A.A. 2014/15
C.L.M. Giurisprudenza
Università degli Studi di Teramo

Informatica Giuridica II
Prof. Guido Saraceni

Elementi di filosofia e di teoria del diritto penale

Elementi di filosofia e di teoria del diritto penale

- I **reati a forma vincolata** reati che richiedono specifiche modalità di condotta. Il bene protetto è tutelato solo contro determinate modalità di azione

- I **reati a forma libera** reati in cui la fattispecie è descritta facendo riferimento solo all'evento (es. la norma penale che punisce l'omicidio tutela il bene della vita indipendentemente dalle modalità di aggressione)

Elementi di filosofia e di teoria del diritto penale

- La qualità personale necessaria per commettere un *reato proprio* può essere *permanente* o *temporanea*, come nel caso del testimone per la falsa testimonianza; può dipendere anche da una condizione temporanea che "attiva" uno status latente, come nel caso dell'elettore che entra armato in un seggio elettorale.

La struttura del reato informatico

1) Reati commessi grazie ad un sistema informatico o telematico

2) Reati commessi contro un sistema informatico o telematico

La struttura del reato informatico

La legge 547/93 non definisce il "sistema informatico".

L'art. 1 della Convenzione di Budapest (23.11.2001) contiene una definizione di "sistema informatico".

La struttura del reato informatico

La Cassazione ha definito il sistema informatico come "una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche".

La struttura del reato informatico

Il soggetto attivo: *normalmente* si tratta di *reati comuni* che diventano *aggravati* nel caso in cui la condotta lesiva sia stata posta in essere dal SYSOP (SYSTEM OPERATOR).

La struttura del reato informatico

Il SYSOP è chiunque può usufruire *senza limitazioni* delle risorse di un elaboratore elettronico e che svolge - in maniera *continuativa o meno* - attività di manutenzione e/o attivazione e/o controllo del sistema.

La struttura del reato informatico

Il Provider ha un dovere di controllo, è responsabile per i reati commessi su internet (ex art.40 c.p.) ?

Esiste comunque una responsabilità del Provider (analogamente a quanto accade per il direttore di un giornale?)

La struttura del reato informatico

ISP (INTERNET SERVICE PROVIDER)

Attività di *mere conduit*

Hosting (memorizzazione)

Caching (memorizzazione temporanea)

La struttura del reato informatico

Il SYS è sempre responsabile se omette di agire prontamente a seguito di una richiesta dell'autorità amministrativa/giudiziaria.

La struttura del reato informatico

Si considera commesso sul territorio dello Stato un reato se nel territorio nazionale si è verificata l'azione o l'omissione, ovvero almeno una parte della condotta o dell'evento (art. 6 c.p.)

La struttura del reato informatico

La legge n.547 del 23 dicembre 1993 ha *disseminato* i reati informatici all'interno del codice penale.

La pedopornografia. La riforma del 2006

La tecnica utilizzata è stata quella della novella legislativa

Vengono inasprite le pene

Viene introdotto il concetto di **immagine virtuale**, ovvero di quella immagine realizzata in modo da far apparire come vere situazioni non vere.

La pedopornografia. La riforma del 2006

LEGGE 38 del Febbraio 2006

Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet

La pedopornografia. La riforma del 2006

La tecnica utilizzata è stata quella della novella legislativa

Vengono inasprite le pene

Viene introdotto il concetto di **immagine virtuale**, ovvero di quella immagine realizzata in modo da far apparire come vere situazioni non vere.

La tutela del domicilio informatico

- La tutela delle aggressioni provenienti da estranei costituisce una estrinsecazione della personalità nella sua dimensione spaziale.

La tutela del domicilio informatico

Non si tratta tanto di proteggere la proprietà o il possesso in sé considerati, quanto di proteggere la libera estrinsecazione della personalità individuale.

La tutela del domicilio informatico

L'art. 615 ter – introdotto con la legge 547/93- salvaguarda il *domicilio informatico*. Il reato è stato inserito nella sezione IV del codice penale dedicata ai delitti contro la inviolabilità del domicilio.

La tutela del domicilio informatico

Alcuni studiosi ritengono che l'istituto protegga una pluralità di beni giuridici che vanno dal diritto alla riservatezza, ai diritti di natura patrimoniale, fino ad interessi collettivi, come quelli di carattere sanitario o militare.

La tutela del domicilio informatico

Dal canto suo, la Cass. Penale ha chiarito che non è rilevante la natura dei dati né il fatto che il titolare dello jus excludendi sia persona fisica, giuridica, privata o pubblica.

La tutela del domicilio informatico

Esattamente, la norma stabilisce che *Chiunque* abusivamente *si introduce* in un sistema *informatico o telematico* protetto da mis*ure di sicurezza*, ovvero *si mantiene* contro la volontà *espressa o tacita* di chi il diritto di escluderlo è punito con la reclusione sino a tre anni.

La tutela del domicilio informatico

La seconda condotta punita dalla norma implica che l'accesso sia avvenuto lecitamente, ma il soggetto agente ha violato i limiti temporali - o teleologici- stabiliti dal titolare del sistema.

La tutela del domicilio informatico

Non rilevano le finalità dell'intrusione, né il fatto che il soggetto agente abbia effettivamente carpito le informazioni altrui.

La tutela del domicilio informatico

Secondo la Cass. Pen. Sez V è una misura di sicurezza 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'accesso nei locali in cui gli impianti sono custoditi.

Offendicula e misure di sicurezza

Non sembra del tutto corretto stabilire un parallelismo concettuale tra gli *offendicula* e le misure di sicurezza di cui al presente articolo.

La frode informatica

Art. 640 ter

"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 ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno…"

La frode informatica

L’alterazione di cui parla la norma può avvenire intervenendo indifferentemente sull’hardware o sul software.

La frode informatica

Ci sono state alcune perplessità nell'estendere la fattispecie di cui all'art.640 c.p. ai casi di *frode informatica.*

Dato che, in questi casi, il raggirato sarebbe l'elaborato elettronico.

La frode informatica

Prima della l.547, a queste ipotesi di reato è stato tuttavia applicato il reato di truffa.

Sul presupposto che una frode informatica implica che vengano ingannati i soggetti preposti al controllo del sistema –nel caso in cui questi soggetti esistano.

La frode informatica

Se l'alterazione avviene modificando le componenti fisiche del sistema ed in modo che sia necessaria una successiva riparazione si può configurare anche il delitto di **danneggiamento di sistemi informatici** (635 c.p.)

La frode informatica

Si tratta di un reato **di danno** a ***consumazione istantanea***.

La frode informatica

Il momento ed il luogo di commissione del reato coincidono con il momento ed il luogo in cui il soggetto agente ha ottenuto una utilità *economicamente valutabile*.

La frode informatica

L'art.640 quinquies punisce con la reclusione fino a cinque anni il ***certificatore di firma elettronica*** che, al **fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno**, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

La diffusione di virus informatici

I virus informatici sono quei programmi che, *operando all'insaputa dell'utente o contro la sua volontà*, riescono a riprodursi, ad alterare, a danneggiare o distruggere dati, informazioni ed applicazioni presenti in un sistema.

La diffusione dei virus informatici

Alcuni virus informatici producono danni appena introdotti nel sistema informatico, altri restano in uno stato di quiescenza e possono essere attivati in ragione di una data o d uno specifico evento (**Time Bomb o Logic Bomb**).

La diffusione dei virus informatici

Art. 615 quinqueis

"*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

La diffusione di virus informatici

di favorire l'**interruzione**, totale o parziale, o l'**alterazione** del suo funzionamento,

si

1) procura,
2) produce,
3) riproduce,
4) importa,
5) diffonde,
6) comunica,
7) consegna

o comunque

La diffusione di virus informatici

"Mette a disposizione di altri apparecchiature, dispositivi o programmi informatici".

La diffusione dei virus informatici

"Il reato si consuma anche se il programma nocivo **non ha ancora prodotto i suoi effetti**, ma possiede **in concreto le potenzialità distruttive**, come nel caso di virus a tempo o ad attivazione collegata a particolari condizioni".

La diffusione di virus informatici

La diffusione dei virus è illecita perché la semplice esistenza e circolazione dei virus rappresenta **un pericolo**.

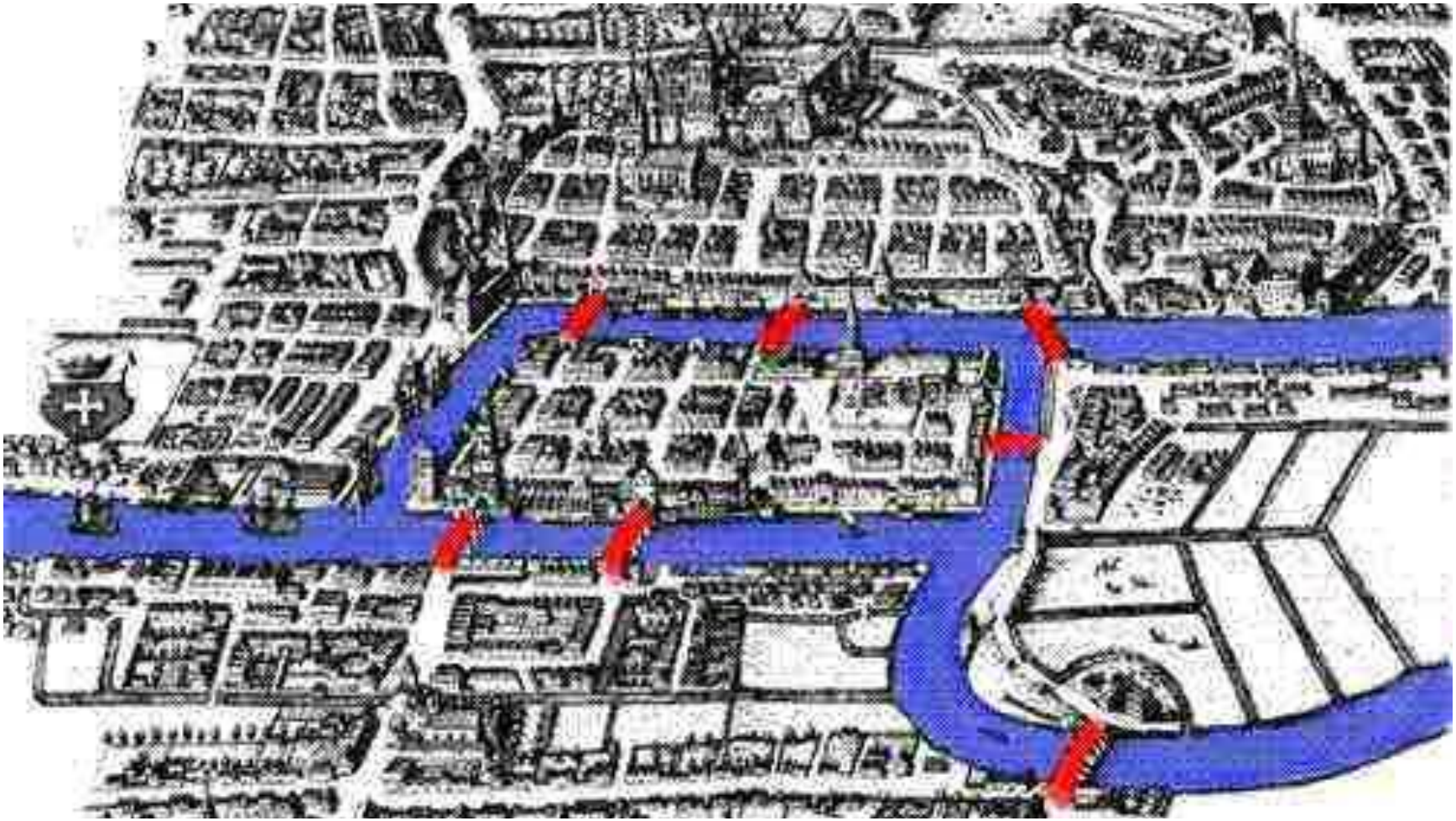
La diffusione di virus informatici

Il dolo specifico serve a fare in modo che non siano imputabili quegli utenti che sono stati infettati e che inconsapevolmente diffondono un virus.

La diffusione di virus informatici

Il dolo specifico evita che possano essere imputati quei soggetti che fanno ricerca sui virus e che, per questo motivo, creano sperimentalmente **programmi nocivi** (non "antivirus" come scrive il libro).

Elementi di Scienza delle Reti



Elementi di Scienza delle Reti

In base agli ultimi studi, la distribuzione dei nodi sembra seguire una *legge di potenza*.

Una legge di potenza può essere rappresentata tramite un *grafico a baffo*.

Elementi di Scienza delle Reti

Gli HUB sono nodi altamente interconnessi.

Gli HUB rappresentano la maggiore forza e la maggiore debolezza delle reti.

Il coefficiente di clustering descrive la coesione di una rete.