LA CRIMINALITA' INFORMATICA IN ITALIA

di Avv. Francesco Albanese e Avv. Valentina Privitera

La diffusione sempre più massiccia della tecnologia informatica in ogni settore e campo che investe l'agire umano in uno con l'utilizzo quasi "compulsivo" dei mezzi di comunicazione su rete e digitali, impone all'operatore del diritto, allorquando deve confrontarsi con addebiti penali mossi a seguito della violazione della normativa di settore, di aggiornarsi ed approfondire – anche sotto un profilo prettamente tecnico fuori campo - la vigente Legislazione in materia di "criminalità informatica" (c.d. «*computer crimes*») .

Le norme incriminatrici introdotte al fine di garantire una repressione efficace dei comportamenti ritenuti offensivi di beni di rilevanza costituzionale, sono compendiate nel Codice Rocco e trovano la loro fonte di impulso all'emanazione nella Legislazione Internazionale e Comunitaria.

Il presente lavoro è finalizzato a fornire un'analisi ed una descrizione delle principali caratteristiche dei reati in materia informatica vigenti in Italia, con brevissimi cenni alla normativa transnazionale e sovranazionale che li ha preceduti.

I dubbi interpretativi che l'applicazione pratica delle fattispecie pone quotidianamente all'operatore del diritto sono direttamente correlati all'espansione massiccia dei mezzi informatici ed al loro continuo progredire in termini di evoluzione scientifica.

Non può che derivarne una evidente complessità in sede processuale di accertamento della penale responsabilità dell'indagato/imputato senza l'ausilio di consulenti e/o periti esperti informatici, con ovvie ricadute in punto di difficoltà pratica, anche al momento della decisione, nella ricostruzione dell'iter psicologico seguito dall'agente all'atto della realizzazione della condotta, ai fini della verifica giudiziale della sua colpevolezza.

Il nesso psichico dell'agente risulterà tanto più affievolito quanto maggiormente complessa sarà la problematica tecnico giuridica-informatica sottesa alla esatta individuazione del momento consumativo ovvero del semplice tentativo del delitto e, prima ancora, alla precisa identificazione della soglia del consentito e del lecito penalmente.

Nell'affrontare la tematica della criminalità informatica non può prescindersi dal menzionare la Raccomandazione del Consiglio d'Europa del 13.9.1989 n. r (89) 9. Essa è il punto di riferimento fondamentale per la materia nel campo del diritto internazionale e derivava dalla necessità che i diversi Paesi che ne fanno parte aderissero ad una politica legislativa uniforme per i pericoli derivanti dalla presenza di c.d. «paradisi informatici» e che instaurassero una stretta collaborazione per la repressione della criminalità informatica sovente a carattere sovranazionale che, di regola, richiede la previsione bilaterale del fatto (*c.d. doppia incriminazione*).

Essa suggerisce alle Nazioni aderenti una lista dei reati informatici ripartiti in due gruppi:

un primo gruppo (la c.d. «lista minima»), comprende fattispecie la cui incriminazione, in virtù della loro diffusione e gravità, è ritenuta necessaria;
un secondo gruppo (la c.d. «lista facoltativa»), riguarda, invece, le condotte da incriminare sulla base della discrezionalità rimessa a ciascun Paese aderente.
I punti nodali riguardano previsioni di diritto penale sostanziale con oggetto una vasta gamma di fattispecie punibili e di diritto processuale penale, con inferenza anche alla disciplina in materia di protezione dei dati personali.
Merita particolare attenzione l'introduzione della Responsabilità penale delle Persone Giuridiche per gli illeciti tipizzati dal testo dell'Accordo.
Il Legislatore Italiano con il D.Lgs 231/2001 in materia di «*Responsabilità amministrativa delle società e degli Enti*» aveva già previsto dettagliatamente specifici criteri di imputazione di fatti di reato ai soggetti collettivi, la Convenzione, tuttavia, estende il novero delle norme incriminatrici riferibili agli Enti.
Rilevante in tema è anche l'attività dell'Unione Europea che, valorizzando al massimo la propria specificità di azione e, pur in assenza di una base normativa nel Trattato di Maastricht del 1992, si è distinta in tema di criminalità informatica, attraverso l'adozione di strumenti atipici quali *programmi di azione* ed *altri documenti programmatici di varia natura*, favorendo la *cooperazione giudiziaria* ed il *ravvicinamento delle normative penali di settore*.
Si segnala l'adozione dei recentissimi atti quali: la Risoluzione del Parlamento Europeo «*Lotta contro la Criminalità Informatica*» del 3.10.2017 e l'VIII Relazione della Commissione Europea del 29.6.2017 sui «*Progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza e invito ad accelerare le iniziative miranti a rafforzare la sicurezza dei cittadini dell'UE attualmente in corso*».
Quanto alla normativa italiana di settore, essa è compendiata nella Legge 23.12.1993, n. 547 (G.U. n. 305 del 30.12.1993), recante «*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*»: il Legislatore ha adeguato la normativa italiana a quella dei Paesi con Legislazione avanzata. Essa contempla quasi tutte le forme di aggressione informatica individuate dal Consiglio d'Europa nella Raccomandazione del 13.9.1989 n. R (89) 9; nonché nella Legge 18.3.2008, n. 48 (G.U. n. 80 del 4.4.2008), recante la «*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*», a mezzo della quale vengono introdotte significative modifiche al Codice Penale, al Codice di Procedura Penale, al D.Lgs 8.6.2001, n. 231 (*Responsabilità amministrativa delle società e degli enti*) ed al D.Lgs 30.6.20013, n. 196 (*Codice Privacy*). Le novità più rilevanti riguardano: sanzioni più gravi per i reati informatici; norme di contrasto più efficace alla pedopornografia in rete; sanzioni anche a carico delle società; possibilità per le forze dell'ordine di chiedere al *provider* il congelamento dei dati telematici per sei mesi; maggiori tutele per i dati personali.

«ESERCIZIO ARBITRARIO DELLE PROPRIE RAGIONI CON VIOLENZA SULLE COSE», ex art. 392 c.p.

La norma è collocata nel Libro II – Dei delitti in particolare; Titolo III – Dei delitti contro l'amministrazione della giustizia; Capo III - **Della tutela arbitraria delle private ragioni.**

Il II comma della norma è stato aggiunto dall'art. 1, L. 23.12.1993, n. 547.

Con riferimento alla natura giuridica del reato, siamo in presenza di un reato comune, di danno, di evento, a forma vincolata.

Il soggetto attivo del reato può essere «chiunque» e, pertanto, è «reato comune»; l'agente può essere il titolare del diritto preteso o anche una persona che sia legittimata ad agire per conto del titolare. Qualora tuttavia quest'ultimo, la cui condotta sarebbe inquadrabile *ex* art. 110 c.p., inizi ad agire in piena autonomia per il perseguimento di propri illeciti interessi, tale comportamento integra gli estremi del reato di estorsione *ex* art. 629 c.p.

L'oggettività giuridica è l'interesse pubblicistico a garantire il monopolio dell'autorità giudiziaria nella soluzione delle dispute fra i portatori di pretese in conflitto (secondo parte della dottrina); è il possesso dei diritti, inteso come lo stato di fatto per il quale una persona si trova nella possibilità di esercitare il contenuto di un qualsiasi diritto (secondo parte della dottrina); è l'interesse del privato al pacifico godimento dei propri rapporti giuridici connesso con l'interesse al processo (secondo parte della dottrina).

La violenza in ambito informatico, quale esercizio arbitrario delle proprie ragioni, è disciplinata dal comma III dell'art. 392 c.p., introdotto dalla Legge 23.2.1993, n. 547, poiché sulla scorta del precedente testo normativo era in dubbio se i «programmi» e i «dati informatici» rientrassero nel concetto di «cosa» ai sensi delle tradizionali forme di esercizio arbitrario delle proprie ragioni.

Quanto alla condotta incriminata, alla meta condotta, al presupposto od al requisito subiettivo della condotta: trattasi del «farsi arbitrariamente ragione da sé» che deve intervenire mediante violenza sulle cose; si ha «violenza sulle cose» allorchè la cosa viene danneggiata o trasformata o ne è mutata la destinazione; la cosa viene «danneggiata» quando è distrutta, dispersa o deteriorata; è «trasformata» quando è materialmente modificata, anche se in senso migliorativo; ne è «mutata la destinazione» quando vi è una mutazione in termini *oggettivi* o anche quando vi è un mutamento di destinazione *soggettiva* nei confronti di chi ne aveva la disponibilità o l'utilizzabilità; il comportamento incriminato consiste nel farsi ragione da sè medesimo ovverosia nella c.d. «autosoddisfazione» che deve essere arbitraria; è lecita la «violenza manutentiva» diretta a mantenere il possesso attuale nonché la «violenza reintegrativa» diretta a recuperare il possesso nell'immediatezza dello spoglio; oltre la condotta di autosoddisfazione arbitraria posta in essere mediante violenza sulle cose, deve essere presente il requisito della «possibilità di ricorrere al giudice», quale mera possibilità di fatto, indipendentemente dalla ammissibilità dell'azione esercitata ovvero quale possibilità giuridica, attivando un diritto suscettivo di effettiva realizzazione

giudiziale; per «giudice» si intende qualsiasi Autorità Giudiziaria in sede contenziosa, sia essa civile, che penale o amministrativa.
Si ha «violenza sulle cose» nell'ambito informatico allorchè 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 (ipotesi di c.d. legge mista alternativa, per cui il reato rimane unico anche se tali modalità della condotta vengono poste in essere tutte)
E' "programma informatico" l'insieme di istruzioni in base alle quali il *computer* opera. Tale programma viene «alterato» quando se ne modifichi l'essenza, facendone perdere la funzionalità originaria; è «modificato» quando sono mutati gli elementi del programma, in modo tale da non fare raggiungere gli obiettivi del programma; è «cancellato» quando vengono soppresse le informazioni che compongono il programma.
E' "sistema informatico" quel sistema di trattamento automatico delle informazioni mediante mezzi elettronici (es. *personal computer*, apparecchi automatici quali fotocopiatrici e apparecchi telefonici funzionanti con carte a banda magnetica, carte a microprocessore).
E' "sistema telematico" la connessione a distanza tra più elaboratori, come nel caso di *Internet*.
Ai fini del reato, il funzionamento di un sistema informatico o telematico è «impedito» quando siano stati disattivati i collegamenti elettrici del *computer*; il funzionamento di un sistema informatico o telematico è invece «turbato» quando vi è un'azione di disturbo al regolare funzionamento dell'elaboratore.
Circa l'elemento soggettivo del reato, esso deve rintracciarsi nel dolo specifico rappresentato dal «fine di esercitare un preteso diritto» (secondo parte della dottrina e la giurisprudenza concorde); ovvero nel dolo generico, quale coscienza e volontà del fatto tipico, poiché il «fine di esercitare un preteso diritto» non è un *quid* che sta al di là del fatto che ne costituisce il reato (secondo altra parte della dottrina).
La consumazione del reato sarebbe da identificarsi nel momento e nel luogo nel quale l'agente pone in essere la condotta violenta finalizzata al farsi ragione da sé (secondo parte della dottrina) ovvero nel momento e nel luogo in cui l'agente si fa ragione da sè medesimo (secondo altra parte della dottrina).
Il tentativo è ritenuto ammissibile e si configura in tutti i casi nei quali la condotta di autosoddisfazione non consegue l'obiettivo preso di mira per cause estranee all'agente.
L'interpretazione giurisprudenziale sotto segnalata, sebbene datata, risulta tutt'oggi vigente nei principi di diritto *illo tempore* espressi.
TRIBUNALE DI TORINO, SENTENZA DEL 12.12.1983, aveva ritenuto responsabile del reato *ex* art. 392 c.p. il dipendente di una *software house* (azienda specializzata principalmente nella produzione di *software* e applicazioni - es. i programmi per p.c.) che, a seguito di un contrasto con i titolari della medesima, aveva ritenuto di sottrarre all'azienda uno dei programmi da lui stesso realizzati e concessi in uso a quest'ultima, costituente uno dei moduli centrali di un più complesso *software* gestionale, inutilizzabile senza tale elemento.

PRETURA DI TORINO, SENTENZA DICEMBRE DEL 1989, aveva ritenuto sussistere il reato ex art. 392 c.p. a seguito dell'operazione di cancellazione dei dati memorizzati su un sistema informatico da parte di un dipendente entrato in contrasto con l'azienda, individuando l'oggetto del reato nel sistema informatico costituito dall'insieme dell'*hardware* e del *software*, divenuto inutilizzabile per effetto della cancellazione dei programmi e dei dati, poichè detta cancellazione ben poteva essere considerata un'ipotesi di danneggiamento materiale equiparabile alla medesima operazione ottenuta mediante abrasione o alterazione chimica di una scritta su un foglio di carta.
PRETURA DI TORINO, SENTENZA DEL 15.5.1996, stabiliva che deve ritenersi violenza sulle cose, tale da integrare l'elemento della fattispecie di cui all'art. 392 c.p., il comportamento di un soggetto il quale, al fine di esercitare un preteso diritto di esclusiva per l'installazione e gestione delle componenti informatiche di macchinari industriali, aveva alterato surrettiziamente il programma di propria produzione installato sugli stessi, inserendo un file di "blocco data" in grado di interrompere automaticamente il funzionamento del macchinario - rendendolo del tutto inservibile - alla scadenza della data prestabilita.

«DOCUMENTI INFORMATICI», ex art. 491-*bis* c.p.
La norma è collocata nel Libro II - Dei delitti in particolare; Titolo VII - Dei delitti contro la fede pubblica; **Capo III - Della falsità in atti.**
E' la fattispecie di falso (materiale e ideologico) in documenti informatici pubblici aventi efficacia probatoria.
L'articolo aggiunto dall'art. 3, L. 23.12.1993, n. 547, modificato dall'art. 3, L. 18.3.2008, n. 48 e, successivamente, così sostituito dall'art. 2, 1° co., lett. e), D.Lgs. 15.1.2016, n. 7, a decorrere dal 6 febbraio 2016, recante «*Disposizioni in materia di abrogazione di reati e introduzione di illeciti con sanzioni pecuniarie civili, a norma dell'art. 2, 3° co., L. 28.4.2014, n. 67*») ha eliminato dalla norma il riferimento ai documenti informatici privati ed alle disposizioni concernenti le scritture private, in ragione dell'abrogazione del reato di falso in scrittura privata di cui all'art. 485 c.p.
L'art. 491-*bis* c.p. è stato introdotto allo scopo di estendere la tutela della fede pubblica ai falsi riguardanti documenti informatici, che hanno caratteristiche particolari e differenti rispetto ai falsi che hanno ad oggetto documenti esclusivamente cartacei.
Vi è un'equiparazione del documento informatico agli atti pubblici e alle scritture private, ai soli fini della applicabilità delle disposizioni sulle falsità in atti di cui al Capo III del Libro II del codice (art. 476 c.p. e ss.).
Nell'originaria formulazione normativa era considerato "documento informatico" il «supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Definizione soggetta a critiche poiché ancorava la nozione ad un supporto materiale informatico. Tuttavia, il documento informatico è caratterizzato da un'intrinseca immaterialità.

Nella nozione attuale riformata è considerato "documento informatico" la «rappresentazione di atti, fatti o dati giuridicamente rilevanti». L'attuale definizione prescinde dall'incorporazione dei dati in un oggetto materiale, con conseguente rilevanza penale dei falsi che abbiano ad oggetto informazioni anche non registrate su alcun supporto materiale. La Riforma del 2008 sopprime la definizione penalistica di documento informatico con conseguente implicito rinvio alla nozione di cui all'ordinamento extrapenale (Codice dell'Amministrazione digitale, art. 1, lett. p, D.Lgs 7.3.2005, n. 82, come modificato dal D.lgs. 4.4.2006, n. 159 e ss.mm.ii.).

Il documento informatico rilevante *ex* art. 491-*bis* c.p. deve possedere efficacia probatoria.

Il Codice dell'Amministrazione Digitale individua quattro categorie di documenti informatici, aventi diverso valore probatorio:

1) IL DOCUMENTO SOTTOSCRITTO CON FIRMA ELETTRONICA NON ALTRIMENTI QUALIFICATA:

Definizione: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1, lett. q, D.Lgs. 7.3.2005, n. 82 – C.A.D.).

Valore Probatorio: «soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità» (art. 21, I co., C.A.D.).

Tecnologia: neutra

Esempi: PIN, firma biometrica, UserID e Password.

2) IL DOCUMENTO SOTTOSCRITTO CON FIRMA ELETTRONICA AVANZATA – FEA:

Definizione: insieme di dati in forma elettronica allegati oppure connessi ad un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1, lett. q-*bis*, D.Lgs. 7.3.2005, n. 82 – C.A.D.).

Valore probatorio: efficacia probatoria della scrittura privata *ex* art. 2702 c.c.; è integrata la forma scritta *ad substantiam*, tranne che per i contratti immobiliari di cui dal n. 1 al n. 12 *ex* art. 1350 c.c., salva l'ipotesi di autentica della sottoscrizione (art. 21, II, II-*bis* co., C.A.D.).

Tecnologia: neutra.

Esempi: firma grafometrica su tablet; P.E.C. verso la P.A.

3) IL DOCUMENTO SOTTOSCRITTO CON FIRMA ELETTRONICA QUALIFICATA:

Definizione: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1, lett. r D.Lgs. 7.3.2005, n. 82 – C.A.D.).

Valore probatorio: efficacia probatoria della scrittura privata *ex* art. 2702 c.c.; è integrata la forma scritta *ad substantiam* (art. 21, II, II-*bis* co., C.A.D.).

Tecnologia: non neutra; certificato qualificato e dispositivo sicuro.
Esempi: smart – card, token USB;
4) IL DOCUMENTO SOTTOSCRITTO CON FIRMA DIGITALE:
Definizione: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, lett. s D.Lgs. 7.3.2005, n. 82 – C.A.D.).
Valore probatorio: efficacia probatoria della scrittura privata *ex* art. 2702 c.c.; è integrata la forma scritta *ad substantiam* (art. 21, II, II-*bis* co., C.A.D.).
Tecnologia: non neutra; certificato qualificato, chiavi asimmetriche e dispositivo sicuro.
Esempi: Smart-card, token USB, MicroSD, Firma remota.
Infine, si segnalano le seguenti massime giurisprudenziali più significative:
CORTE DI CASSAZIONE, SEZ. V, 9.12.2010, N. 10200: La falsificazione della richiesta del rilascio di firma digitale integra il reato di cui agli artt. 483, 491-bis, trattandosi di attività diretta alla P.A, ed assimilabile alla richiesta di un certificato o autorizzazione amministrativa;
CORTE DI CASSAZIONE, SEZ. VI, 16.1.2009, N. 7752: La falsificazione di atti contenuti nei supporti del sistema informatico di un ente pubblico integra il reato di falsità materiale in atto pubblico (artt. 476 e 491-bis) anche quando gli stessi siano documentati in forma cartacea (un caso di alterazione nel sistema informatico di un ospedale del contenuto di un referto medico).
CORTE DI CASSAZIONE, SEZ. V, 27.1.2005, N. 11930: con riferimento all'archivio informatico di una P.A. (patronato ENASCO, nel caso di specie), la condotta del p.u. che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici di pertinenza della P.A., confezioni un falso documento informatico destinato a rimanere nella memoria dell'elaboratore, integra una falsità in atto pubblico, punibile rispettivamente ai sensi degli artt. 476 e 479, se posta in essere antecedentemente alla formulazione dell'art. 491- *bis*.

«ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO», ex art. 615-*ter* c.p.
La norma è collocata nel Libro II – Dei delitti in particolare; Titolo XII – Dei delitti contro la persona; Capo III – Dei delitti contro la libertà individuale; **Sezione IV – Dei delitti contro la inviolabilità del domicilio.**
L'articolo è stato aggiunto dall'art. 4, L. 23.12.1993, n. 547.
La natura giuridica del reato è quella di reato comune, di danno, di mera condotta, a forma libera.
In relazione alla protezione penale *ante Lege* 23.12.1993, n. 547 per l'accesso abusivo a sistema informatico o telematico, in assenza nel codice penale di una norma incriminatrice che sanzionasse l'accesso abusivo ai sistemi informatici, la giurisprudenza e la dottrina minoritaria tutelavano i beni giuridici sottesi attraverso

il ricorso a fattispecie delittuose già esistenti: il reato di violazione di domicilio (art. 614 c.p.); il reato di sostituzione di persona (art. 494 c.p.); il reato di intercettazione abusiva di comunicazioni telefoniche e telegrafiche (art. 617 c.p.). La giurisprudenza maggioritaria escludeva che le condotte illecite intrusive di beni informatici potessero essere sussunte, senza compromettere i principi di legalità e di tassatività, nelle fattispecie penali di cui sopra. Analogamente la dottrina maggioritaria, riteneva impraticabili tali operazioni ermeneutiche facenti leva su un'inammissibile ricorso all'analogia e, comunque, su forzature implicanti un prezzo elevato sul piano del principio di legalità, sottolineando la necessità di un intervento chiarificatore del legislatore.

Esistono tesi contrapposte sull'oggettività giuridica della norma. Di seguito vengono riportate le più significative:

I tesi (dottrinale e giurisprudenziale): bene giuridico è il «domicilio informatico» per la collocazione della norma fra i «delitti contro l'inviolabilità del domicilio». Il domicilio informatico deve considerarsi come un'espansione ideale dell'area di rispetto pertinente al soggetto interessato e volto a garantire il diritto di esplicare liberamente qualsiasi attività lecita all'interno del luogo informatico, rappresentando - più che un nuovo bene giuridico - una specificazione dell' «inviolabilità del domicilio» ordinariamente inteso, imposta dalla natura dei luoghi informatici. Lo *jus excludendi* del titolare che caratterizza il «domicilio fisico» si estende anche al «domicilio informatico», indipendentemente dal fatto che il contenuto del sistema abbia o meno carattere personale. La giurisprudenza di legittimità, afferma che la norma tutelando i sistemi informatici e telematici protetti, non mira solo a garantire la «riservatezza» delle informazioni contenute nel sistema, ma l' «intera sfera della personalità del titolare», in tutte le sue possibili esplicazioni, anche di carattere economico-patrimoniale. Il bene giuridico protetto, non concerne semplicemente i contenuti personalissimi dei sistemi informatici ma ricomprende lo *jus excludendi* del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso. Il «domicilio informatico» è costituito dal luogo fisico in cui sono contenuti dati di qualsivoglia natura salvaguardati contro ogni tipo di intrusione, indipendentemente dalle finalità che muovono l'autore dell'abuso. Se ne deduce che il bene tutelato dalla norma sulla violazione di domicilio (art. 614 c.p.) - *pax domestica*, riservatezza e quiete della vita familiare - non costituisce, quanto meno in via esclusiva, l'oggetto della tutela della norma in esame, malgrado la sua collocazione tra i reati contro la violazione di domicilio.

II tesi (dottrinale): la tutela della «fruizione indisturbata» del sistema informatico assimilata alla tutela del «pacifico godimento della proprietà fondiaria» poiché i sistemi informatici non possono essere assimilati ai luoghi privati riconducibili alla nozione di domicilio rilevante per il diritto penale, poiché i contenuti del sistema informatico non sempre - ed anzi solo in un numero esiguo di casi - presentano carattere strettamente personale. Si effettua un parallelismo fra il bene protetto dall'art. 615- *ter* c.p. e quello di cui all'art. 637 c.p. «*Ingresso abusivo nel fondo altrui*» e si afferma che, la norma ex art. 615-ter c.p., tutela l'indisturbata fruizione del sistema informatico analogamente alla tutela offerta dall'art. 637 c.p. che, nel

reprimere l'ingresso abusivo nel fondo altrui, protegge da ogni possibile turbativa la proprietà fondiaria.
III tesi (dottrinale): la tutela dell'«integrità» del sistema e dei dati e dei programmi in esso contenuti. Secondo tale orientamento interpretativo il bene giuridico tutelato sarebbe da identificarsi nell' «integrità» del sistema, dei dati e dei programmi in esso contenuti, dal pericolo a cui è esposto in presenza di un accesso abusivo, invocando in tal senso la previsione del 2° co., n. 3, che configura quale circostanza aggravante del reato in esame la distruzione di dati o programmi ovvero l'interruzione del sistema, così introducendo un ulteriore requisito per la configurabilità del reato non previsto dalla norma incriminatrice, ovvero la messa in pericolo dell'integrità del sistema e dei dati. Per i sostenitori di tale tesi la natura giuridica del reato *ex* art. 615-*ter* c.p. è quella di «reato di pericolo astratto», per cui il legislatore incrimina una condotta *presumendone iuris et de iure* la pericolosità, la cui sussistenza in concreto non è necessaria per integrare gli estremi del reato.
Anche con riferimento alla struttura del reato esistono differenti schemi interpretativi.
Secondo l'orientamento maggioritario si tratta di un reato di danno e, tale tesi, deriva dal parallelismo fra la «fattispecie di accesso abusivo» e quella di «violazione di domicilio». L'intrusione nell'elaboratore altrui, quali che sia la natura dei dati o dei programmi in esso contenuti, integra la lesione del bene protetto, la *privacy* informatica.
A mente dell'orientamento minoritario l'art. 615-ter c.p. è un reato di pericolo. Tale tesi, pur sposando l'oggettività giuridica del «domicilio informatico», ritiene che il reato *ex* art. 615-*ter* c.p. anticipi la tutela penale al mero pericolo che, l'agente, penetrando nel *computer invito domino*, possa carpire quanto di più riservato possa esservi.
Passando all'interpretazione giurisprudenziale a più riprese proposta della locuzione "sistema informatico", in assenza di una definizione legislativa italiana, si fa ricorso alla nozione fornita dalla Convenzione di Budapest. Trattasi del complesso organico di elementi fisici (*hardware*) ed astratti (*software*) che compongono un apparato di elaborazione dati. L'art. 1 della Convenzione di Budapest lo definisce come qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate che, in base ad un programma, compiono l'elaborazione automatica dei dati. E' una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, che sono caratterizzate, per mezzo di un'attività di codificazione e di 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 combinazioni diverse, e dall'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 ().
Costituisce invece "sistema telematico" ogni forma di telecomunicazione che si giovi dell'apporto informatico per la sua gestione oppure che sia al servizio di

tecnologie informatiche, indipendentemente dal fatto che la comunicazione avvenga via cavo, via etere o con altri sistemi. Si riferisce a relazioni di interconnessione – comunicazione tra più elaboratori elettronici a distanza, attraverso un sistema di telecomunicazione che si giovi dell'apporto informatico per la relativa gestione.

Con riferimento al presupposto per la tutela penale, è indispensabile che il titolare del diritto abbia adottato delle misure di protezione al sistema informatico o telematico. Invero, i sistemi tutelati penalmente, sono solo quelli protetti da «misure di sicurezze» per effettuare l'accesso, adottate dal legittimo titolare. E' sufficiente qualsiasi misura di protezione, anche banale e facilmente raggirabile da persona mediamente esperta, purchè idonea a rendere esplicita e non equivoca la volontà del titolare di riservare l'accesso solo a determinate persone, ovvero di porre un generale divieto di accesso. Anche l'adozione di una protezione costituita da una semplice parola-chiave (*password*), pure facilmente accessibile o ricostruibile, rappresenta una esplicitazione corretta del divieto di accesso al sistema e legittima la tutela in sede penale. Assumono rilevanza non solo le «protezioni interne» al sistema informatico, come le chiavi di accesso, ma anche le «protezioni esterne», come la custodia degli impianti e la «protezione a mezzo di misure di carattere organizzativo», che disciplinano le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo (orientamento dottrinale e giurisprudenziale maggioritario). La lettura testuale della norma che prevede «misure di sicurezza» al plurale porterebbe a ritenere che una semplice parola chiave o un codice di accesso non integrano il requisito in analisi, che dovrebbe essere inteso come qualcosa di più complesso rispetto ad una *password* (orientamento dottrinale minoritario).

Sono misure di sicurezza quelle: 1) *di tipo logico*, interne al sistema e preordinate alla tutela dell'*hardware* e del s*oftware* = codici alfabetici o numerici da digitarsi alla tastiera o da memorizzare su bande magnetiche di tessere da inserire in un apposito lettore; 2) *di tipo fisico* = es. chiave metallica per l'accensione dell'elaboratore; 3) *di protezione dei locali* = es. porte blindate, personale di vigilanza, ecc…

Passando in disamina la condotta incriminata occorre distinguere: 1. «*l'introduzione nel sistema informatico o telematico*»: l'accesso rilevante penalmente non è il semplice «collegamento «fisico» (es. accensione dello schermo del p.c.) ma è necessario l'«accesso virtuale» che richiede l'inizio di un dialogo con il *software.* Costituisce «introduzione» in un sistema informatico o telematico protetto il superamento delle barriere di protezione che presidiano l'accesso alla memoria interna del sistema, con l'effetto di potere richiamare i dati ed i programmi che vi sono contenuti (di potere aprire uno o qualunque dei documenti memorizzati nel sistema) o, comunque, di avere libertà di movimento all'interno dell'elaboratore per soddisfare gli scopi dell'intromissione abusiva. Nell'ipotesi di sistemi con «barriere progressive» preordinate a penetrare nel cuore del sistema o «barriere alternative» in base agli archivi oggetto di consultazione, secondo taluni, è sufficiente che l'operatore abbia realizzato delle procedure per cui si trovi nelle

condizioni muoversi all'interno del sistema anche superficialmente; secondo altri, l'accesso è consumato solo se superati tutti gli ostacoli, altrimenti è solo tentato; 2. la «*permanenza nel sistema informatico o telematico*»: è sanzionato il mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare dello *ius excludendi*; alla condotta prodromica dell'accesso assentito al sistema segue quella del permanervi illegittimamente, in difformità agli accordi del titolare del sistema ovvero oltrepassando i limiti posti dall'autorizzazione. Occorre escludere il concorso materiale tra l'ipotesi di «introduzione abusiva» e quella di «mantenimento abusivo», poiché la permanenza nel sistema che faccia seguito ad un'introduzione illegittima, costituisce un semplice *post-factum* del tutto irrilevante e non integra l'ipotesi del mantenimento nel sistema. Le condotte di cui all'art. 615-*ter* c.p., presuppongono il requisito dell' «abusività» dell'introduzione (assenza di consenso da parte del titolare) ovvero dell' «utilizzazione abusiva» dell'accesso autorizzato (violazione delle condizioni e dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, per delimitarne oggettivamente l'accesso), indipendentemente dagli scopi e dalle finalità che soggettivamente hanno motivato l'ingresso al sistema.

L'elemento soggettivo del reato è il dolo generico, inteso quale coscienza e volontà di introdursi o di mantenersi nell'altrui sistema informatico o telematico ovvero nella memoria interna di un elaboratore, in assenza del consenso del titolare dello *ius excludendi* e con la consapevolezza che quest'ultimo ha predisposto misure di protezione del sistema.

La consumazione del reato (il tempo), per l'ipotesi di «introduzione», è fatta coincidere con il momento in cui sono oltrepassate tutte le barriere a cui è subordinato l'accesso ai dati ed ai programmi contenuti nella memoria del sistema. E' fattispecie a consumazione istantanea. Il reato non è consumato se l'agente ha soltanto iniziato a colloquiare con il sistema altrui ma non è riuscito ad oltrepassare le barriere di protezione; per l'ipotesi di «permanenza», nel momento in cui l'autore si trattiene all'interno del sistema, nonostante il dissenso del titolare del diritto di esclusione. E' fattispecie a carattere permanente, la cui consumazione cessa nel momento in cui si interrompe l'accesso.

La consumazione del reato (il luogo) avviene nel luogo in cui ha fisicamente sede il sistema oggetto di intrusione e non nel luogo in cui si trovi fisicamente l'agente all'atto in cui realizza materialmente le attività intrusive abusive. Di norma, trattasi di accessi «virtuali» o a «distanza» attraverso un collegamento effettuato con un *modem*.

Il tentativo è configurabile, tutte le volte in cui l'agente cerchi di aggirare le protezioni esistenti. Sono necessari atti idonei diretti in modo non equivoco alla violazione delle barriere di protezione della *privacy*, ben potendo accadere che il soggetto si colleghi al sistema senza sapere che l'accesso ai dati è protetto ed, in tal caso, il delitto non si configura neppure nella sua forma tentata.

Le circostanze aggravanti del reato sono ad effetto speciale (aumento di pena oltre il terzo); comportano la procedibilità d'ufficio, anziché a querela come per le ipotesi base; sono collegate al ruolo dell'attore ovvero alla oggettiva gravità della condotta;

Circa i rapporti del reato in disamina con altre fattispecie di reato: le ipotesi di concorso ammesso sono quelle con il reato ex art. 491-*bis* c.p. di falsificazione dei documenti informatici; con il reato *ex* art. 635-*bis* c.p. di danneggiamento dei sistemi informatici e telematici; con il reato *ex* art. 640-*ter* c.p. di frode informatica realizzata attraverso l'alterazione dei dati o dei programmi; con il reato *ex* art. 621 c.p. di rivelazione di documenti segreti di cui si sia venuti a conoscenza abusivamente; con il reato *ex* art. 513 c.p. di turbata libertà dell'industria o del commercio e con i reati *ex* att. 615 – *quater* c.p. e 615 –*quinquies* c.p. Le ipotesi di concorso escluso sono quelle con il reato *ex* art. 622 c.p. di rivelazione del segreto professionale; con il reato *ex* art. 623 c.p. di rivelazione del segreto industriale, poiché tali delitti presuppongono che l'agente sia detentore legittimo del segreto che indebitamente divulghi. Il reato ex art. 615-ter c.p. non può concorrere con il reato *ex* art. 646 c.p. di appropriazione indebita che rimane assorbito dal primo nell'ipotesi di duplicazione dei dati contenuti in un sistema informatico o telematico.

Non sussiste rapporto di specialità fra il reato *ex* art. 615-*ter* c.p., che sanziona l'accesso abusivo ad un sistema informatico e quello *ex* art. 167, D.Lgs 30.6.2003 n. 196, concernente l'illecito trattamento dei dati personali, trattandosi di fattispecie differenti per condotte finalistiche e attività materiali che escludono la sussistenza di una relazione di omogeneità.

Da ultimo, considerata l'attualità della tematica, occorre menzionare nell'ambito della presente trattazione anche la tecnica di c.d. "PHISHING" volta ad ottenere, tramite artifizi e raggiri ed inducendo in errore l'utente, le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare (es. relativi alla gestione *on line* dei conti correnti) ed a svolgere, senza autorizzazione, operazioni bancarie o finanziarie. Tale condotta, secondo giurisprudenza, può integrare gli estremi dei reati *ex* artt. 494 c.p. (sostituzione di persona), 615-*ter* c.p. (accesso abusivo a sistema informatico o telematico) e 640 c.p. (truffa). Per un ulteriore approfondimento si consiglia la consultazione della Scheda Informativa sintetica redatta in materia dal *Garante Privacy* e datata 15.12.2016.

La responsabilità amministrativa da reato degli enti di cui al D.Lgs. 8.6.2001, n. 231, in relazione alla commissione del delitto ex art. 615-ter c.p., l'art. 24-*bis*, 1° co., prevede l'applicazione all'ente della sanzione pecuniaria da cento a cinquecento quote.

E' anche prevista la confisca obbligatoria ex art. 240, II comma, n. 1 e n. 1-bis c.p. per gli *strumenti informatici* utilizzati per la commissione del reato, che saranno destinati alla polizia e la confisca obbligatoria anche per il profitto ed al prodotto del reato ed, in via sussidiaria, la confisca per equivalente di beni di valore pari al profitto o al prodotto del reato.

Si riportano qui di seguito le massime giurisprudenziali più significative in materia.

CORTE DI CASSAZIONE, SEZ. V, 29.7.2016, N. 33311: ai fini della configurabilità del reato di cui all'art. 615-*bis* c.p., l'accesso abusivo ad un sistema informatico consiste nella obiettiva violazione delle condizioni e dei limiti risultanti

dalle prescrizioni impartite dal titolare del sistema per delimitarne l'accesso, compiuta nella consapevolezza di porre in essere una volontaria intromissione nel sistema in violazione delle regole imposte dal *dominus loci,* a nulla rilevando gli scopi e le finalità che abbiano soggettivamente motivato tale accesso. (Nella fattispecie, la S.C., ha ritenuto immune da censure la condanna del cancelliere di un tribunale che si era introdotto nel sistema del casellario giudiziale ed aveva preso visione dei precedenti di un soggetto ricorrendo all'artificio consistente nell'indicazione di un procedimento inesistente ovvero relativo a soggetto diverso).
CORTE DI CASSAZIONE, SEZ. V, SENT., 13.3.2017, N. 11994: integra il delitto previsto dall'art. 615-*ter* c.p., la condotta del collaboratore di uno studio legale, cui sia stata affidata esclusivamente la gestione di un numero circoscritto di clienti, che accede all'archivio informatico dello studio provvedendo a copiare e a duplicare, trasferendoli su altri supporti, i *files* riguardanti l'intera clientele dello studio professionale e, pertanto, esulanti dalla competenza che gli era stata attribuita.
CORTE DI CASSAZIONE, SEZ. V, 31.3.2016, N. 13057: integra il reato di cui all'art. 615-*ter* c.p. la condotta di colui che accede abusivamente all'altrui casella di posta elettronica trattandosi di uno spazio di memoria, protetto da una *password* personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un *account* registrato presso il *provider* del servizio. (In motivazione la S.C. ha precisato che anche nell'ambito del sistema informatico pubblico, la casella di posta elettronica del dipendente, purchè protetta da una *password* personalizzata, rappresenta il suo domicilio informatico sicchè è illecito l'accesso alla stessa da parte di chiunque, ivi compreso il superiore gerarchico).
CORTE DI CASSAZIONE, SEZ. V, 22.2.2016, N. 6906: integra il reato *ex* art. 615-*ter* c.p., aggravato dalla previsione di cui al terzo comma, dall'essere il sistema di interesse pubblico, la condotta di colui che, essendosi procurato le credenziali relative alla carta *Postepay* della persona offesa, accede all'area riservata alla gestione della carta, la quale costituisce una componente del sistema informatico Poste Italiane, ente conferente le credenziali per l'accesso alle diverse aree personali e gestore delle stesse.
CORTE DI CASSAZIONE, SEZ. V, 15.12.2014, N. 52075: in tema di accesso abusivo a sistema informatico o telematico, la scriminante dell'esercizio di un diritto (art. 51 c.p.) non è configurabile qualora l'agente, per acquisire dati o elementi utili alla sua difesa in giudizio, accede indebitamente alla casella di posta elettronica di un collega di studio, prendendo cognizione delle *e-mail* inviate o ricevute, non essendo consentite intromissioni nella sfera di riservatezza delle controparti processuali o l'esercizio di facoltà riservate agli organi pubblici (In motivazione la S.C. ha specificato che tale attività illecita non può nemmeno essere ricondotta nell'ambito delle indagini difensive, che non possono essere compiute dagli imputati e devono comunque arrestarsi di fronte agli ambiti di privato dominio).
CORTE DI CASSAZIONE, SEZ. V, 19.11.2014, N.47938: ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico, non

assumono rilievo le violazioni commesse dal soggetto autorizzato in ordine alle indicazioni relative all'orario nel quale gli accessi possono essere effettuati in quanto si tratta di prescrizioni che attengono al solo profilo della organizzazione interna dell'ufficio presso il quale il sistema è operativo e non, invece, all'accesso ed al tempo di permanenza nel sistema informatico.
Conclusivamente non può che rammentarsi che, accedere o mantenersi all'interno di una casella di posta elettronica altrui o di un *account Facebook*, *Instagram* ovvero di altro *social network* la cui identità digitale appartiene ad altro soggetto, integra gli estremi del reato *ex* art. 615-*ter* c.p., non solo quando la *password* viene sottratta, ma anche quando è legittimamente conosciuta dall'agente, tutte le volte in cui esista un dissenso espresso o tacito da parte del titolare dell'*account*.

«DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI», EX ART. 615-QUATER C.P.

La norma è collocata nel Libro II – dei Delitti in particolare, titolo XII– dei Delitti contro la persona, Capo III – dei delitti contro la libertà individuale, **Sezione IV– dei delitti contro la inviolabilità del domicilio.**
L'articolo è stato aggiunto dall'art. 4, l. 23.12.1993, n. 547.
La natura giuridica è quella di reato comune, di pericolo, di mera condotta, a forma vincolata.
Quanto alla *ratio* della norma ed alla natura giuridica del reato, è sanzionata l'abusiva acquisizione e diffusione, con qualsiasi modalità, dei mezzi o codici di accesso preordinati a consentire a soggetti non legittimati l'introduzione nel sistema informatico o telematico altrui protetto da misure di sicurezza. Trattasi della repressione di condotte prodromiche alla realizzazione del delitto *ex* art. 615-*ter* c.p. e, nella specie, di una particolare ipotesi connotata e qualificata dalla sostituzione illegittima dell'agente al titolare del sistema mediante l'uso della *password* di quest'ultimo. E' configurato quale "reato ostativo", poiché finalizzato ad evitare il compimento di più gravi delitti contro la riservatezza o contro il patrimonio.
Sul bene giuridico tutelato dalla norma esistono diverse tesi contrapposte. Secondo una pima tesi si tratta della tutela anticipata del domicilio informatico; secondo una seconda tesi, l'obiettività giuridica è da identificarsi nel rafforzamento della tutela della segretezza dei dati e dei programmi contenuti in un elaboratore; a mente di una terza tesi, la noma esprime una tutela anticipata più ampia dei beni giuridici potetti da una serie di norme penali informatiche (patrimonio, riservatezza, fede pubblica) col fine di prevenire, in via generale, la commissione dei reati informatici; secondo una quarta tesi, oggetto di tutela è la prevenzione degli accessi abusivi effettuati senza alterazione del *software* di protezione del sistema e mediante la sostituzione illegittima del titolare dell'accesso nell'uso della *password.*
L'oggetto materiale della condotta incriminata sono i «codici», le «parole chiave» o gli «altri mezzi idonei all'accesso» ad un sistema informatico o telematico che sia protetto da misure di sicurezza. Il «codice di accesso (o parola chiave)», è la chiave che permette di collegarsi logicamente al sistema. può trattarsi di sequenza

alfabetiche, numeriche o alfanumeriche o numero-logiche che, se digitate alla tastiera o altrimenti comunicate all'elaboratore (es. attraverso un microfono o un lettore ottico), consentono l'accesso ai dati ed ai programmi contenuti nella memoria interna; «qualsiasi mezzo idoneo all'accesso», sono i mezzi di accesso fisici (chiavi meccaniche, chiavi elettroniche e cioè tesserini magnetici di riconoscimento, carte di credito, ecc…); mezzi logici (parole chiave nel senso di *password* ovvero i mezzi che consentono di collegarsi logicamente al sistema); indicazioni o istruzioni idonee a realizzare un accesso abusivo (le informazioni tecniche riservate che non svelano il codice di accesso, ma il metodo idoneo a raggiungere lo scopo).

Le condotte sanzionate penalmente consistono, alternativamente, nell' «acquisire» i mezzi necessari per accedere al sistema informatico altrui, indipendentemente dalle modalità di acquisizione ("procurarsi"); nel «procurare» ad altri codici, parole chiavi o altri mezzi idonei a consentire l'accesso abusivo; nel «diffondere», «comunicare» o «consegnare» a terzi detti mezzi (sia per iscritto che oralmente); nel «fornire» le informazioni, indicazioni, istruzioni idonee a consentire l'accesso ad un sistema informatico altrui protetto da misure di sicurezza; la «detenzione», invece, indicata nella dizione della rubrica ma non nel contenuto della disposizione, per taluni è ricompresa nella nozione di «procurarsi»;

Il reato si consuma nel momento e nel luogo in cui si realizza la condotta tipica e, quindi, allorché il soggetto agente acquisisca la disponibilità del codice di accesso entrando materialmente in possesso di esso, o pervenendo autonomamente alla sua individuazione, ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o la consegna a terzi di tali mezzi o di informazioni sul modo di eludere le barriere di protezione di un sistema informatico.

Il tentativo non è configurabile alla luce della sua natura giuridica di reato di pericolo astratto, a causa dell'eccessivo arretramento della tutela penale che ne deriverebbe.

L'elemento soggettivo è il dolo specifico, ovverosia coscienza e volontà di procurarsi, riprodurre, diffondere e comunicare codici di accesso o mezzi similari al fine di procurare a sé od altri un profitto o di arrecare ad altri un danno

Le circostanze aggravanti sono ad effetto speciale (aumento di pena superiore ad un terzo della pena base); sono agganciate o all'abuso da parte dell'agente di una particolare posizione funzionale oppure alla particolare importanza e delicatezza del sistema informatico o telematico coinvolto.

Quanto al rapporto dell'art. 615-quater c.p. con l'at. 615-ter c.p., v'è da sottolineare che, le due previsioni non concorrono, prevedendo l'art. 615-*quater* c.p. condotte prodromiche all'illecito ex art. 615-*ter* c.p. Esse possono concorrere quando i reati in questione siano realizzati dallo stesso agente che, in precedenza, abbia diffuso a terzi estranei la *password* per consentire loro l'accesso al sistema.

La casistica giurisprudenziale più significativa è la seguente:

CORTE DI CASSAZIONE, SEZ. 2, 26.11.2013, N. 47021: integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici e

telematici e non quello di ricettazione la condotta di chi riceve i codici di carte di credito abusivamente scaricati dal sistema e li inserisce in carte di credito clonate poi utilizzate per il prelievo di denaro contante attraverso il sistema *bancomat*.
corte di cassazione, sez. 5, 27.6.2002, n. 24847: 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 l. 248 del 2000 che, invece, concerne la tutela del diritto d'autore, con la conseguenza che tra le due previsioni non sussiste alcun rapporto di specialità.
CORTE DI CASSAZIONE, SEZ. 2, 22.9.2003 N. 36288: integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici o telematici la condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad un altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (*c.d. 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»), integra il delitto di ricettazione (art. 648 c.p.) di cui costituisce reato presupposto quello *ex* art. 615-*quater* c.p.

«DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO», ex art. 615-quinquies c.p.
La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione IV – Dei delitti contro la inviolabilità del domicilio.**
L'articolo è stato prima aggiunto dall'art. 4, L. 23.12.1993, n. 547, e successivamente così modificato dall'art. 4, L. 18.3.2008, n. 48 (*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica*).
La natura giuridica del reato è quella di reato comune, di pericolo astratto, di mera condotta, a forma libera.
La Riforma del 2008 estende la protezione contro una più ampia gamma di fonti di rischio, non solo i software infetti (Virus informatici), ma anche gli hardware infetti (apparecchiature e dispositivi informatici) diretti a danneggiare o interrompere un sistema informatico o telematico; amplia le condotte sanzionate e prevede che quella che costituiva la caratteristica intrinseca delle fonti di rischio, vale a dire lo scopo o l'effetto di danneggiare, rappresenti (anche) il fine perseguito dal soggetto agente con la sua condotta.

Trattasi di reato di pericolo astratto per cui la rilevanza penale delle condotte tipizzate prescinde dal verificarsi del danneggiamento informatico ex art. 635-bis c.p., realizzando un'anticipazione di tutela.
Il bene giuridico tutelato sono i sistemi informatici e telematici, nonché i dati, le informazioni ed i programmi in essi contenuti.
È sanzionato penalmente il comportamento dell'agente consistente nel «procurarsi» hardware o software "infetti" (nel concetto di "procurarsi" è ricompresa anche la mera detenzione); nella «produzione» di hardware o software "infetti" (non si intende la mera progettazione ed è rilevante anche la produzione o scrittura di un codice sorgente); nella «comunicazione» di hardware o software "infetti", con riferimento, secondo taluni, ad un contatto tra soggetti conferenti e riceventi e si può specificare come comunicazione telematica oppure più estensivamente come qualsiasi forma di esternazione preordinata alla realizzazione dei programmi in oggetto; secondo altri, è integrata solo dalla cessione del programma per via telematica; secondo altri ancora, la «comunicazione» è il mezzo attraverso cui si realizza la «diffusione»; nella «diffusione» di hardware o software "infetti", consistente nella messa in circolazione di programmi infetti attuata attraverso le reti telematiche ma anche con la materiale introduzione degli stessi nei sistemi informatici ovvero con la vendita di dischi o nastri magnetici che li contengano o, ancora, con l'incorporazione degli stessi in un supporto informatico; nella «consegna» di hardware o software "infetti": cessione del supporto fisico sul quale è registrato il programma che viene così posto nella disponibilità altrui; nel «comunque mettere a disposizione» hardware o software "infetti": è una clausola di chiusura del sistema della fattispecie volta ad includere qualsiasi modalità con cui gli oggetti di cui trattasi vengano messi nella disponibilità di terzi da parte dell'agente.
L'oggetto materiale della condotta incriminata sono gli hardware ed i software infetti.
Gli hardware infetti sono apparecchiature e dispositivi informatici, funzionalmente caratterizzati nel senso della idoneità a danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero a favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Esempi: dongle usb (chiave di protezione dei dati da copie); smart card (dispositivo delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione dati ad alta sicurezza); skimmer (dispositivo capace di leggere ed, in certi casi, anche di immagazzinare su una memoria i dati della banda magnetica dei badge – es. di una carta di credito).
I software infetti sono programmi informatici funzionalmente caratterizzati ovverosia programmi virus capaci di riprodurre se stessi infettando altri programmi nei quali si inseriscono con effetti devastanti per la sicurezza del sistema sociale che si affida progressivamente sempre di più al controllo dei sistemi informatizzati.
Le forme di contaminazione sono: la cancellazione totale dell'hard-disk, la modifica dei files contenuti in quest'ultimo, l'alterazione del contenuto del video,

la perdita di funzionalità specifiche dei programmi fino alla sostituzione o all'alterazione delle funzioni.
"Malware" è la definizione generica adatta per ogni software nocivo in grado di arrecare danno al sistema; è l'acronimo di "Malicious Software", letteralmente «software dannoso». Vi rientrano, a titolo esemplificativo e non esaustivo. "Virus" è un programma che si replica e infetta tutti i computer a cui si connette, modificando il sistema per "assecondarlo" nell'infezione, spesso distruggendo funzionalità vitali per l'esecuzione dei programmi sani e del sistema.ù
"Spyware" è un malware che "spia" gli utenti rubando le informazioni personali dal computer per inviarle al suo creatore. Alcune delle informazioni catturate dallo spyware includono: numeri di carte di credito, siti web visitati, le credenziali di accesso ai siti ed alla posta elettronica, ecc. Il danno reale ai sistemi è spesso molto limitato (autoavvio e monitoraggio) perché lo scopo primario è sottrarre più informazioni possibili; eliminarlo è relativamente semplice, ma il danno a livello economico e di privacy è rilevante, specie se lasciato agire troppo a lungo.
"Keylogger" è costituito da una serie di strumenti (hardware o software) in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio o di un altro computer. Viene spesso integrato all'interno di spyware o trojan per catturare la password d'accesso al sistema o altri dati sensibili (carte di credito, password siti di e-commerce, ecc...) per inviarle ad un server remoto.
"Troyan horse": è il malware tra i più diffusi e pericolosi; è un codice maligno nascosto all'interno di un altro software apparentemente utile (cavallo di Troia per ingannare gli utenti) ma che in modo occulto attiva la connessione ad un server maligno, scaricando poi altri malware per infettare il PC che sono utili per assumere il controllo completo del computer. Non si può installare automaticamente ma è l'utente che con la sua attività lo «accetta».
"Worm" sono tra i malware più dannosi, soprattutto per i computer collegati in rete LAN (aziendale o meno); di regola, fanno uso di falle di sicurezza note per intrufolarsi all'interno di ogni computer allacciato in LAN senza l'intervento degli utenti; la principale differenza tra i virus e i worm consiste nel fatto che, questi ultimi, si replicano usando i protocolli di rete e le sue falle note, garantendosi piena autonomia di azione, replicandosi ed infettando senza alcuna interazione degli utenti, mentre i virus, possono diffondersi solo se veicolati da mezzi fisici e richiedono un minimo d'interazione da parte degli utenti (devono essere eseguiti e avviati). Un Worm ha un livello di replicazione molto più alto di un virus e spesso arreca danno senza nemmeno avviarlo e moltiplicandosi all'infinito in un solo PC intasando il disco rigido e la rete. Alcuni esempi di worm sono i famosi "Iloveyou" e il temuto worm "Conficker", un malware recente molto avanzato che integra al suo interno le caratteristiche nocive di virus, trojan e worm.
Circa l'elemento soggettivo del reato era da rintracciarsi, *ante* Riforma, nel dolo generico, poiché era sufficiente la consapevolezza nell'agente dell'esistenza e della natura del programma virus messo in circolazione nonché la volontà di diffonderlo. Ad oggi, *post* Riforma, l'elemento soggettivo del reato è il dolo specifico, essendosi ristretta, sul piano soggettivo, la possibilità della punizione penale, allo scopo di

escludere il reato tutte le volte in cui si è in presenza di quelle situazioni professionali, di studio, ricerca o addirittura mere curiosità personali che possono comportare la detenzione o la messa a disposizione di terzi degli oggetti in questione, senza il fine del danneggiamento illecito.
Il reato si consuma nel momento e nel luogo in cui esiste già la mera «detenzione» consapevole degli oggetti in questione, che derivi da «riproduzione», «produzione», «acquisizione» o «importazione» (ovviamente in presenza dell'elemento soggettivo); nel caso della «consegna», con la *traditio* del supporto contenente il virus ad altra persona, oppure con il primo atto di diffusione e, quindi, con l' «introduzione» "da vicino" nell'altrui sistema informatico o per via telematica con la comunicazione del virus ad altro sistema.
Si esclude la configurabilità del tentativo onde evitare di arretrare eccessivamente la soglia di punibilità in violazione del principio di offensività. Ammettendo il tentativo si finirebbe per sanzionare la mera ideazione degli oggetti pericolosi.

«VIOLAZIONE, SOTTRAZIONE E SOPPRESSIONE DI CORRISPONDENZA», ex art. 616 c.p.
La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**
Il IV comma oggi vigente è stato sostituito dall'art. 5, L. 23.12.1993, n. 547.
La tutela ex art. 616 c.p. è limitata alla sola corrispondenza «statica».
La formulazione della norma con l'introduzione dei reati informatici prevede, oltre l'ipotesi classica della "corrispondenza epistolare" anche quella telegrafica, telefonica, "informatica" e "telematica", nonchè, residualmente ogni altra forma, attuale o futura, di "comunicazione a distanza".
L'art. 616 c.p. tutela il solo «profilo statico» della corrispondenza/ comunicazione informatica o telematica, poiché si limita ad estendere a tali forme di comunicazione il principio di inviolabilità del supporto materiale in cui sia stato fissato il contenuto della corrispondenza – comunicazione informatica o telematica.
Il «profilo dinamico» della corrispondenza/comunicazioni "informatiche" e "telematiche", è invece tutelato dall'art. 617-quater c.p. ("Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche").

«INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE», ex art. 617 – *quater* c.p.
La norma è collocata nel libro II – dei delitti in particolare, titolo II – Dei delitti contro la persona, capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**
L'articolo è stato aggiunto dall'art. 6, l. 23.12.1993, n. 547. per l'aumento della pena per i delitti non colposi di cui al presente titolo commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, vedi l'art. 36, 1° co., l. 5.2.1992, n. 104, come sostituito dall'art. 3, 1° co., l. 15.7.2009, n. 94.

L'art. 617-quater c.p. descrive un reato comune, di danno, di mera condotta, a forma vincolata; l'elemento soggettivo è il dolo generico; il tentativo è configurabile.
Il bene giuridico tutelato è la «segretezza», la «libertà» e la «riservatezza» delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.
L'oggetto materiale del reato riguarda le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, nella fase «dinamica» della loro trasmissione. I più comuni strumenti di comunicazione *on line* sono la posta elettronica (*e-mail*) e le varie modalità di comunicazione simultanea come le *chat line*, la *videoconferenz*a, che consente in tempo reale lo scambio e la condivisione di documenti, immagini, suoni. per la telematica, ad es. la tecnologia alla base delle trasmissioni televisive satellitari, dei sistemi *videotex*, *pay tv* e *pay per view,* la telemedicina per intervenire a distanza sul paziente intrasportabile. E'considerato sistema telematico, anche il sistema telefonico cellulare e la telefonia a rete fissa.
La condotta incriminata è la congiunta realizzazione di più condotte fra quelle sanzionate dall'art. 617-quater c.p., dà luogo ad un solo reato, trattandosi di norma a più fattispecie anche alternative.
E' «intercettazione» la presa di cognizione che si realizza attraverso la modalità della intromissione nella comunicazione in corso tra terzi, in cui il soggetto captante non è anche conversante. essa deve avere ad oggetto il contenuto di una comunicazione informatica o telematica in atto, nel momento dinamico della sua trasmissione.
L'«interruzione» e l'«impedimento» consistono nel compimento di atti tecnicamente idonei, da un lato, a far cessare una comunicazione in corso e, dall'altro, ad impedire che una nuova comunicazione abbia inizio (es. utilizzo di un *software* che causi lo spegnimento del modem di chi sta navigando in internet con l'interruzione della comunicazione in corso);
La «rivelazione» al pubblico si verifica qualora, l'agente, ha in qualsiasi modo - anche per via occasionale, o perfino con l'assenso dei dialoganti - acquisito la conoscenza del contenuto di una "comunicazione in atto", e poi ne renda pubblico il relativo contenuto.
Le circostante aggravanti del reato sono circostanze ad effetto speciale (aumento superiore ad un terzo della pena base); il particolare disvalore è identificato dal fatto che il reato è commesso in danno di un sistema informatico o telematico utilizzato dallo stato da altro ente pubblico o da impresa esercente servizio di pubblica necessità, o da un soggetto con una particolare qualifica (pubblico ufficiale o incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o con abuso della qualità di operatore del sistema o esercente anche abusivamente, la professione di investigatore privato); operatore di sistema è colui che controlla il processo di ricezione, elaborazione e diffusione dei dati, potendo influire sulla loro destinazione o integrità.
In relazione ai rapporti con altre fattispecie di reato è ammesso il concorso formale tra il reato *ex* art. 617-*quater* c.p. e quello *ex* art. 615 – *ter* c.p.; è escluso il concorso formale tra l'art. 617-*quater* c.p. e l'art. 617-*quiquies* c.p. *«installazione di*

apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche», operando l'assorbimento di quest'ultimo nel primo, poiché, l'attività di fraudolenta intercettazione presuppone necessariamente la previa installazione delle apparecchiature atte a realizzare l'intercettazione, configurandosi un'ipotesi di progressione criminosa.
Si segnalano le seguenti massime giurisprudenziali:
CORTE DI CASSAZIONE, SEZ. 5, 8.7.2015 N. 29091: per la configurabilità del reato di interruzione di comunicazioni informatiche non è necessario l'uso di mezzi fraudolenti, poiché tale requisito è riferibile esclusivamente alla condotta prevista dalla *prima parte* dell'art. 617-*quater* c.p., che tutela la *riservatezza* delle comunicazioni dalle intromissioni abusive attuate con captazioni fraudolente, mentre l'art. 617-*quater seconda parte*, tutela la *libertà delle comunicazioni*, che può essere impedita con qualsiasi mezzo anche non fraudolento.
CORTE DI CASSAZIONE, SEZ. V, 14.10.2003, N. 44362: nella condotta del titolare di esercizio commerciale il quale, d'intesa con il possessore di una carta di credito contraffatta, utilizza tale carta di credito mediante il terminale pos in dotazione, sono ravvisabili sia il reato di cui all'art. 615 - *ter* c.p. e quello di cui all'art. 617 - *quater* c.p.: il primo reato perché l'uso di una chiave contraffatta rende abusivo l'accesso al pos; il secondo perché, con l'uso di una carta di credito contraffatta, si genera un flusso di informazioni relativo alla posizione del vero titolare della carta di credito e diretto all'addebito sul suo conto della spesa fittiziamente effettuata, per cui vi è fraudolenta intercettazione di comunicazioni.

«INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE», ex art. 617- quinquies c.p.

La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**
L'articolo è stato aggiunto dall'art. 6, L. 23.12.1993, n. 547.
Si tratta di un reato comune, di pericolo concreto, di mera condotta, a forma vincolata; l'elemento soggettivo del reato è il dolo generico; il tentativo secondo taluni è configurabile, secondo alti, no.
Nella sua applicazione pratica, la fattispecie delittuosa in esame, ha dato vita ad interpretazioni giurisprudenziali variegate, non a causa di particolari dubbi esegetici che potevano sorgere, ma per le peculiari forme alternative di manifestazione delle condotte.
Si segnalano in particolare le massime giurisprudenziali sotto riportate.
CORTE DI CASSAZIONE, SEZ. 2, 7.11.2011, N. 40035: è configurabile il tentativo del delitto di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (la S.C. sottolinea che la giurisprudenza da lungo tempo ammette, in linea di principio, la configurabilità del tentativo rispetto ai delitti di pericolo, rigettando anche il motivo di doglianza dei ricorrenti inerente la non configurabilità del delitto ex art. 617-quinquies c.p.

nella sua forma tentata. Nella fattispecie concreta, nel pc sequestrato agli imputati, erano state trovate memorizzate diverse ore di filmati prodotti da microcamere poste al di sopra di sportelli bancomat).
CORTE DI CASSAZIONE, SEZ. 5, 30.1.2007, N. 3252: integra il delitto ex art. 617-quinquies c.p. la condotta di colui che installa abusivamente apparecchiature atte ad intercettare comunicazioni relative ad un sistema informatico posizionando nel «postamat» di un ufficio postale una fotocamera digitale, considerato che, l'intercettazione, implica che l'agente si inserisca nelle comunicazioni riservate, traendo indebita conoscenza delle stesse.
CORTE DI CASSAZIONE, SEZ. 2, 4.12.2007, N. 45207: l'utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico, integra la condotta del delitto ex art. 617-quinquies c.p., dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione con il sistema, rientra nella nozione di «intercettare» di cui alla norma incriminatrice (in specie, l'apparecchiatura sequestrata all'imputato era idonea a copiare i codici alfanumerici dei supporti magnetici inseriti negli sportelli bancari automatici).
CORTE DI CASSAZIONE, SEZ. V, 13.10.2010, N. 36601: integra il reato ex art. 617-quinquies c.p. la condotta di colui che installi, all'interno del sistema bancomat di un'agenzia di banca, uno scanner per bande magnetiche con batteria autonoma di alimentazione e microchip per la raccolta e la memorizzazione dei dati, al fine di intercettare comunicazioni relative al sistema informatico. Trattandosi di reato di pericolo, non è necessario accertare, ai fini della sua consumazione, che i dati siano effettivamente raccolti e memorizzati, ma solo l'idoneità del mezzo captativo.

«FALSIFICAZIONE, ALTERAZIONE O SOPPRESSIONE DEL CONTENUTO DI COMUNICAZIONI INFORMATICHE O TELEMATICHE», ex art. 617-sexies c.p.

La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**
L'articolo è stato aggiunto dall'art. 6, L. 23.12.1993, n. 547.
Si tratta di un reato comune, di danno, di mera condotta, a forma vincolata.
Il bene giuridico tutelato è la libertà delle comunicazioni informatiche o telematiche, sotto il particolare profilo della «sicurezza», «genuinità» e «veridicità» delle stesse, in cui ripone fiducia la generalità dei consociati.
E' stata criticata la scelta legislativa per la "procedibilità d'ufficio" del delitto in esame, a fronte della "procedibilità a querela", una volta prevista, per il falso in scrittura privata ex art. art. 485 c.p., oggi abrogato dal D.Lgs. 7/2016 (creazione di una corrispondente figura di illecito civile di analoga portata precettiva cui si riconnette l'irrogazione di una sanzione punitiva di natura civile).
La condotta incriminata consiste nella «formazione», in tutto o in parte, di una comunicazione falsa quale creazione ex novo di una comunicazione mai avvenuta tra coloro che appaiono parteciparvi; l' «alterazione», anche parziale, di una comunicazione vera è la modificazione del testo originale della conversazione

attraverso aggiunte, sostituzioni o eliminazioni; la «soppressione», anche parziale, di una comunicazione vera è una qualunque condotta che impedisca al destinatario della comunicazione di apprenderne il contenuto. Tra le ipotesi di «soppressione» rientra oltre la "distruzione", anche il mero "occultamento".
Epilogo di tutte le descritte condotte, per la consumazione del reato, deve essere l'uso da parte dell'agente del contenuto della comunicazione falsa, o alterata, o l'uso da parte di terzi, con il consenso dell'agente.
L' «uso» giuridicamente rilevante, ai fini penali, è quello oggettivamente idoneo a produrre effetti vantaggiosi per l'agente o dannosi per altri, con esclusione della rilevanza penale dei casi di mera fuoriuscita del contenuto della comunicazione falsa o alterata dalla sfera individuale del soggetto agente, o della scolastica esibizione per pura ostentazione.
La realizzazione congiunta di più condotte, fra quelle tipizzate dalla norma, integra un solo reato.
L'elemento soggettivo del reato è il dolo specifico poiché il fatto deve essere commesso al fine di procurare a sé o ad altri un vantaggio (qualche utilità, patrimoniale o non patrimoniale), o ad altri un danno (ossia un pregiudizio giuridicamente apprezzabile). Non hanno rilevanza penale le condotte che si risolvono in un vantaggio a favore dello stesso soggetto passivo.
Per le circostanze aggravanti del reato, l'art. 617-sexies c.p., rinvia alle circostanze aggravanti ex art. 617-quater c.p. di cui infra si è già trattato.
Il reato si perfeziona nel momento e nel luogo in cui avviene l'«uso» della comunicazione informatica o telematica falsa; la dottrina maggioritaria esclude la configurabilità logica ed ontologica dell' «uso» di un documento soppresso; la dottrina minoritaria ritiene che possa farsi «uso» di una comunicazione soppressa, proprio traendo vantaggio dalla conoscenza delle informazioni in essa contenute, e dalla contemporanea ignoranza di esse da parte del destinatario.
Il tentativo è configurabile allorquando l'agente pone in essere atti idonei diretti in modo non equivoco alla realizzazione di talune delle condotte sanzionate penalmente dalla norma; come in materia di falso non è punibile, neppure a titolo di tentativo, l'ipotesi del c.c. «falso grossolano», perché radicalmente inidoneo ad offendere il bene giuridico tutelato.
La produzione giurisprudenziale più significativa selezionata afferisce alla pronuncia del Giudice della Legittimità (sez. V, 29.5.2017, n. 39768), la quale, nel fare una *summa* delle principali caratteristiche del reato, statuisce che, il dolo richiesto dall' art. 617-sexies c.p., è specifico e consiste nella coscienza e volontà di procurarsi un vantaggio, non necessariamente patrimoniale, o di recare ad altri un danno. Deve, poi, essere oggettivamente riscontrabile, la materiale alterazione o soppressione della comunicazione. Occorre, infine, che dell'alterazione compiuta l'agente abbia fatto uso o abbia semplicemente tollerato un uso ad opera di altri; deve, quindi, esservi stata consapevolezza della diffusione esterna di una rappresentazione informativa non genuina o non corrispondente a verità (in specie, ad una dipendente di un Comune era stato imputato di aver formato falsamente e quindi inviato ad un soggetto partecipante ad una procedura concorsuale, facendone

così uso, la notifica di avvenuta lettura della e-mail di convocazione, in realtà mai pervenuta all'interessata, per un colloquio previsto nell'ambito della procedura concorsuale di mobilità volontaria per un posto di agente di Polizia Municipale, indetto da quel Comune, al fine di occultare la propria responsabilità relativamente all'invio di tale comunicazione all'indirizzo e-mail errato; tale errore aveva determinato l'esclusione del soggetto partecipante dalla graduatoria).

«RIVELAZIONE DEL CONTENUTO DI DOCUMENTI SEGRETI», ex art. 621 c.p.

La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**

Il secondo comma è stato aggiunto dall'art. 7, L. 23.12.1993, n. 547.

E' un reato comune, di danno, di mera condotta, a forma vincolata.

La *voluntas legis* era quella di non lasciare vuoti di tutela in materia di segreti, offrendo protezione ai documenti di contenuto segreto diversi da quelli di natura epistolare.

Non assume rilievo il «rapporto» da cui scaturisce l'apprendimento della notizia segreta (come per gli artt. 622 c.p. «Rivelazione di segreto professionale» e 623 c.p. «Rivelazione di segreti scientifici o industriali»), ma il «contenitore» della notizia, l'«apprendimento abusivo» della stessa contenuta in un supporto materiale;

L'oggettività giuridica è la tutela della libertà personale quale diritto del singolo all'esclusività della conoscenza o quantomeno al controllo su ogni informazione relativa alla sua vita riguardo a cui egli abbia interesse alla riservatezza, mentre sono indirettamente tutelati gli interessi sottostanti del diritto alla riservatezza: onore, decoro, salute, patrimonio.

Circa la condotta incriminata, la norma sanziona alternativamente le condotte di «rivelazione» di un segreto, consistente nel rendere noto ad una o più persone anche non determinate (al pubblico), con qualsiasi mezzo o modo, una parte giuridicamente apprezzabile o l'intero contenuto di un documento destinato a rimanere segreto. Essa deve avvenire senza giusta causa; di «impiego» di un segreto, consistente nell'utilizzazione dello stesso per finalità o con modalità tali da trarne un qualunque profitto (patrimoniale o non patrimoniale, giusto o ingiusto) per sé o per altri. Si esclude il reato quando la condotta si sia risolta a beneficio del titolare del segreto.

Il presupposto della condotta è costituito dalla cognizione abusiva (uso non conforme alle facoltà legittime) del contenuto di atti, documenti e supporti informatici.

Quanto all'oggetto materiale del reato, esso è costituito dal contenuto segreto di atti o documenti che non costituiscano «corrispondenza», nell'ampia accezione di corrispondenza informatica, telematica ovvero effettuata con ogni altra comunicazione a distanza. E' espressamente considerato come «documento» oggetto di tutela anche il supporto informatico (il supporto di memoria interno – hard disk, o esterno - dischi magnetici, ottici, ecc…, all'elaboratore, sul quale possono essere registrati e conservati per un certo lasso di tempo dei dati o

informazioni, nonché programmi – software, di elaborazione degli stessi, destinati ad essere letti ed eventualmente elaborati da un sistema informatico). Gli atti o i documenti possono essere «pubblici» o «privati» il cui contenuto è destinato a rimanere segreto, in forza di legge, per la loro stessa natura ovvero per volontà, espressa o tacita, presunta o effettiva, dell'avente diritto.
L'elemento soggettivo del reato è il dolo generico, inteso quale coscienza e volontà del fatto tipico che deve, quindi, coprire la natura segreta dell'atto, la natura abusiva della cognizione del suo contenuto e del nocumento cagionato (se si accede alla tesi della previsione normativa del «nocumento» quale elemento costitutivo – evento - del reato).
Il reato si consuma nel momento e nel luogo in cui si realizza l'evento del nocumento (se si accede alla tesi della previsione normativa del «nocumento» quale elemento costitutivo – evento - del reato) ovvero nel momento e nel luogo in cui si realizza taluna delle condotte incriminate (se si accede alla tesi della previsione normativa del «nocumento» quale condizione obiettiva di punibilità).
Il tentativo, secondo l'opinione maggioritaria, è configurabile in assoluto. Non sarebbe configurabile per coloro che accedono alla tesi della previsione normativa del «nocumento» quale condizione obiettiva di punibilità, poiché il fatto non sarebbe punibile fintatochè non si verifichi il nocumento.
In relazione ai rapporti della norma in commento con altre fattispecie di reato, il reato ex art. 621 c.p., può concorrere con qualsiasi altro reato la cui commissione abbia consentito l'avvenuta cognizione abusiva del contenuto dell'atto segreto. Quando sono integrati reati contro il patrimonio (ad es. appropriazione indebita, furto, rapina, estorsione) caratterizzati dal fine di trarre profitto con la condotta di spoglio materiale dei documenti, la condotta di «rivelazione» o di «impiego» assume il carattere di post factum non punibile che integra l'evento di profitto cui tende il dolo specifico dei delitti in considerazione. Non è configurabile il concorso fra l'art. 621 c.p. e quelli previsti dagli artt. 261 c.p. («Rivelazione di segreti di Stato»), 326 c.p. («Rivelazione ed utilizzazione di segreti ufficio»), 622 c.p. («Rivelazione di segreto professionale»), 623 c.p. («Rivelazione di segreti scientifici o industriali»), 683 c.p. («Pubblicazione delle discussioni o delle deliberazioni segrete di una delle Camere»), 684 c.p. («Pubblicazione arbitraria di atti di un procedimento penale»), 685 c.p. («Indebita pubblicazione di notizie concernenti un procedimento penale»).
Si segnalano le seguenti pronunce rese sul punto dalla Suprema Corte di Cassazione.
CORTE DI CASSAZIONE, SEZ. V, 9.2.1974, N. 1192 = il reato di rivelazione del contenuto di documenti segreti è punibile soltanto a querela della persona offesa. La titolarità del diritto di querela non può che spettare al soggetto interessato alla conservazione del segreto, a colui cioè che ha legittimo interesse alla «non rivelazione» del segreto, sia che l'atto o il documento, pubblico o privato si trovi presso di lui, sia che si trovi presso terzi.
CORTE DI CASSAZIONE, SEZ. V, 12.5.2014, N. 51089 = ai fini dell'integrazione del reato di rivelazione del contenuto di documenti segreti ex art. 621 c.p. è

necessario che dalla rivelazione e dall'utilizzazione del segreto derivi, quale condizione di punibilità, un nocumento, intendendosi per tale un pregiudizio giuridicamente rilevante di qualsiasi natura in danno del titolare del diritto alla segretezza (in specie, la S.C., ha ritenuto integrato il nocumento nella rivelazione di oltre 3200 informazioni relative ad una società e rivelate ad altra concorrente della prima con la determinazione di una turbativa illecita al mercato nei confronti della società titolare di tali informazioni).
CORTE DI CASSAZIONE, SEZ. V, 16.1.2009, N. 17744 = il nocumento costituisce condizione oggettiva di punibilità del reato ex art. 621 c.p. di rivelazione del contenuto di documenti segreti, pertanto, qualora dalla rivelazione del segreto documentale non derivi un nocumento - inteso come pregiudizio giuridicamente rilevante di qualsiasi natura - al titolare del diritto alla segretezza, va esclusa la sussistenza del reato anche solo tentato.

«ALTRE COMUNICAZIONI E CONVERSAZIONI», ex art. 623-bis c.p.
La norma è collocata nel Libro II – Dei delitti in particolare, Titolo XII – Dei delitti contro la persona, Capo III – Dei delitti contro la libertà individuale, **Sezione V – Dei delitti contro la inviolabilità dei segreti.**
L'articolo è stato prima aggiunto dall'art. 4, L. 8.4.1974, n. 98, sulla riservatezza, la libertà e la segretezza delle comunicazioni, e successivamente così sostituito dall'art. 8, L. 23.12.1993, n. 547.
Circa l'ambito di applicazione, l'art. 623-bis c.p., è una noma di chiusura del sistema sanzionatorio posto a tutela della segretezza, riservatezza e libertà delle comunicazioni a distanza.
Ha la funzione di estendere l'oggetto materiale di tutti i delitti «contro la inviolabilità dei segreti» contenuti nella sezione V del titolo XII della parte speciale del c.p. fino a comprendere nell'ambito di tutela qualsiasi forma trasmissione a distanza di suoni, immagini o altri dati.
Attraverso tale norma, il Legislatore, ha colmato il vuoto di tutela che si era venuto a creare in relazione alle comunicazioni attuate attraverso «onde elettriche» come tali non assimilabili alle «onde guidate»; la previgente disposizione normativa prevedeva, infatti, l'estensione della disciplina dettata in materia di delitti contro l'inviolabilità dei segreti, relativa alle comunicazioni ed alle conversazioni telegrafiche e telefoniche, a qualunque altra trasmissione di suoni, immagini o altri dati effettuata con collegamenti su fili o ad onde guidate.
Per "onde guidate" deve intendersi la trasmissione a distanza di suoni, immagini od altri dati effettuata a mezzo di conduttori fisici, nonché i casi di trasporto tramite antenne, ponti radio e fibre ottiche.
L'eliminazione del riferimento al mezzo con cui si effettua la trasmissione del dato consente l'applicabilità della normativa a tutela del segreto anche alle comunicazioni effettuate attraverso ogni altro strumento concepito dall'evoluzione del progresso tecnico-scientifico.
In relazione a tale fattispecie si segnala la Giurisprudenza di Legittimità sotto riportata.

CORTE DI CASSAZIONE, SEZ. V, 6.5.2004, N. 25488 = sussiste il reato di cui al combinato disposto degli artt. 617-bis e 623-bis c.p., nel caso di installazione di apparecchio ricevente atto ad intercettare le comunicazioni degli organi di polizia effettuate attraverso la loro centrale operativa, poiché la nuova formulazione della noma si riferisce ad ogni genere di «trasmissione a distanza di suoni, immagini ed altri dati», senza più il limite che dovesse comunque trattarsi di trasmissione «con collegamento su filo o ad onde guidate» (in specie, l'imputato aveva installato sul suo furgone, fuori dei casi consentiti dalla legge, un apparato radioricevente al fine di intercettare le comunicazioni della polizia di Stato, con l'aggravante di avere commesso il fatto ai danni di pubblici ufficiali nell'esercizio delle loro funzioni).
CORTE DI CASSAZIONE, SEZ. I, 17.6.2008, N. 29515 = la messa in opera di un apparecchio radioricevente atto a captare le trasmissioni operative delle forze dell'ordine integra il reato di installazione di apparecchiature al fine di intercettare comunicazioni a distanza, previsto dagli artt. 617-bis e 623-bis c.p. (in specie, l'indagato, dopo l'applicazione della misura di prevenzione, aveva fatto collocare intorno alla sua abitazione un sofisticato sistema di videosorveglianza e installato uno "scanner" radioricevente in grado di captare le comunicazioni delle forze di polizia).

«DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI» ex art. 635-bis c.p.

La norma è collocata nel Libro II – Dei delitti in particolare; Titolo XIII – Dei delitti contro il patrimonio; **Capo I – Dei delitti contro il patrimonio mediante violenza alle cose o alle persone.**

Il secondo comma è stato così sostituito dall'art. 2, 1° co., lett. m), D.Lgs. 15.1.2016, n. 7, a decorrere dal 6 febbraio 2016.

L'articolo è stato prima aggiunto dall'art. 9, L. 23.12.1993, n. 547, e successivamente così sostituito dall'art. 5, L. 18.3.2008, n. 48.

Si tratta di un reato comune, di danno, di evento, a forma libera; il tentativo è configurabile.

Il reato ex art. 635- bis c.p. è stato introdotto con la Riforma del 1993 poiché nonostante gli sforzi interpretativi non era possibile ricondurre i fatti di danneggiamento aventi ad oggetto beni immateriali, quali i «dati» ed i «programmi informatici», nell'area operativa dell'art. 635 c.p., stante la precisa indicazione dell'oggetto materiale della condotta - cose mobili o immobili.

A seguito della Riforma del 2008, l'art. 635-bis c.p., ha ad oggetto la protezione in via esclusiva del software o dei dati e/o delle notizie in esso contenute (invalidazione funzionale delle componenti immateriali), ferma l'applicabilità della disposizione generale sul danneggiamento per ciò che riguarda la tutela dell'inviolabilità della parte fisica delle apparecchiature informatiche o telematiche (invalidazione materiale).

L'oggettività giuridica è costituita dall' integrità del patrimonio e da beni di natura non meramente patrimoniale, quali gli interessi all' integrità ed alla funzionalità dei dati e dei programmi informatici.

La condotta incriminata consiste nella distruzione», nel «deterioramento», nella «cancellazione», nell'«alterazione» e nella «soppressione» di informazioni, dati o programmi informatici altrui.
La fattispecie, che riflette un reato di evento a forma libera, può essere integrata anche mediante un comportamento omissivo.
Quanto alla nozione di «altruità», l'art. 635-bis c.p., richiede l' «altruità» dei beni oggetto di danneggiamento informatico. Stante la difficoltà di individuare la persona offesa sulla base dell' «altruità», in dottrina, si è proposto di fare riferimento a tutti gli interessi giuridicamente rilevanti, di natura obbligatoria, che confluiscono sui dati facendo leva sulla figura dell' «interessato» (ovverosia la persona cui i dati si riferiscono) introdotta dal Codice Privacy (D.lgs. 196/2003).
La clausola di riserva posta all'incipit della norma circoscrive l'ambito di operatività dell'art. 635-bis c.p. all'aggressione alla integrità fisica o logica di informazioni, dati o programmi non sussumibili in fattispecie astratte diverse e più gravi (es. falsità per soppressione ex art. 491-bis c.p. e accesso abusivo a sistema informatico o telematico ex art. 615-ter c.p., qualora a tale reato segua il danneggiamento).
L'elemento soggettivo del reato è il dolo generico, da intendersi quale coscienza e volontà del fatto tipico, non dovendo l'agente perseguire alcun fine specifico, ma solo avere la consapevolezza di distruggere, deteriorare, cancellare, alterare o sopprimere i beni informatici protetti.
I contorni del reato de quo sono delineati in modo plastico dalla giurisprudenza del Supremo Consesso di seguito riportata.
CORTE DI CASSAZIONE, SEZ. II, 15.9.2016, N. 38331 = ai fini della configurabilità del reato ex art. 635-bis c.p., è necessario che tali dati abbiano il carattere dell'altruità rispetto all'autore della condotta, sicchè il reato non sussiste nel caso in cui il titolare di una casella di posta elettronica protetta da password, riservatagli dal datore di lavoro, cancelli le e-mail ivi contenute, benchè ricevute in ragione del rapporto di lavoro, poichè queste ultime appartengono al dipendente, che ha il potere di esclusiva sulla casella di posta elettronica.
CORTE DI CASSAZIONE, SEZ. V, 5.3.2012, N. 8555 = il reato ex art. 635-bis c.p. deve ritenersi integrato anche quando la manomissione e l'alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo, comunque non reintegrativo, dell'originaria configurazione dell'ambiente di lavoro (in specie, la S.C., ha ritenuto la sussistenza del reato in un caso in cui era stato cancellato, mediante l'apposito comando e, dunque, senza determinare la definitiva rimozione dei dati, un rilevante numero di file, poi recuperati grazie all'intervento di un tecnico informatico specializzato).
CORTE DI CASSAZIONE, SEZIONI UNITE, 13.12.1996, N. 1282 = antecedentemente all'entrata in vigore della L. 547/1993, 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 c.p., in quanto, mediante la distruzione di un bene immateriale, si produceva

l'effetto di rendere inservibile l'elaboratore. Il principio di diritto espresso è che, tra il delitto di cui all'art. 635 c.p. e l'analoga speciale fattispecie criminosa prevista dall'art. 9 L. 547/1993 – che ha introdotto l'art. 635-bis c.p. sul danneggiamento di sistemi informatici e telematici – esiste un rapporto di successione di leggi penali nel tempo, disciplinato dall'art. 2 c.p.

«FRODE INFORMATICA», ex art. 640-ter c.p.

La norma è inserita nel Libro II – Dei delitti in particolare, Titolo XIII - Dei delitti contro il patrimonio, **Capo II – Dei delitti contro il patrimonio mediante frode.**

L'articolo è stato aggiunto dall'art. 10, L. 23.12.1993, n. 547.

Il terzo comma è stato inserito dall'art. 9, 1° co., lett. a, D.L. 14.8.2013, n. 93, convertito, con modificazioni, dalla L. 15.10.2013, n. 119 (*Contrasto alla violenza e femminicidio*)

Il quarto comma è stato così modificato dall'art. 9, 1° co., lett. b, D.L. 14.8.2013, n. 93, convertito, con modificazioni, dalla L. 15.10.2013, n. 119

E' un reato comune, di danno, di evento, a forma vincolata; il tentativo è configurabile.

La *ratio* della norma in esame trova la sua genesi nella difficoltà di ricondurre le ipotesi di "truffa informatica" nell'ambito di operatività della "truffa" ex art. 640 c.p., considerato il divieto di analogia in *malam partem* che non consentiva di assimilare l'operazione di intervento fraudolento sul funzionamento di una macchina alla condotta ingannevole verso un individuo persona fisica (induzione in errore della vittima che presuppone un rapporto relazionale ed interpersonale fra soggetto agente e soggetto ingannato).

Quanto al bene giuridico, occorre sottolineare che trattasi di fattispecie incriminatrice plurioffensiva posta a tutela del «patrimonio», del «regolare funzionamento dei sistemi informatici» e della «riservatezza» dei dati che ne deve accompagnare l'utilizzazione, oltrechè, della «libertà negoziale».

L'art. 640-ter c.p. prevede due differenti ipotesi tassative e tra di loro alternative che rappresentano gli «artifizi» ed i «raggiri» propri della frode informatica: «alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico» significa alterazione che può essere ottenuta o agendo sul software - la componente logica del computer; ovvero operando sull'hardware, cioè sulle parti elettroniche, meccaniche, magnetiche, ottiche del computer. Si fa riferimento, quindi, ad ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei dati; «intervenendo senza diritto su dati, informazioni o programmi» sta a ricomprendere ogni azione che produca una qualche modifica ai regolari processi dell'elaboratore. L'espressione "senza diritto" significa assenza del consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico, pertanto, assenza del diritto di agire generalmente intesa, ma anche una modalità di azione «non consentita da norme giuridiche, né da altre fonti», Le condotte di truffa informatica possono essere commesse anche nella forma

omissiva, qualora sussista in capo al soggetto agente l'obbligo giuridico di impedire l'evento (c.d. posizione di garanzia).
L'elemento soggettivo del reato è il dolo generico, quale coscienza di porre in essere le condotte tipizzate dalla norma e la volontà di procurare a sé o ad altri un profitto ingiusto con altrui danno.
La frode informatica si consuma nel luogo di esecuzione dell'attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico; si consuma nel momento in cui l'agente interviene sui dati del sistema informatico in modo da modificarne il funzionamento rispetto a quanto in precedenza possibile e nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui. Il conseguimento dell' «ingiusto profitto con altrui danno» costituisce l'evento del reato che ne realizza la consumazione.
Significative appaiono le massime giurisprudenziali selezionate e sotto riportate.
CORTE DI CASSAZIONE, SEZ. I, 20.5.2016, N. 36359 = il reato di frode informatica si consuma nel momento in cui il soggetto agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui.
CORTE DI CASSAZIONE, SEZ. II, 25.1.2011, N. 6958 = il reato di frode informatica aggravata, commesso in danno di un ente pubblico, si consuma nel momento in cui il soggetto agente (nella specie: il pubblico dipendente infedele) interviene, senza averne titolo, sui dati del sistema informatico, alterandone, quindi, il funzionamento.
CORTE DI CASSAZIONE, SEZ. II, 11.11.2009, N. 44720 = 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. (Nella fattispecie l'imputato, dopo essersi appropriato della "password" rilasciata a un terzo, responsabile di zona di una compagnia assicurativa, manipolava i dati del sistema predisponendo false attestazioni di risarcimento dei danni).
CORTE DI CASSAZIONE, SEZ. II, 24.2.2011, N. 9891 = integra il reato di frode informatica, e non già soltanto quello di accesso abusivo ad un sistema informatico o telematico, la condotta di introduzione nel sistema informatico delle Poste italiane S.p.A. mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro depositate sul conto corrente del predetto.
CORTE DI CASSAZIONE, SEZ. VI, 14.12.1999, N. 3067 = possono formalmente concorrere i reati di accesso abusivo a un sistema informatico (art. 615-ter c.p.) e di frode informatica (art. 640-ter c.p.): tattasi di reati totalmente diversi, il secondo dei quali postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del primo: la differenza fra le due ipotesi criminose si ricava, inoltre, dalla diversità dei beni giuridici tutelati, dall'elemento soggettivo e dalla previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi dei sistemi protetti, caratteristica che non ricorre nella

frode informatica (In specie, è stata ritenuta la possibilità di concorso dei due reati nel comportamento degli indagati che, digitando da un apparecchio telefonico sito in una filiale italiana della società autorizzata all'esercizio della telefonia fissa un numero corrispondente ad un'utenza extraurbana, e facendo seguire rapidamente un nuovo numero corrispondente a un'utenza estera, riuscivano a eludere il blocco del centralino nei confronti di tali telefonate internazionali, così abusivamente introducendosi nella linea telefonica e contestualmente procurandosi un ingiusto profitto con danno per la società di esercizio telefonico).
CORTE DI CASSAZIONE, SEZ. II, 30.9.2015, N. 41777 = integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito (art. 55 del D.Lgs. 231/2007), la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua. L'elemento specializzante è costituito dall'utilizzo «fraudolento» del sistema informatico. (Fattispecie, nella quale l'indagato, introdottosi nel sistema informatico di una società di gestione dei servizi finanziari, utilizzava senza diritto i dati relativi a carte di credito appartenenti a cittadini stranieri ed effettuava, così, transazioni commerciali, conseguendo un ingiusto profitto).

Reggio Calabria, 24 Settembre

Avv. Francesco Albanese Avv. Valentina Privitera