Il fenomeno dei computer crimes e le scelte del legislatore, tra ampliamento di fattispecie e introduzione di nuovi reati (a cura del Dottor Antonio Guzzo Responsabile Ced – Sistemi Informativi del Comune di Praia a Mare).

Il Fenomeno dei computer crimes

Nell'ultimo decennio c'è stata una vera e propria rivoluzione e cambiamento di tendenza nell'universo criminale. Sono apparsi sulla scena i cd. computers crime i reati informatici. Le peculiarità del crimine informatico sono: a-territorialità del contesto di riferimento, prossimità con la vittima senza la dinamica del face to face e anonimità dell'autore del reato. Tali caratteristiche determinano conseguenze sia a livello repressivo sia a livello investigativo. L'indeterminatezza del locus commissi delicti, un reato informatico si celebra all'interno di uno spazio virtuale in cui gli utenti connessi ad internet non sono necessariamente residenti nel medesimo Stato, implica problematiche connesse alla perseguibilità del reato. In materia di criminalità informatica non vi è una normativa internazionale uniforme. Un condotta sanzionata in Italia può non esserlo in altri paesi. L'attività di ricerca dei mezzi di prova può arrestarsi a causa di tale differenziazione. In tal senso la legislazione italiana è all'avanguardia in quanto la cd. teoria dell'ubiquità, sancita dall'art. 6 del c.p., stabilisce che un reato si considera commesso in territorio tanto se vi si è originata la condotta quanto se si è consumato l'evento. Internet è un potente strumento di comunicazione in grado di abbattere le barriere spazio temporali permettendo ad individui lontani geograficamente di dialogare. Sul piano criminale significa che possibili vittime sono tutti coloro che utilizzano la Rete. La Rete offre ai fruitori, leciti ed illeciti, l'opportunità di celare la propria identità attingendo a strumenti tecnici: gli anonimyzer ed i proxy. L'utente nel corso della navigazione web si riconosce mediante una cd. targa virtuale (ip address) assegnata dall'Internet Service Provider. Tale segno di riconoscimento può essere nascosto collegandosi ad un sito web o server che funge da intermediario con il sito visitato. Il risultato sarà l'impossibilità di risalire all'ip dell'utente in quanto si visualizzerà l'ip del anonimyzer o proxy. Sul piano investigativo la strategia messa in campo dalla Polizia Postale e delle Comunicazioni prevede una ripartizione delle vittime in utenti privati, qualificati ed infrastrutturali a cui corrispondono modus operativi specifici, un'accurata selezione degli operatori impegnati nelle indagini e una capillare presenza sul territorio. Nel caso di utenti privati, vittime in particolare di condotte riferite al fenomeno all'utilizzo di dialer, al phishing ed all'identify theft (furti identità), il momento repressivo è preceduto da una campagna di sensibilizzazione finalizzata ad innalzare il livello di guardia da parte dei cittadini. Inoltre, mediante la posta elettronica la Polizia Postale e delle Comunicazioni è permanentemente in contatto con i navigatori del web. Ciascun ufficio territoriale è dotato di un indirizzo di posta elettronica consultabile sul sito web della polizia di stato (www.poliziadistato.it). In aggiunta vi è il monitoraggio delle chat da parte degli investigatori della Polizia Postale e delle Comunicazioni, importante nell'azione repressiva contro la pedofilia on line.

Tale impatto derivante dall'utilizzo delle tecnologie digitali dell'informatica e della telematica ha inciso in maniera dirompente sulla creazione di nuove attività criminali e cioè a nuove modifiche sostanziali nelle modalità i cui tali attività criminali possono svolgersi. Prima di passare a definire le fattispecie criminose in oggetto è doveroso dapprima definire il concetto di reato con il quale si intende una condotta (un azione, un'omissione) riferibile alla volontà umana (tale fattispecie è molto importante in quanto richiama il concetto di dolo o di colpa) in contrasto con l'ordinamento giuridico, il quale di fronte alla violazione di uno o più beni giuridici protetti, commina una sanzione di tipo penale. Un reato è una condotta sancita, vietata dall'ordinamento penale, il quale a fronte della violazione di questo divieto reagisce con una sanzione penale (reclusione, sanzioni pecuniarie, etc.).

Un *computer crime* è un comportamento, implicante l'uso di un sistema informatico, previsto e punito come reato dalla legge. Quindi un computer crime è un reato che in qualche modo ha nella sua fattispecie un sistema informatico e che prevede l'uso di un pc. I crimini informatici si dividono in"crimini informatici propri" e "crimini informatici impropri" sulla base del bene giuridico protetto. Uno dei problemi della computer crime è la facilità di comunicazione in quanto sulla rete si trova di tutto.

Crimini Informatici Propri e Crimini Informatici Impropri

Il Legislatore ha individuato i computer crimes sulla base del bene giuridico protetto. Ha introdotto nuove norme per i reati compiuti contro i computer (i cosiddetti crimini informatici propri) ed ha inserito i reati compiuti per mezzo dei computer (crimini informatici impropri) all'interno delle vecchie disposizioni, ritenendo il computer un mezzo simile ad altri. In genere per i crimini informatici propri si è generata una normativa ex-novo mentre per quanto concerne i crimini informatici impropri si è adeguata la normativa precedente a questo nuovo mezzo. Un altro problema importante connesso all'impatto dell'informatica sul diritto penale affianco a quei reati che minacciano la sfera privata, il patrimonio, etc è quello relativo alla rapida circolazione delle informazioni I reati informatici minacciano non solo la sfera privata ed il patrimonio, ma possono agevolare la rapida circolazione delle informazioni, venendo a costituire un efficace mezzo di comunicazione utilizzato anche per scopi illegali. Nella categoria dei crimini informatici, eterogenei per modalità operative e scopi della condotta, possono essere distinte alcune tipologie o categorie:

1. ***Crimini con finalità di profitto*** per l'autore e di danno per la vittima (*appropriazione o manipolazione di programmi ed informazioni, frodi elettroniche, ecc.*);
2. ***Crimini diretti contro il computer*** (contro il sistema informatico) in cui il sistema informatico è l'oggetto materiale del reato per provocarne la distruzione o l'inservibilità (*sabotaggio, vandalismo, danneggiamento informatico*);
3. ***Crimini correlati all'uso del computer*** che così diviene cosa pertinente al reato o strumento necessario per agevolare o per consumare la condotta illecita ossia vi sono una serie di reati la cui realizzazione viene facilitata dall'utilizzo di un pc (pensiamo ad esempio al traffico di materiale pedo-pornografico su internet).

I reati informatici sono in genere reati commissivi, di condotta o di evento (vuol dire che non sono in genere reati omissivi, ossia perchè possa essere configurata questa fattispecie reato ci deve essere sempre un "*facere*" o un "*agere*"), e possono essere di condotta o di evento, cioè può essere sufficiente che l'agente ponga in essere su un determinato comportamento, una determinata condotta a prescindere dall'evento che si verifichi oppure possono essere reati di evento ossia che sia necessario perché si configura la fattispecie penale che si verifichi un determinato scopo e che si raggiunga lo scopo che l'agente si è prefissato (ossia che a sua volta causa un evento pericoloso o dannoso per la persona offesa o per il titolare del sistema oggetto di intrusione, sabotaggio o danneggiamento). Il concetto della querela di parte è un grosso handicap nel ristabilimento della legalità in questo ambiente. Nelle fattispecie non aggravate da particolari circostanze (articoli del codice penale che richiamano le cosiddette circostanze aggravanti), la perseguibilità del reato è generalmente a querela di parte cioè affinchè possa intervenire l'autorità giudiziaria ci deve essere la parte danneggiata che deve denunciare questo fatto cioè deve chiedere essa la tutela dell'autorità giudiziaria. Questa opzione legislativa ha però evidenziato alcuni grossi limiti per quanto concerne la sicurezza generale del sistema perché accade spesso che i soggetti attaccati non ritengano conveniente richiedere l'intervento dell'autorità giudiziaria perché la notorietà che consegue all'intervento dell'autorità giudiziaria è per loro un danno maggiore di quello subito dall'attacco criminale. Ovviamente questa omertà da parte delle vittime facilita il ripetersi degli attacchi criminosi. Uno dei limiti del nostro sistema è quello di prevedere quasi sempre la querela di parte sottovalutando gli interessi generali alla sicurezza informatica che probabilmente travalica e va oltre quello che può essere l'interesse della singola persona o della singola azienda a vedere tutelato il proprio sistema informatico. Questa opzione legislativa ha però evidenziato alcuni limiti e spesso la

querela non c'è. Accade infatti spesso, ad esempio, che imprese vittime di attacchi al proprio sistema informatico preferiscono non denunziare il fatto all'autorità giudiziaria per timore di diminuire la propria immagine o la parvenza di efficienza ed affidabilità sul mercato. Ciò facilita il ripetersi di fatti criminosi.

I reati informatici

Quando parliamo di crimini informatici è necessario dapprima definire il concetto di bene giuridico informatico. L'introduzione dei sistemi di produzione e trasmissione a distanza di informazioni, che consentono di memorizzare, elaborare e diffondere i dati con l'impiego di un linguaggio elettronico, ha creato un nuovo bene economico, che può essere definito "*bene giuridico informatico*". Il bene giuridico informatico può essere venduto o ceduto in uso (ad es. il software) ma può anche essere indebitamente sottratto, danneggiato o manomesso per cui deve essere protetto non solo con accorgimenti di carattere tecnico, ma anche con adeguati strumenti legislativi ossia questa parte dell'economia ha bisogno di essere protetta dall'ordinamento. Il primo grosso problema che si è verificato è la pirateria informatica. La pirateria informatica è in grado di ledere beni giuridici diversi (patrimonio, fede pubblica, ordine pubblico, inviolabilità dei segreti e del domicilio) e spazia nei settori più disparati, estendendosi dall'intrusione nel sistema di elaborazione altrui con conseguente furto di dati allo "*sniffing"* ("ascolto" e "cattura" dei dati in rete), all'illecita duplicazione del software, fino al sabotaggio delle banche dati. L'informatizzazione intesa come produzione e la gestione di informazioni ha agito su vari livelli sociali ed organizzativi determinando:

A) la formazione di un corpo normativo specifico ;

B) la considerazione della rete come lo spazio di interconnessione tra le aziende ed i vari comparti della pubblica amministrazione, nonché il luogo dove si concentrano rilevanti interessi economici ed elevati investimenti (un luogo giuridicamente rilevante);

C) la modifica dei comportamenti individuali e delle categorie tradizionali delle azioni criminali.

Le modalità comunicative, strettamente correlate all'impiego delle tecnologie digitali, hanno migliorato l'efficienza operativa delle strutture criminali (sovente le strutture criminali sono state più veloci nell'informatizzazione di quanto non lo siano stati i soggetti, per motivi di bilancio, i soggetti demandati alla repressione di questi comportamenti) che si adattano a tutte le innovazioni e sfruttano ogni potenzialità dei nuovi mezzi di comunicazione. E' noto che esistono delle organizzazioni criminali etniche che sono specializzate su determinati reati informatici ad esempio sulle clonazioni di carte di credito, etc. La diffusione delle reti telematiche ha moltiplicato le possibilità di esposizione dei sistemi informatici ad attacchi esterni ed ha ampliato la gamma delle condotte illecite possibili. Negli anni settanta un comportamento illecito fu considerato quello che si verificò nell'università di Roma La Sapienza, quando alcune persone per motivi ideologici considerando i computer come strumento di controllo sociale, entrarono nel ced (Centro Elaborazione Dati) e distrussero alcune macchine. Oggi la rete consente la realizzazione di attacchi molto più semplici e potenti.

Metamorfosi di reati tradizionali

Alcune fattispecie di reato tradizionali, come furti di informazioni, spionaggio, frodi, gioco d'azzardo, prostituzione, traffici vari (armi, droga, ad esempio è possibile acquistare all'estero armi di tutti i tipi come negli Stati Uniti ad esempio in Inghilterra è lecito acquistare baionette decorative), molestie, minacce, pedofilia, pornografia, criminalità organizzata e terrorismo, hanno subito una evoluzione e sono in grado di articolarsi solamente all'interno dei nuovi sistemi di comunicazione digitale (cyberpedofilia, cyberterrorismo, cyberstalting, hacking, diffusione di virus informatici, frodi telematiche, spamming, net-strike, diffusione di informazioni illegali on-line). Nel 1989 il consiglio d'Europa emette una raccomandazione la n° 9 del 13-9-89 nella quale invita i governi a rivedere la propria legislazione per affrontare queste nuove problematiche. Alla fine del

1993 in Italia viene recepita la raccomandazione n° 9 del 1989 con la legge 23 Dicembre 1993 n° 547. Questa legge infatti rappresenta il momento centrale in Italia di analisi del fenomeno dei computer crimes. Con tale legge si è effettuata una duplice operazione: da una parte un innesto di nuove fattispecie nel vecchio tronco dell'impianto codicistico; dall'altro si è proceduto alla modifica di preesistenti fattispecie penali. Questa operazione di "chirurgia legislativa" è stata attuata con il chiaro intento di stigmatizzare i nuovi e dilaganti fenomeni di criminalità informatica. Infatti la prevenzione e la repressione di tali fenomeni è legata in maniera forte alla legge 23 dicembre 1993, n. 547 (*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*), che ha introdotto nuove fattispecie sanzionatorie laddove si trattava di attacchi a sistemi informatici, ovvero ha integrato disposizioni preesistenti laddove l'interferenza con un sistema informatico non faceva altro che modificare ed ampliare una fattispecie già prevista **.** L'ordinamento italiano è pervenuto, in leggero ritardo, alla definizione di una disciplina generale dei c.d. computer crimes, con la legge 23 dicembre 1993 n. 547, dopo un anno dall'intervento a tutela del software, attuato dal decreto legislativo 29 dicembre 1992 n. 518, che ha modificato all'uopo la legge 22 aprile 1941, n. 633.
Esaminiamo ora quali sono le principali fattispecie penali che sono state introdotte nel codice penale e che appartengono alla categoria di crimini informatici (computer crimes).
1) La prima fattispecie criminale che noi esaminiamo è una abbastanza nota ed è rappresentata dall'***Esercizio arbitrario delle proprie ragioni*** normata dall'art. 392 c.p. che testualmente così recita: "Chiunque al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo mediante violenza sulle cose è punito, a querela della persona offesa con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorchè la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. Si ha, altresì, violenza sulle cose allorchè un programma informatico viene alterato, modificato o cancellato in tutto o in parte viene impedito o turbato il funzionamento di un sistema informatico telematico." Sarebbe come dire che se un soggetto fosse stato introdotto per dolo o per errore in una centrale di rischio inserisce un virus nel computer di questa centrale e distrugge tutto. In tale fattispecie criminosa il soggetto attivo del reato di esercizio arbitrario delle proprie ragioni mediante violenza sulle cose può essere anche chi esercita il preteso diritto pur non avendone la titolarità. Può anche essere persona diversa dal titolare del diritto illecitamente tutelato, quando questa abbia agito secondo lo schema della negotiurum gestio cioè una fattispecie relativa a condotta di violenza sulle cose attuata per esercitare il presunto diritto di proprietà di un figlio dell'agente. Infine può essere anche colui che non abbia la titolarità del diritto arbitrariamente esercitato, ma che agisca quale mero negotiorum gestor dell'effettivo titolare (fattispecie relativa all'arbitrario esercizio di un diritto del quale è risultato essere titolare il coniuge del soggetto agente). Inoltre affinchè tale fattispecie criminosa si verifichi è necessario, da un lato, quale elemento essenziale di carattere oggettivo, che la pretesa fatta valere dall'autore del fatto possa formare oggetto di una contestazione giudiziaria, senza che abbia, tuttavia, decisiva rilevanza la fondatezza o non della pretesa stessa, e, dall'altro quale essenziale elemento di carattere soggettivo, che l'imputato abbia agito nel ragionevole convincimento della legittimità della sua pretesa. Tale reato richiede oltre che il dolo generico anche quello specifico, rappresentato dal fine particolare di esercitare un proprio diritto: detto fine, se può non essere esclusivo, non può tuttavia concordare con scopi diversi incompatibili, che escludano, cioè prima ancora che il fine specifico voluto dalla norma , l'intento di farsi, sia pure arbitrariamente, ragione da se medesimo, come quando, ad esempio, si pongano in essere violenza sulle cose o minacce di una gravità eccezionale che esorbitano da quel fine o rendono comunque palese la concomitanza di un fine diverso come quello di rappresaglia o di vendetta. Passiamo ora ad esaminare come il legislatore ha analizzato tale fattispecie in due periodi temporali diversi.
TESTO PRE-1993
Articolo 392 c.p. Esercizio arbitrario delle proprie ragioni con violenza sulle cose. (constava di due commi) che cosi recitava :**"**Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito a

querela della persona offesa, con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione." Perché è importante l'intervento del legislatore in quanto nel diritto penale le norme non possono essere interpretate estensivamente. La fattispecie è tassativa e non può essere allargata in quanto vi è un principio cardine della attuale civiltà giuridica che dice nullum crimens sine previa lege penale. Dato che le fattispecie devono essere chiare perché è un ordine di non fare qualcosa se nella fattispecie non ci rientra. Un esempio classico ci viene dato dall'emissione di onde elettromagnetiche di Radio Vaticano.

TESTO POST 1993

Articolo 392 c.p. Esercizio arbitrario delle proprie ragioni con violenza sulle cose.

Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito a querela della persona offesa, con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. 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. *(Terzo comma aggiunto dall'art. 1, L. 23 dicembre 1993, n. 547, che modifica ed integra le norme del codice penale e del codice di procedura penale in tema di criminalità informatica).*

2) Un altro reato informatico è l'***Attentato ad impianti di pubblica utilità*** normato dall'art. 420 c.p. che cosi testualmente recita : "Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni. 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 in essi contenuti o ad essi pertinenti. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni". Nello sostanza tale fattispecie criminosa stabilisce di punire chiunque commetta un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità o dati, informazioni e programmi in essi contenuti o pertinenti. Passiamo ora, anche per questa fattispecie, ad esaminare come il legislatore ha analizzato tale fattispecie in due periodi temporali diversi.

TESTO PRE 1993

Articolo **420 c.p. Attentato a impianti di pubblica utilità.**

Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità o di ricerca o di elaborazione di dati, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o l'interruzione del suo funzionamento, la pena è della reclusione da tre a otto anni.

Si può notare come già prima del 1993 si parlava "impianti di elaborazione dati" ed evidente che questa non fa parte del codice penale ed è stata aggiunta dopo ma ad un certo punto ci si è resi conto che questo inciso inserito in quel comma non era sufficiente. Allora è stato riformulato l'articolo.

TESTO POST 1993

Articolo 420 c.p. Attentato a impianti di pubblica utilità

Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni. 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 in essi contenuti o ad essi pertinenti. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni.

Con questa nuova formulazione il legislatore ha inteso introdurre una nuova figura di reato diretta ad una più estesa tutela dell'ordine pubblico, sanzionando penalmente qualsiasi attività diretta a distruggere o danneggiare impianti di pubblica utilità o di ricerca o di elaborazione di dati, attività considerata di per se stessa idonea a turbare la serena e ordinata convivenza sociale indipendentemente dal verificarsi in concreto del relativo turbamento. Affinchè tale reato possa configurarsi è necessaria la presenza di un impianto inteso concettualmente come il complesso di strutture, apparecchi, attrezzature e congegni concorrenti ad uno stesso scopo ed indispensabili per un determinato fine. Di fondamentale importanza è anche il concetto di pubblica utilità con il quale si intende un'attività pubblica cioè non limitata a singoli soggetti (ad es. una centralina computerizzata dei semafori in una città, un portale web di un ministero). Un esempio di attentato ad impianti di pubblica utilità ci viene dato da azioni di sabotaggio effettuate da determinati soggetti che manomettano i dischi software in uso presso l'elaboratore elettronico di un centro di calcolo universitario.

3) Un altro reato è quello dell'***Accesso abusivo ad un sistema informatico o telematico*** normato dall'art. 615 *ter* c.p. che cosi testualmente recita :"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero si mantiene contro la volontà espressa o tacita del titolare, 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 del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente 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 ([1].)". Questo articolo è stato fatto su ricalco di un altro articolo che prevede la violazione di domicilio, per cui è stato individuato un domicilio informatico al quale sono state date le stesse tutele date al domicilio fisico. Il concetto di introduzione ha dato luogo a qualche difficoltà interpretativa. 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.

Esaminiamo ora una massima della cassazione penale dove per massima intendiamo un abstract del principio affermato dalla sentenza di cassazione.

Cassazione Penale E*lemento materiale del reato*

Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa. Cioè io vado li, non voglio far niente di male ed entro proprio come fanno gli attaccanti. (Fattispecie in cui il reato è stato ravvisato nella condotta degli imputati, che si erano introdotti in una centrale Telecom ed avevano utilizzato apparecchi telefonici, opportunamente modificati, per allacciarsi a numerose linee di utenti, stabilendo, all'insaputa di

[1] • Articolo aggiunto dall'*art. 4, L. 23 dicembre 1993, n. 547*

costoro, contatti con utenze caratterizzate dal codice 899). Qual è il dubbio di questa sentenza? E' che non si capisce se per il giudice questo accesso sia stato quello di entrare nella centralina telefonica ovvero sia stato l'accesso al sistema. Vi è un po' di confusione.
[Sez. V, sent. n. 11689 del 06-02-2006 (ud. del 06-02- 2006), C.V. (rv. 236221)]

Definizione di sistema informatico data nel 1999 dalla Cassazione
Deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella *legge 23 dicembre 1993 n. 547*, che ha introdotto nel codice penale i cosiddetti "computer's crimes", un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate per mezzo di un'attività di "codificazione" e "decodificazione" dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata e immune da errori logici. Nella specie, è stata ritenuta corretta la motivazione dei giudici di merito che avevano riconosciuto la natura di "sistema informatico" alla rete telefonica fissa sia per le modalità di trasmissione dei flussi di conversazioni sia per l'utilizzazione delle linee per il flusso dei cosiddetti "dati esterni alle conversazioni" in un caso in cui erano stati contestati i reati di accesso abusivo a sistema informatico (*art. 615-ter c.p.*) e di frode informatica (*art. 640-ter cod. pen. Sez. VI, sent. n. 3067 del 14-12-1999 (ud. del 04-10-1999), Piersanti (rv 214945).* Secondo questa definizione di sistema informatico stabilire che cosa sia o meno un sistema informatico spetta soltanto al giudice di merito, (tribunale, corte d'appello, etc.) in quanto vedere se questo mix di hardware e software è tale da consentire un'individuazione del sistema informatico è una valutazione di fatto. Passiamo ora a definire il concetto di "accesso". Nella prassi quotidiana si parla di "accesso al sistema" quando l'utente si connette da remoto ad un elaboratore ovvero quando lo utilizza localmente. Tutta la terminologia usata dal legislatore risente però dell'analogia con la violazione di domicilio. Ciò causa qualche problema.

4) Un altra fattispecie criminosa ci viene data dall'art 615-quater c.p ***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*** che cosi testualmente recita:
"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 sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma *dell'articolo 617-quater*[2]" . Questa fattispecie è caratterizzata dal procurare a se un profitto o recare ad altri un danno (abusivamente cioè se si procura questo mezzo per accedere in modo non legato ad una posizione che gli consente di farlo). In tema di criminalità informatica, l'art. 615 quater c.p. si applica anche all'ipotesi di detenzione o diffusione abusiva delle pics-card, schede informatiche che consentono di vedere programmi televisivi criptati attraverso al decodificazione di segnali trasmessi secondo modalità tecniche di carattere telematico. Nello specifico tratteremo sia questa fattispecie criminosa sia quella in materi di clonazioni di cellulari.
Esaminiamo ora la fattispecie in materia di clonazioni di cellulari. Questo reato è importante perché l'acquisizione di codici ci consente di accedere a dei sistemi informatici.
Cassazione Penale *Elemento materiale del reato e fattispecie (clonazione cellulari)*

[2] Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

Secondo la cassazione nel 2003 tale fattispecie integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici (*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 un'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") integra il delitto di ricettazione (*art. 648 c.p.*), di cui costituisce reato presupposto quello ex *art. 615-quater c.p.* Quindi anche fattispecie criminali note come la ricettazione acquisiscono la loro movenza particolare in questo campo. Il cittadino non sempre pensa alla rete mobile quando interagisce con i sistemi informatici. (*Sez. II, sent. n. 36288 del 22-09-2003 (ud. del 17-01-2003), De Alfieri (rv 226699),* **in senso conforme** *Sez. II, sent. n. 5688 del 14-02-2005 (ud. del 17-12-2004) (rv 230693).*
Può capitare che la suprema Corte di Cassazione che annovera tra le sue funzioni quella di nomofilachia cioè di cura di una uniforme interpretazione della legge, abbia delle decisioni discordanti sulla legge stessa. E' evidente che per errore può succedere ma anche scientemente può succedere ma può ripensarci e ribaltare le decisioni prese in precedenza. Nel caso in cui ciò succede, è previsto che il caso si ripresenti, allora decideranno sul merito le sezioni unite (sono una particolare configurazione della Suprema Corte di Cassazione formate da un numero congruo di componenti che provengono da diverse sezioni)

Cassazione Penale *Elemento materiale del reato e fattispecie (pic card per pay-tv)*
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 della *legge n. 248 del 2000* che invece concerne la tutela del diritto di autore, con la conseguenza che tra le due previsioni non sussiste alcun rapporto di specialità. *Sez. V, sent. n. 24847 del 27- 06-2002 (cc. del 29-05-2002), Mammoliti (rv 222064).*
Che cosa significa tutto ciò?. In pratico un soggetto si procura un card e si vede un film. Da un lato forse ha compiuto un accesso ad un sistema informatico e telematico protetto, dall'altro ha lucrato ai danni di colui che detiene i diritti d'autore un uso a gratis di questo film che ha visto. Nel caso di specie la cassazione dice si al primo e no al secondo ossia si al reato di detenzione abusiva di codici di accesso ai sistemi informatici e telematici e no a quell'altro.
SENTENZA CONTRARIA:
Non configura il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (*art. 615-quater c.p.*) il possesso di un decodificatore di segnali satellitari e di schede per la ricezione degli stessi (cosiddette "Pic-card" o "Smart-card"), **atteso che con tali strumenti non si viola alcun domicilio informatico**, protetto da misure di sicurezza, ma si utilizzano irregolarmente servizi di trasmissione o comunicazione ad accesso condizionato, contravvenendo in tal modo alle disposizioni sul diritto d'autore di cui all'art. 6 del D.Lgs. 15 novembre 2000, n. 373, sanzionato solo in via amministrativa prima dell'entrata in vigore della legge 7 febbraio 2003, n. 22. (Sez. V, sent. n. 22319 del 20-05-2003 (cc. del 16-04- 2003), Amuso (rv 225394). Quindi come vediamo sono due sentenze che dicono esattamente il contrario in quanto probabilmente ci vorrà un po' di tempo perché venga compreso appieno che cos'è il sistema informatico e telematico. In realtà è auspicabile che i crimini informatici siano necessariamente da reprimere e stroncare nel senso niente querela di parte, obbligo di azione penale etc. Per cui il reato si considera commesso laddove si verifica l'evento, nel caso di fattispecie criminosa di furto di identità digitale. Uno dei primi casi di computer 's crimes è stata quella di una dipendente delle poste italiana, la quale mobbizzata per anni, una volta collocata in pensione è entrata nel sistema amministrativo delle poste ed ha volontariamente diminuito gli stipendi dei suoi dirigenti. Secondo i criminologi esistono due binari

secondo i quali si regge il rispetto di una norma e cioè i cosiddetti freni inibitori interni (il fatto che si consideri che questo è male), in assenza la durezza della repressione.

5) Un altro reato è quella della ***diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*** normata dall' art. 615 *quinquies* c.p.[3] che cosi testualmente recita: "Chiunque diffonde, comunica o consegna un programma informatico (da lui stesso o da altri redatto) avente per scopo o per effetto il danneggiamento (art. 635 bis c.p.) di un sistema informatico o telematico o dei dati e programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329."
Facciamo ora un breve excursus normativo su quelli che sono definiti i programmi maligni. Per malware che corrisponde alla contrazione in inglese di malicious software (programma malvagio) intendiamo dei programmi che hanno come scopo precipuo quello di danneggiare un pc ovvero di interromperne, alterarne o rallentarne il funzionamento, ovvero di cancellarne una parte della memoria o ancora di cagionare la perdita di dati, informazioni e programmi conservati all'interno di un qualsivoglia sistema informatico. Il virus è un software che una volta mandato in esecuzione, è in grado di infettare un pc e di autoriprodursi, facendo copie di se stesso, replicandosi senza che l'utilizzatore del sistema contaminato riesca il più delle volte, a rilevarne l'indesiderata presenza. I worms sono dei programmi maligni che traggono giovamento dalla integrazione delle reti. Tipico è il caso dei c.d. worm (letteralmente verme), malware che modifica il sistema aggredito in modo da essere eseguito automaticamente. Esso si replica sfruttando per lo più su internet tant'è che viene in genere trasportato attraverso messaggi di posta elettronica, venendo allocato nei c.d. "attachment" o allegati. Tra i più famosi nonché pericolosi worms si annoverano Nimda che è entrato in azione una settimana dopo i tragici eventi dell'11 settembre 2001, infettò 8.300.000 pc e provocò danni stimati in circa 650 milioni di dollari. Oltre a virus e worm, tra i programmi maligni è opportuno menzionare gli spyware, i trojan horse, le logic bomb e i web dialer. Lo spyware è un tipo di programma che raccoglie informazioni riguardanti l'attività on line di un utente (ad esempio siti visitati, acquisti eseguiti in rete, etc,). La maliziosità di tale software sta nel fatto che tali informazioni vengono carpite senza che l'utente stesso ne sia informato preventivamente e dunque senza il consenso di lui. Lo spyware poi, una volta acquisiti i dati e le notizie utili, provvederà a inoltrarli ad un database gestito quasi sempre da organizzazioni commerciali, che sfrutteranno quei dati e quelle notizie per trarne profitto. Dunque uno spyware viene realizzato non con il fine di danneggiare un sistema (anzi l'attività di reperimento di informazioni ne presuppone l'integrità) bensì per violare la privacy del cibernauta.

Passiamo ora ad esaminare l'analisi del reato ex art. 615 quinquies c.p dove il soggetto attivo del reato è chiunque ergo trattasi reato comune. Il reato comune è quello che non è proprio di una certa categoria di persona e si rivolge a chiunque (sono reati tipici dei pubblici ufficiali). Per cui il presupposto oggettivo è la nozione di sistema. Mentre nel delitto di cui al 615 ter era necessario che il sistema sia protetto, per questo reato non è necessario che il sistema sia protetto. Quanto alla nozione di sistema ci si può rifare alla definizione sopra vista a proposito del delitto di cui all'art. 615 ter c.p. Va aggiunto che mentre ai fini della configurabilità del delitto di cui all'art.615 ter c.p. è necessario che il sistema sia protetto da misure di sicurezza (ergo la forzatura o aggiramento delle stesse è elemento costitutivo del reato), ciò non è invece richiesto per il delitto di cui all'art.615 quinquies c.p., che dunque tutela ogni forma di sistema informatico, protetto o meno. Varie sono le condotte punibili, consistenti nel: **consegnare**, cioè dare materialmente un supporto (per es. un C.D.R., un floppy-disk) contenente un malware; **comunicare**, cioè portare a conoscenza di un soggetto ovvero di un numero determinato di persone le informazioni o le idee alla base del programma maligno, indipendentemente dalle modalità con le quali avviene la comunicazione

[3] Articolo aggiunto dall'*art. 4, L. 23 dicembre 1993, n. 547*

stessa (direttamente tra persone con lo scambio "fisico" di supporti ovvero on-line, con la trasmissione da un sistema a uno o più sistemi diversi); **diffondere**, cioè divulgare, comunicare a più persone indiscriminatamente ovvero a un numero imprecisato di soggetti o di sistemi (secondo ampia parte della dottrina si è in presenza sostanzialmente di più "comunicazioni", in realtà, invece, "diffondere" vuol dire "contagiare"). Diffondere viene inteso come la possibilità di diffondere il virus a più persone. Passiamo ora ad analizzare l'elemento soggettivo del reato. Il delitto de quo è delitto (solo) doloso e precisamente a dolo generico (cioè non interessa che cosa voglia fare il soggetto con la diffusione di questo virus interessa che semplicemente abbia divulgato il virus in maniera consapevole e cosciente), a prescindere dunque dal movente (ludico-vandalico, emulativo, estorsivo, terroristico…), che spinge l'"*infettatore*" informatico ad agire, essendo sufficiente la consapevolezza e la volontà di diffondere, comunicare e consegnare il programma e la consapevolezza degli effetti che esso può produrre. Attualmente la giurisprudenza si è orientata nel senso suddetto, ossia che ad integrare il coefficiente minimo di colpevolezza del delitto di cui all'art.615 quinquies c.p. sia sufficiente il dolo generico [4]. Quanto alla **procedibilità**, il delitto di cui all'art.615 quinquies c.p. è procedibile d'ufficio perché il bene che viene tutelato non è quello del soggetto che riceve il danno quanto quello della sicurezza della trasmissione dei dati.

6) Un altro reato informatico è quello inerente il ***danneggiamento di sistemi informatici o telematici*** normato dall'art. 635 bis c.p. [5] che cosi testualmente recita: "Chiunque distrugge, deteriora o rende, in tutto o 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. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni." A norma di tale articolo viene punito chiunque distrugga, deteriori, renda inservibili in tutto o in parte sistemi informatici o telematici altrui oppure dati, programmi e informazioni di terzi. Esaminiamo ora l'interpretazione giurisprudenziale data dalla Cassazione Penale. Antecedentemente all'entrata in vigore della legge 23 dicembre 1993 n. 547 (in tema di criminalità informatica), che ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer, in modo tale da renderne necessaria la creazione di nuovi, configurava un'ipotesi di danneggiamento ai sensi dell'art. 635 cod. pen. in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore. (*Sez. U., sent. n. 1282 del 13-12-1996 (cc. del 09-10- 1996), Carpanelli (rv 206844).* La Corte di Cassazione con tale sentenza ha precisato che tra il reato di cui all'art. 635 c.p. e l'analoga speciale fattispecie criminosa prevista dall'art. 9 legge n° 547 del 1993, la quale ha introdotto l'art. 635bis c.p. sul danneggiamento di sistemi informatici e telematici, esiste un rapporto di successione di leggi nel tempo, disciplinato dall'art. 2 c.p. Questo articolo 635 bis è un caso di ostruzionismo del legislatore perché il danneggiamento (art. 635) prevedeva che si danneggiasse qualcosa di materiale mentre il software non è materiale. Però la cassazione ci dice che evidentemente per punire qualcuno che aveva compiuto qualcosa prima del 1993, danneggiare il software rendeva inutilizzabile l'hardware per cui era una forma di danneggiamento dell'hardware.

7) Un altro reato informatico è quello relativo alla ***frode informatica*** normato dall'art. 640 ter c.p. [6] che cosi testualmente recita: "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. La pena è della reclusione da uno a cinque anni e della multa da euro

[4] si veda Trib. Bologna Sez. I Pen., sent. 21 Luglio 2005

[5] Articolo aggiunto dall'art. 9, L. 23 dicembre 1993, n. 547.

[6] Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547.

309 a euro 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. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante .” Si può notare che nella fattispecie semplice, cioè nella quale non ricorrono aggravanti, la sanzione è piuttosto modesta (è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032). Per una cosa molta grave, invece, il danno anche qui si procede a querela di parte (la querela della persona offesa potrebbe non venire mai perché il danno per la persona offesa potrebbe essere maggiore se si affronta il cosiddetto streptus fori (cioè si viene a sapere) che non quello che ha subito. Passiamo ora ad esaminare il momento consumativo del reato secondo la Cassazione Penale.
Il reato di frode informatica (art. 640-ter cod. pen.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa (la truffa funziona in questo modo io raggiro una persona ed ottengo un vantaggio per me ed un danno per la persona raggirata) dalla quale si differenzia solamente 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. Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui. Nella specie, l'agente, utilizzando il sistema telefonico fisso installato in una filiale della società italiana per l'esercizio telefonico, con la veloce e ininterrotta digitazione di numeri telefonici, in parte corrispondenti a quelli per i quali il centralino era abilitato e in parte corrispondenti a utenze estere, riusciva ad ottenere collegamenti internazionali, eludendo il blocco predisposto per le chiamate internazionali per le quali il sistema non era abilitato, così esponendo debitoriamente la società italiana per l'esercizio telefonico nei confronti dei corrispondenti organismi esteri autorizzati all'esercizio telefonico. (Sez. VI, sent. n. 3065 del 14-12-1999 (ud. del 04-10-1999), De Vecchis (rv 214942).

8) Altra fattispecie criminosa è quella concernente la ***violazione, sottrazione e soppressione di corrispondenza*** normata dall’art. 616 c.p. che cosi testualmente recita:” 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 prendere 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 euro 30 a euro 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 tre anni. Il delitto è punibile a **querela della persona offesa**. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, **informatica o telematica**, ovvero effettuata con ogni altra forma di comunicazione a distanza [7].” Tale norma punisce chiunque prenda cognizione del contenuto di una corrispondenza chiusa a lui non diretta, ovvero sottragga o distrugga una corrispondenza chiusa o aperta a lui non diretta (anche informatica o telematica). In tale fattispecie criminosa oggetto della tutela penale non è il segreto, che eventualmente sarà affidato alla corrispondenza, ma la corrispondenza in sé, la quale è dalla legge per se stessa ritenuta segreta indipendentemente cioè dalla segretezza o non segretezza del suo contenuto. A tal proposito si veda *Cass., 10 luglio 1997, Realai, CP 98, 1378 nt. Gallucci; invi 98, 2361, nt. Larizza* nella quale la suprema corte ha precisato che è inibito a prendere visione della corrispondenza diretta al coniuge, senza il consenso espresso o tacito di quest’ultimo. Passiamo ora ad esaminare in tale fattispecie criminosa il concetto di giusta causa esaminato dalla cassazione penale. In materia di violazione, sottrazione e soppressione di corrispondenza, la nozione di giusta causa, alla cui assenza l'art. 616, secondo

[7] Comma così sostituito dall'*art. 5, L. 23 dicembre 1993, n. 547*, che modifica ed integra le norme del codice penale e del codice di procedura penale in tema di criminalità informatica. Il precedente testo così disponeva: «Agli effetti delle disposizioni di questa sezione per corrispondenza s'intende quella epistolare, telegrafica o telefonica».

comma, cod. pen., 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. Nel caso in esame la Corte ha ritenuto sussistere la giusta causa relativamente alla rivelazione del contenuto della corrispondenza del coniuge in un giudizio civile di separazione. (Sez. V, sent. n. 8838 del 01-10-1997 (cc. del 10-07-1997), Reali (rv 208613).

9) Un altro reato informatico è quello inerente ***l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*** normata dall'art. 617 quater c.p. [8] che cosi testualmente recita: "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 si 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 di 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 del sistema;

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

Tale norma punisce chiunque fraudolentemente intercetti, impedisca o interrompa comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, nonché mediante qualsiasi mezzo di informazione al pubblico ne riveli il contenuto. L'interesse tutelato dalla norma è chiaramente la riservatezza delle comunicazioni e la libertà e regolarità delle stesse che devono essere libere, complete e senza interruzioni. Com' è ovvio la particolarità del mezzo informatico non incide sul fine delle comunicazioni telematiche, che è comunque la trasmissione di dati tra soggetti in forma riservata. In proposito, sembra opportuno segnalare che tale previsione è il luogo parallelo informatico di quanto già previsto per le comunicazioni e conversazioni telefoniche o telegrafiche (art. 617), stante il fatto che il concetto di "intercettazione", assunto nell'art. 617 quater, corrisponde a "presa di cognizione della comunicazione" di cui all'art. 617. Un esempio di tale fattispecie criminosa ci viene dato ad esempio da un esercizio commerciale che utilizza, mediante un terminale POS in sua dotazione, una carta di credito contraffatta, atteso che il titolare dell'esercizio commerciale è ben legittimato ad utilizzare il POS e l'accesso abusivo genera un flusso di informazioni ai danni del titolare della carta contraffatta diretto all'addebito sul suo conto della spesa fittiziamente effettuata (*si veda Cass. Sez. V, 14 ottobre 2003 – 19 novembre 2003, n° 44362, CED 227253; CP 05, 1580, nt. Aterno*)

10) Altra fattispecie criminosa è quella concernente ***l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche*** normata dall'art 617 quinquies c.p. [9] che cosi testualmente recita:" Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad 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'articolo 617-quater." Tale norma punisce chiunque fuori dai casi consentiti dalla legge installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi. La circolazione internet di reti

[8] Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.

[9] Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.

wireless si configura in questa fattispecie criminosa. Altro esempio ci viene dato secondo la cassazione (Cass., sez V, 5 dicembre 2006 – 30 gennaio 2007, n° 3252, CED 236035) dall'installazione di una fotocamera digitale su un "postamat" di un ufficio postale.

11) Un altro reato è quello della ***falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche normato*** dall'art. 617 sexies c.p. [10] che cosi testualmente recita: "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'articolo 617-quater* ." Tale norma punisce chiunque al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, formi falsamente, alteri o sopprima in tutto o in parte il contenuto (intercettato anche occasionalmente) di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.
12) Altra fattispecie criminosa è quella della ***falsità informatica*** normata dall'art. 491 bis c.p. [11] che cosi testualmente recita : "Se alcuna delle falsità previste dal 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 per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.". Con tale articolo si equipara il supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi al documento cartaceo ai fini delle disposizioni sulle falsità documentali relative agli atti pubblici ed alle scritture private. Infatti l'archivio informatico di una pubblica amministrazione deve essere considerato alla stregua di un registro tenuto da un soggetto pubblico, con la conseguenza che la condotta del pubblico ufficiale che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici della pubblica amministrazione, confezioni un falso atto informatico destinato a rimanere nella memoria dell'elaboratore , integra una falsità in atto pubblico, a seconda dei casi, materiale o ideologica. In ordine alla falsità degli atti, essa può essere di due forme: la falsità materiale, ossia la non genuinità del documento e la falsità ideologica, ossia la non veridicità dello stesso. Si ha dunque falsità materiale quando "vi è una divergenza tra autore apparente e autore reale del documento o quando quest'ultimo è stato alterato successivamente alla sua formazione"; si ha falsità ideologica quando "il documento contiene attestazioni o dichiarazioni non veritiere".

Documento informatico: orientamento giurisprudenziale
Circa la nozione penale di "documento informatico", anzitutto, non sono mancate le critiche di una parte della dottrina circa la scelta legislativa di introdurre nell'ordinamento penale la prima definizione di documento informatico. L'art 3 della l. 547/93 comunque, ha introdotto un primo concetto di documento informatico, ma è con il DPR 513/97, successivamente confluito nel DPR 445/2000, ("Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa") che il legislatore ha offerto una completa e più idonea definizione di documento informatico, come "la rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti" (art.1); inoltre l'art. 8 del d.p.r citato, stabilisce l'efficacia legale del documento informatico prodotto in ottemperanza alle disposizioni dello stesso D.P.R. Il legislatore del '93 con l'art. 491 bis non si è limitato solo a disporre che alle alterazioni delle registrazioni informatiche si applicano le stesse pene previste per i documenti pubblici o privati, ma ha addirittura aggiunto che "se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizione del capo stesso concernenti rispettivamente gli atti pubblici e le scritture

[10] Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.
[11] Articolo aggiunto dall'art. 3, L. 23 dicembre 1993, n. 547

private". In altre parole, la registrazione informatica dei dati deve essere considerata una forma di scrittura e non un *tertium genus*.

13) Un altro reato informatico è rappresentato dalle altre ***comunicazioni e conversazioni*** normato dall'art. 623 *bis* c.p. che cosi testualmente recita: "Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati."
L'art. 623 *bis* c.p. assimila le comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche a qualunque altra trasmissione a distanza di suoni, immagini o altri dati.

Altri crimini informatici sono stati introdotti dalla legislazione speciale. Ad esempio:
1. l'art. 4 della Legge 13 dicembre 1989 n. 401 (Svolgimento di attività organizzata per l'accettazione e la raccolta, anche per via telefonica e telematica, di scommesse o per favorire tali condotte in assenza di concessione, autorizzazione o licenza);
2. la Legge 3 agosto 1998 n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù);
3. la Legge 18 agosto 2000 n. 248 (Norme di tutela del diritto di autore) e successive modificazioni;
4. l'art. 12 del d.l. n. 143 del 1991 (Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante);
5. il D.lgs 30 giugno 2003, n.196 (Codice in materia di protezione dei dati personali).