Tecniche Informatiche di ricerca giuridica

Nicolò Ghibellini
Università di Ferrara
ghbncl@unife.it

Quarta Lezione

I crimini informatci

Normativa di riferimento

1. L. n. 547 del 1993;
2. L. n. 48 del 2008 (ratifica Convenzione di Budapest sui crimini informatici)

Tecnica legislativa particolare:

- Introduzione di nuove fattispecie criminose nel codice penale
- Modifica articoli del codice penale preesistenti

Condotte criminose in ambito informatico

è possibile distinguere tra:

1. fatti illeciti commessi su parti del sistema (il sistema rappresenta l'oggetto del reato)
2. fatti commessi a mezzo del sistema (il sistema è mezzo del reato)

Esercizio arbitrario delle proprie ragioni (art. 392 c.p.)

comma 3

"*si ha altresì violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico*"

NB: <u>difficoltà di assimilare il programma informatico alle cose mobili tradizionalmente intese</u>

Oggetto del reato

- Programma informatico: qualunque software (sia realizzato dalla software house sia dal privato) registrato su supporti magnetici, ottici o di altra natura;
- Sistema informatico: insieme di risorse che immette, tratta ed emette automaticamente dei dati che può memorizzare o recuperare
- Sistema telematico: reti di telecomunicazione

Condotte criminose

- Alterazione: il sw viene modificato in modo da ridurne o impedirne il funzionamento
- Modificazione: il sw viene mutato in modo da perdere le sue caratteristiche originali
- Cancellazione: distruzione parziale o totale del programma
- Impedimento funzionamento sistema informatico o telematico: è reso difficoltoso l'originario svolgimento del servizio
- Turbamento funzionamento sistema informatico o telematico: è impedito il godimento della risorsa

Attentato ad impianti di pubblica utilità (art. 420 c.p.)

comma 2

"*la pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi ad essi pertinenti*"

Questo comma (unitamente al comma 2) è stato abrogato dalla L. n. 48 del 2008)

Falsità nei documenti informatici (art. 491-bis c.p.)

"Se alcuna delle falsità del presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. ***A tal fine un documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli****"*

Documento informatico

- Art. 3, L. 547/93: introduzione di un primo concetto di documento informatico (ai fini penali), inteso quale qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.
- Art. 1, DPR 513/97 (successivamente confluito nel DPR 445/2000): fornisce una più idonea definizione di documento informatico "*la rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti*"

Nuovo art. 491-bis cp

- *“Se alcuna delle falsità del presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*”

Ratio della modifica all'art. 491-bis cp

La L. n. 48 del 2008, eliminando la definizione di documento informatico ai fini penali opta -correttamente- per una tutela diretta dei contenuti trattati con tecnologie informatiche

Tutela del “domicilio informatico”

art.4 L. 547/93

- introduce nel codice penale gli artt. 615 *ter*, *quater*, *quinquies* (nell’ambito dei delitti contro l’inviolabilità del domicilio)
- sistemi informatici/telematici non solo come strumenti per compiere l’illecito penale, ma anche come luogo ove l’uomo trasferisce alcune delle proprie facoltà intellettuali

Quindi…

sistemi informatici e telematici

⇓

espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 c.p.

Domicilio informatico

"*non solo è il luogo ove il soggetto avente diritto può esplicare liberamente qualsiasi attività lecita, ma è un'area la cui tutela, grazie all'art. 615 c.p. si estende anche nello ius excludendi alios*"

(Cass.Pen. n. 3097/1999)

Accesso abusivo sistema informatico o telematico (art. 615-*ter* c.p.)

"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"

Condotte criminose

1. **Introduzione** in un sistema informatico o telematico protetto da misure di sicurezza
2. **Mantenimento** in un sistema informatico o telematico protetto da misure di sicurezza

Natura del reato

- reato di pericolo:

  rischio che chi accede abusivamente a un sistema sia in grado di impadronirsi o conoscere quanto custodito in esso.

- Il momento consumativo:

  intrusione in quanto tale (no rilevanza dell'effettiva presa di coscienza del contenuto delle informazioni contenute nel sistema o il successivo intervento dannoso sul sistema)

Concreta applicazione art. 615-*ter* c.p.

- necessario che il sistema oggetto del reato sia stato protetto da delle misure (minime) di sicurezza, tali da offrire un impedimento, un ostacolo minimo all'intruso
- la presenza di un sistema di sicurezza è sufficiente ad evidenziare la volontà del titolare del diritto, di escludere chi da lui non autorizzato ad accedere al sistema.

Misura minima di sicurezza

orientamento dottrinario maggioritario

⇓

richiesta nome utente e password ("*account*")

L'utilizzo di una "parola chiave" per essere identificati dal sistema costituirebbe un requisito sufficiente ad integrare il reato di cui all'art. 615-*ter* nel caso di intrusione da parte di terzi non autorizzati.

Misura minima di sicurezza

orientamento minoritario

⇓

- account non è un requisito sufficiente per definire un sistema protetto o comunque dotato di misure di sicurezza
- account non è ritenuto uno strumento sufficiente a garantire quel grado di sicurezza richiesto dalla norma

Cassazione Penale n. 12372 del 2000

- non occorre che le misure di scurezza siano costituite da chiavi d'accesso o altre analoghe protezioni (protezione interna)
- è sufficiente qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi

Ratio della decisione

l'art. 615 ter c.p. non punisce solo chi abusivamente si introduce in un sistema protetto ma anche chi vi si mantiene contro la volontà espressa o tacita di chi il diritto di escluderlo.

⇓

"*contravvenzione alle disposizioni del titolare*"

⇓

Volontà (anche implicita) del titolare di disporre autonomamente e liberamente dell'unità di elaborazione, escludendo o limitando gli accessi alle persone legittimate

Cassazione Penale n. 46509 del 2004

impostazione più rigorosa

"*non è ravvisabile il reato di accesso abusivo in quanto il sistema informatico nel quale l'imputato si inseriva abusivamente non risulta obiettivamente protetto da misure di sicurezza*"

⇓

manca il presupposto

della protezione del sistema

Riassumendo…

misura di sicurezza

rilevante per la configurazione del reato ex art. 615-*ter* c.p.

a. qualunque meccanismo idoneo a far trasparire la volontà (anche implicita) di escludere
b. presenza di un'obiettiva protezione del sistema

Circostanza aggravante

operatore di sistema

1. operatore in senso stretto: addetto alle operazioni di input e output, di avviamento o di arresto del sistema;
2. programmatore: scrive, con appositi linguaggi, le operazioni che il computer sarà chiamato ad effettuare;
3. sistemista: studia le possibili evoluzioni di un sistema per ottimizzarlo e implementarlo;
4. analista: scopre o inventa gli algoritmi

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-*quater* c.p.)

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, 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 fino ad un anno e con la multa fino a euro 5.164,00".

Condotte criminose

- diffusione: mettere a conoscenza di una o più persone indeterminate i codici di accesso, in qualunque forma, attraverso la disponibilità degli stessi
- riproduzione: produzione di una copia abusiva di un codice, di una “parola chiave” o di ogni altro mezzo idoneo all’accesso;
- consegna: cessione materiale del codice a una determinata persona;
- comunicazione: mettere a conoscenza di una o più persone determinate dei codici di accesso.

Concreta applicazione art. 615-*quater* c.p.

- il sistema informatico/telematico deve essere protetto da misure di sicurezza
- Dottrina

  l'esistenza delle misure minime di sicurezza costituisce una vera e propria condizione obiettiva di punibilità

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-*quinquies* c.p.)

"*chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in lui contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, l'alterazione del suo funzionamento* "

Nuovo art. 615-*quinquies* cp

“ *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 funzonamento, 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 10.3292*”

Modifiche all'art. 615-*quinquies* cp

1. Dolo specifico
2. Condotte tipizzate

Danneggiamento di sistemi informatici (art. 635-*bis* c.p.)

"chiunque distrugge deteriora o rende, in tutto in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni…"

Nuovo art. 635-*bis* cpc

“ *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*”

Modifiche all'art. 635-*bis* cpc

- Punibilità a querela della persona offesa
- Aspetto problematico: concreta individuazione della persona offesa dal reato

1. interessato, titolare e responsabile del trattamento/sistema;
2. concessionario, utilizzatore, concedente, proprietario de programma
3. Parteners commerciali o di lavoro

Artt. 635-*ter*, *quater*, *quinquies* cp

La L. n. 48 del 2008 introduce:

1. art. 635-*ter* cp (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)
2. art. 635-*quater* cp (danneggiamento di sistemi informatici o telematici)
3. art. 635-quinquies cp (danneggiamento di sistemi informatici o telematici di pubblica utilità)

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

"*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 se 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 516 a euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal n.1 del secondo comma dell'art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema […]* ".

Novità

- Il Legislatore ridisegna la figura tradizionale del reato di truffa
- Nuovo concetto di *"induzione in errore di una persona mediante artifizi o raggiri"*
- Il raggirato è il computer soggetto alla alterazione ad opera del reo

Cassazione Penale n. 3065 del 1999

il reato di frode informatica:

- ha la medesima struttura e i medesimi elementi costitutivi della truffa
- si differenzia dalla truffa solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

Condotte criminose

- alterazione in qualunque modo del funzionamento di un sistema informatico/telematico, procurando a sé o ad altri un ingiusto profitto con danno per il soggetto passivo;
- intervento senza diritto in qualunque modo su dati, informazioni o programmi contenuti in un sistema informatico/telematico, procurando a sé o ad altri un ingiusto profitto con danno altrui

Modalità operative della condotta

- Intervento sui dati inseriti nel computer

  i dati potrebbero essere manipolati dal soggetto attivo (alterazione o immissione abusiva). In questo caso esiste concorso di reato con l'art. 491-*bis* (delitto di falso informatico);

- Intervento sul programma operativo del sistema

  il software viene alterato affinché il computer (o il sistema) operi in modo differente da come è stata progettata al fine di compiere illeciti;

- Intervento sulle informazioni

  ovvero sulla correlazioni fra i dati contenuti in un elaboratore o in un sistema.