art. 24 bis D. Lgs. 8 giugno 2001, n°231

DELITTI INFORMATICI

"In relazione alla commissione dei delitti di cui agli articoli 615 ter, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater e 635 quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

In relazione alla commissione dei delitti di cui agli articoli 615 quater e 615 quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

In relazione alla commissione dei delitti di cui agli articoli 491 bis e 640 quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)."