INTRODUZIONE

La capillare diffusione tecnologica degli ultimi decenni ha inciso in modo sempre piu pregrante nei comportamenti umani, inserendosi nella vita di ciascuno di noi e coinvolgendo inevitabilmente la sfera del diritto. Proprio questa intersezione tra tecnologia e diritto ha portato alla creazione di una nuova branca della scienza forense, la *digital forensics*, finalizzata all'individuazione delle prove nei supporti informatici.

Il filo conduttore che lega ogni capitolo di questa disamina consiste nell' evidenziare il dirompente impatto dell'evidenza digitale e, allo stesso tempo, fornire una visione d'insieme sugli aspetti di questo poliedrico strumento investigativo, seppur la non uniformità della materia e l'assenza di una disciplina universale hanno posto non poche difficoltà durante la stesura del lavoro.

Al fine di comprendere preliminarmente il quadro all'interno del quale ci muoviamo, in apertura verrà analizzato il panorama legislativo italiano, attraverso un *excursus* sull'evoluzione normativa che ha caratterizzato i *cyber-crimes*, dalla legge n. 547 del 1993 alla Convenzione di Budapest e alla successiva legge di ratifica n. 48 del 2008.

Lo studio verrà poi affrontato sotto il profilo tecnico. Saranno, pertanto, esposte le principali criticità legate al rinvenimento delle prove, focalizzando l'attenzione sulle fasi della *digital forensic* e dedicando un approfondito esame al tema dell'alibi informatico e ai delitti di Garlasco e di Perugia, *leading case*s in materia di falso alibi.

Successivamente si passeranno in rassegna i mezzi di ricerca della prova digitale. Saranno prima esaminati quelli tipici, dall'ispezione al sequestro all'intercettazione di conversazioni telematiche. Si giungerà poi alla trattazione delle forme tecnologicamente piu avanzate di investigazione, soffermandoci soprattutto sullo spinoso tema del c.d. captatore informatico, di cui saranno evidenziate sia le principali questioni che nel corso del tempo hanno impegnato

dottrina e giurisprudenza sia la sua introduzione formalizzata nel codice ad opera della riforma Orlando.

Nella parte conclusiva di questo elaborato, infine, particolare attenzione sarà dedicata al documento informatico inteso come veicolo di prova nell' ambito del processo civile.

CAPITOLO 1

ASPETTI DI CARATTERE GIURIDICO DELLA *DIGITAL EVIDENCE*

1.1 Il quadro normativo

Lo sviluppo tecnologico informatico che ha caratterizzato l'ultimo trentennio ha favorito la nascita e la proliferazione di una nuova branca di studio di fatti penalmente rilevanti la cui connotazione principale – insieme ad altre, che si tratteranno nel corso della presente trattazione – è quella del *locus commissi delicti*, che, per la prima volta, non coincide più – almeno *prima facie* – con un luogo fisico tradizionalmente inteso, bensì con il cosiddetto *cyber*-spazio[1].

Tentando una preliminare, nonché parziale, definizione, potremmo dire che i *cyber crime* è quel delitto coincidente con un fatto umano, commissivo o omissivo, antigiuridico e colpevole, posto in essere in danno a un sistema o a un programma informatico o telematico, ovvero per mezzo degli stessi, che richiede, dunque, per la sua consumazione, l'utilizzo di un sistema di elaborazione[2].

La creazione di tali fattispecie ha indotto il legislatore, non soltanto nazionale, a prevedere una serie di normative volte a regolare la materia dei reati informatici, disciplina particolarmente complessa, dato l'elevato *standard* di competenze tecniche richieste per approcciarvisi e data, altresì, la delicatezza delle questioni ad essa sottese[3].

È evidente, infatti, come tali difficoltà eminentemente tecnico-pratiche vadano di pari passo con una serie di problematiche prettamente penalistiche e processualpenalistiche. Si vedrà come il modo di atteggiarsi dei delitti *de*

[1] C. PECORELLA, *Il diritto penale dell'informatica*, Milano, 2006.

[2] Tale definizione è tratta dall'art. 1 della Convenzione di Budapest, che verrà trattata *infra* in maniera maggiormente approfondita.

[3] C. PECORELLA, *Il diritto penale dell'informatica*, cit.

quibus abbia reso opportune alcune riflessioni, tutt'altro che sopite, volte a far combaciare gli stessi con la dottrina penalistica sostanziale e procedimentale.

Il legislatore è, dunque, intervenuto colmando, spesso su impulsi di matrice sovranazionale, il *vulnus* che la nascita dei cosiddetti *computer crimes* aveva lasciato scoperto. Mentre, è stata prevista un'apposita disciplina per le fattispecie di reato tradizionali per le quali si è assistito alla nascita di una loro corrispondente versione informatica, è stato, altresì, necessario procedere alla creazione di determinate figure delittuose *ad hoc*, prima del tutto sconosciute, che si passeranno in rassegna in via massimamente sintetica nel prosieguo del presente elaborato.

1.1.1 La Legge 547/93 sui reati informatici

Il primo intervento normativo sufficientemente organizzato nella materia *de qua* all'interno del nostro ordinamento è avvenuto ad opera della Legge 23 dicembre 1993, n. 547, recante "modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", entrata in vigore il 14 gennaio 1994[4].

L'esigenza di un provvedimento normativo volto ad un'ordinata previsione dei reati informatici era fortemente sentita, posto che, prima della sua emanazione, la dottrina e la giurisprudenza di legittimità avevano, non senza difficoltà, tentato di ricondurre tali fattispecie a quelle tradizionali già previste nel codice di riferimento, con evidenti problemi in punto di rispetto del principio di tassatività e, più in generale, di quello di legalità.

Ma se tale operazione, già di per sé, aveva presentato sufficienti problematiche, la principale questione rimasta irrisolta verteva, invece, sui delitti posti in essere attraverso l'elaboratore che coinvolgevano non tanto l'*hardware*, quanto il *software* e i dati in esso contenuti[5].

[4] L. LUPARIA, *Sistema penale e criminalità informatica*, Milano, 2009.

[5] L. LUPARIA, *Sistema penale e criminalità informatica*, cit.

Con l'intervento normativo in esame, pertanto, il legislatore italiano, colmando le predette lacune e tentando di uniformarsi a quanto già previsto in ambito internazionale, ha disciplinato, per la prima volta, nuove forme di aggressione criminosa, inserendole nel codice penale e collocandole accanto alle fattispecie tradizionali di riferimento.

Tale collocazione, tutt'altro che priva di significato, deriva dalla precisa scelta operata dal legislatore di non considerare i *cyber crimes* come delitti offensivi di beni giuridici nuovi rispetto a quelli tutelati dalle fattispecie incriminatrici preesistenti[6].

Prima di elencare e fornire una breve analisi delle principali figure delittuose introdotte dalla Legge 547/93, è opportuno segnalare che le aggressioni che essa mira a reprimere e punire sono, sostanzialmente, quella alla riservatezza dei dati e delle comunicazioni informatiche, quella all'integrità dei dati e dei sistemi informatici, le condotte in tema di falsità, nonché la gamma delle cosiddette frodi informatiche.

I reati introdotti dalla legge in oggetto sono i seguenti: l'accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.); la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.); la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-*quinquies* c.p.); l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.); l'installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.); la falsificazione, l'alterazione o la soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-*sexies* c.p.); il danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.) e la frode informatica (art. 640-*ter* c.p.)[7].

Il medesimo intervento normativo ha, inoltre, previsto la modifica delle fattispecie di cui agli artt. 392 c.p., riguardante l'esercizio arbitrario delle proprie ragioni, 616 c.p., in tema di violazione, sottrazione o soppressione di

[6] C. PECORELLA, *Il diritto penale dell'informatica*, cit.

[7] C. PECORELLA, *Il diritto penale dell'informatica*, cit.

corrispondenza e 621 c.p., relativamente alla rivelazione del contenuto di documenti segreti.

Nella stessa circostanza, il legislatore ha, infine, provveduto ad estendere il campo di azione del delitto di attentato a impianti di pubblica utilità, disciplinato dall'art. 420 c.p., nonché le ipotesi di falsità, regolate dal Capo III del Titolo VII, fino a ricomprendervi i documenti informatici[8].

Prendendo le mosse dalla fattispecie disciplinata dalla norma dell'art. 615-*ter* c.p., si rileva che l'art. 4 L. 547/93 ha previsto come reato la condotta di chi, abusivamente, s'introduce in un sistema informatico o telematico[9], purché esso sia protetto, ovvero la condotta di chi vi permane contro la volontà di chi è titolare dello *ius excludendi*.

Con tale norma, il legislatore intende, dunque, punire chi viola la riservatezza delle comunicazioni o delle informazioni trasmesse attraverso un sistema informatico, indipendentemente dalla rivelazione a terzi delle informazioni indebitamente captate o dal danneggiamento del sistema medesimo. Quest'ultima condotta, ininfluente ai fini del perfezionamento del delitto *de quo*, ne costituisce una circostanza aggravante, segnatamente prevista dal comma 2, n. 3 dell'art. 615-*ter* c.p.

Senza dilungarsi oltremodo sul punto, è agevole comprendere come, già da una prima lettura della norma, la condotta ivi punita risulti di difficile individuazione in concreto[10]. Alcuni[11] ritengono che la norma punisca esclusivamente l'ingresso virtuale nel sistema, compiuto mediante apparecchi elettronici o telematici tali da consentire lo scambio di informazioni. Secondo

---

[8] C. PECORELLA, *Il diritto penale dell'informatica*, cit.

[9] La definizione di "sistema informatico" è rinvenibile nell'art. 1 della Convenzione di Budapest: *"computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"*. Trattasi di una definizione particolarmente ampia, che permette di includere nella disciplina della Convenzione qualsiasi strumento informatico o telematico, come, ad esempio, ogni dispositivo elettronico dotato di *software* o di *firmware* che gli permetta il funzionamento mediante l'elaborazione dell'informazione, come, *ex multis*, un telefono cellulare.

[10] L. LUPARIA, *Sistema penale e criminalità informatica*, cit.

[11] Si segnala, in particolare, R. BORUSSO – S. RUSSO – C. TIBERI, *L'informatica per il giurista. Dal* bit *a* internet, Milano, 2009.

altri[12], invece, il delitto si configura anche con il mero ingresso materiale nei locali in cui si trova l'elaboratore e ciò sulla scorta del fatto che esiste un'ipotesi aggravata della fattispecie che si perfeziona attraverso l'uso della violenza (segnatamente, il comma 2, n. 2).

Dal dato letterale ci si avvede di come la norma sia modellata sulla scorta di quanto previsto per la fattispecie tradizionale della violazione di domicilio, di cui al vicino art. 614 c.p. Invero, il bene giuridico tutelato dalla norma di cui all'art. 615-*ter* c.p. è il cosiddetto domicilio informatico, inteso proprio quale estensione di quello fisico.

Trattandosi, a differenza di quest'ultimo, di uno spazio caratterizzato da apertura e flessibilità, esso può divenire oggetto di tutela soltanto in base alla volontà del suo titolare di renderlo riservato, volontà che deve emergere in tutta la sua evidenza. Si richiede, infatti, esplicitamente, che il sistema violato sia protetto da una forma di sicurezza[13].

L'art. 615-*quater* c.p. prevede un'altra forma di reato, anch'esso introdotto dall'art. 4 L. 547/93, che punisce la condotta di chi, abusivamente, si procura, riproduce, diffonde, comunica o consegna i codici di accesso a sistemi informatici, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Anche in questo caso, il delitto si perfeziona a prescindere dall'utilizzo dei codici dei quali si sia entrati in possesso. Ciò che è richiesto, ancora una volta, è che il sistema informatico sia protetto da misure di sicurezza. Trattandosi, evidentemente, di un reato di pericolo, in quanto tale volto ad evitare la consumazione di delitti più gravi, quali quelli contro la riservatezza (*ex multis*, l'esaminato reato di cui all'art. 615-*ter* c.p.) o contro il patrimonio (come la frode informatica, disciplinata dalla norma dell'art. 640-*ter* c.p., della quale si tratterà *infra*).

---

[12] In particolare, si segnala E. GIANNANTONIO, *L'oggetto giuridico dei reati informatici,* nell'ambito del Seminario su Computer crimes*: i reati informatici* del 15 e 16 dicembre 2000, in http://www.giustizia.it/cassazione/convegni/dic2000/giannantonio.pdf.

[13] Cass. pen., sez. V, 7 novembre 2000, n. 12732 fa riferimento sia a strumenti di protezione logica, come l'impostazione di un *account* o l'adozione di un *firewall*, sia a strumenti di protezione fisica atti a custodire materialmente l'impianto.

La norma *de qua* punisce anche chi permette ad altri la possibilità di porre in essere i descritti comportamenti attraverso l'indicazione di istruzioni tecniche. L'art. 615-*quinquies* c.p. si pone a completamento della normativa qui richiamata, volta a tutelare, nella sua globalità, il diritto dell'individuo di godere in modo indisturbato del proprio sistema informatico, senza subire alcun danno illecito.

Tale fattispecie, finalizzata alla repressione della diffusione – particolarmente ampia – dei cosiddetti virus informatici[14], è stata oggetto di correttivi ad opera della L. 48/08 di ratifica della Convenzione di Budapest del 13 novembre 2001.

In particolare, si segnala che la fattispecie, che già sanzionava la diffusione, la comunicazione e la consegna di programmi informatici virali, ad opera delle anzidette modifiche ricomprende, oggi, anche le attività consistenti nel procurarsi, produrre, riprodurre, importare o mettere a disposizione di altri i programmi e le apparecchiature informatiche[15].

L'art. 617-*quater* c.p. e l'art. 617-*quinquies* c.p. sanzionano, rispettivamente, chi, senza esserne autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e chi installa apparecchiature dirette a intercettare, interrompere o impedire tali comunicazioni.

Le norme in esame, al pari di quella contenuta nell'art. 617-*sexies* c.p., di cui si dirà, si riferiscono a comunicazioni informatiche in cui si ha una precisa identificazione del destinatario. In mancanza di ciò, quando, cioè, i destinatari sono indecifrabili, non essendo individuabile una corrispondenza inviolabile, il reato non si configura. La fattispecie di cui all'art. 617-*quinquies* c.p. configura un reato di pericolo: se verrà portata a compimento la condotta vietata dall'art. 617-*quater* c.p., l'autore risponderà a tale titolo.

Il citato art. 617-*sexies* c.p. punisce, invece, chi falsifica, altera o sopprime il contenuto di comunicazioni informatiche, allo scopo specifico di

[14] Per tali s'intendono programmi che si attivano da soli in un determinato momento temporale o al verificarsi di una data condizione e che sono forieri di gravi danni ai sistemi informatici o telematici, impiegati, solitamente, per scopi di sabotaggio.

[15] L. LUPARIA, *Sistema penale e criminalità informatica*, cit.

procurare a sé o ad altri un vantaggio e di arrecare ad altri un danno. Per il perfezionamento di tale delitto occorre che l'autore faccia uso di queste comunicazioni o, comunque, ne permetta ad altri l'utilizzo. Ai sensi dell'art. 635-*bis* c.p. risponde penalmente chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Particolarmente interessanti sono i correttivi introdotti in questo ambito dalla Convenzione di Budapest, che ha inteso distinguere tra il danneggiamento di informazioni, dati e programmi e quello di sistemi informatici o telematici[16].

Prima della sua riscrittura ad opera della citata Convenzione, la dottrina[17] aveva sottolineato che la norma *de qua* si limitava a riprodurre pedissequamente le condotte tipiche della fattispecie tradizionale di danneggiamento (distruggere, deteriorare, rendere inservibili), senza tener conto della peculiarità dei beni aggrediti.

Per tale ragione, con i predetti correttivi, il legislatore ha provveduto ad inserire all'interno della norma le aggressioni che possono caratterizzare i beni informatici *de quibus*, quali la cancellazione, l'alterazione e la soppressione. È preferibile, pertanto, esaminare la fattispecie di cui all'art. 635-*bis* c.p. congiuntamente alle successive.

Invero, proprio ad opera dello spacchettamento operato dalla Convenzione di Budapest, sono, oggi, presenti nel codice, oltre al citato art. 635-*bis* c.p., l'art. 635-*ter* c.p., che prevede la punibilità della medesima condotta qualora le informazioni, i dati e i programmi aggrediti siano di pubblica utilità e i corrispondenti artt. 635-*quater* e 635-*quinquies* c.p., i quali prevedono, rispettivamente, il danneggiamento di sistemi informatici o telematici e il medesimo danneggiamento qualora tali sistemi siano dello Stato, di un ente pubblico o, comunque, di pubblica utilità[18].

---

[16] La definizione di "dato informatico" è rinvenibile nel citato art. 1 della Convenzione di Budapest, ove si legge che *"computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"*.

[17] In particolare, s.v. G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 2000.

[18] G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, n. 3, 2010.

L'art. 635-*quinquies* c.p. si pone come norma di sbarramento preventiva rispetto alle descritte fattispecie, costituendo un reato di pericolo e non di danno, punendo i fatti diretti ad ostacolare gravemente il funzionamento del sistema. A differenza di quanto avviene con riferimento all'art. 635-*bis* c.p., nella norma dell'art. 635-*quinquies* c.p. non viene fatta menzione dell'appartenenza di tali sistemi allo Stato o ad altri enti pubblici, bensì alla sola pubblica utilità degli stessi.

Anticipando la soglia del penalmente rilevante a un momento precedente, prodromico soltanto eventualmente al conseguimento del fine lesivo, qualora esso venga effettivamente raggiunto, l'autore incorrerà in un aggravio sanzionatorio. Notevolmente importante è la figura delittuosa disciplinata dall'art. 640-*ter* c.p., ossia la cosiddetta frode informatica, introdotta dall'art. 10 L. 547/93, con il quale è stato esteso quanto previsto dall'art. 640 c.p., con riferimento alla tradizionale figura della truffa, ad un altro e differente oggetto della condotta, che non investe, qui, una persona fisica, bensì un sistema informatico.

L'esigenza di tale previsione è stata avvertita segnatamente a causa delle difficoltà che incontrava la giurisprudenza nel configurare tali condotte come truffa, posto che, appunto, esse non si traducevano nell'induzione in errore di una persona, con tutti gli annessi – nonché particolarmente rilevanti – risvolti di natura psicologica, bensì di un elaboratore elettronico. La prevalente dottrina [19] ha elaborato tre principali tipi di condotta: l'alterazione o l'immissione di dati, l'alterazione dei *software* finalizzata alla frode e l'alterazione delle informazioni.

Ai fini del perfezionamento del delitto *de quo* è richiesta la percezione di un ingiusto profitto con relativa causazione di un altrui danno: tale è il momento di consumazione del reato. Interessanti sono anche le sue ipotesi circostanziate: il medesimo articolo prevede, quali circostanze aggravanti, la commissione del fatto a danno dello Stato o di un ente pubblico o con lo scopo di far esonerare taluno dal servizio militare, la commissione mediante abuso

[19] R. BORUSSO – S. RUSSO – C. TIBERI, *L'informatica per il giurista. Dal* bit *a* internet, Milano, 2009.

della qualità di operatore del sistema e, soprattutto, la commissione mediante furto o, comunque, utilizzo indebito di un'identità digitale.

Tale ultima circostanza aggravante, particolarmente rilevante a causa della sua ampia diffusione nella prassi, è stata introdotta ad opera di un successivo intervento normativo, coincidente con il D.L. 93/13, convertito con L. 119/13, provvedimento inizialmente nato come cosiddetto decreto anti-femminicidio e violenza di genere e, poi, esteso nella sua portata riformatrice.

Relativamente alle ulteriori modifiche operate dalla L. 547/93 richiamate in apertura, è opportuno sottolineare che, con riferimento al reato di esercizio arbitrario delle proprie ragioni mediante violenza sulle cose di cui all'art. 392 c.p., il predetto intervento normativo ha provveduto a modificare la norma *de qua* specificando che si ha violenza sulle cose anche qualora venga alterato, modificato o cancellato, in tutto o in parte, un programma informatico o sia turbato il funzionamento di un sistema informatico o telematico[20].

E ancora, come anticipato, sempre la L. 547/93 ha modificato l'art. 616 c.p. avente ad oggetto la tutela del bene giuridico della segretezza e dell'inviolabilità della corrispondenza, garantito dall'art. 15 Cost., estendendo il concetto di "corrispondenza", fino a ricomprendervi, in aggiunta a quelle epistolare, telegrafica e telefonica, anche quella informatica o telematica.

Lo stesso può dirsi essere avvenuto con riferimento alla fattispecie di rivelazione del contenuto di documenti segreti di cui all'art. 621 c.p. a quelle inerenti i reati di falsità cui al Capo III, Titolo VII, ora estesi anche ai documenti informatici e al concetto di "impianto di pubblica utilità" rinvenibile nella norma dell'art. 420 c.p., i cui commi 2 e 3 risultano abrogati, poiché, oggi, inseriti nell'art. 635-*quiquies* c.p., di cui si è detto *supra*, ad opera della ratifica nel nostro ordinamento della Convenzione di Budapest, della quale ci si accinge a trattare[21].

---

[20] L. LUPARIA, *Sistema penale e criminalità informatica*, cit.

[21] Per quanto concerne le modifiche introdotte al codice di procedura penale, ci si riserva un esame delle stesse in seguito, nell'ambito riservato alla trattazione procedurale della *digital evidence*.

1.1.2 La Convenzione di Budapest del 2001 e la legge di ratifica 48/08

Con la Legge n. 48 del 18 marzo 2008 è stata ratificata nel nostro ordinamento la Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001. Questo risultato è il frutto di svariati anni di lavoro di un gruppo di esperti, il Comitato Europeo per i Problemi Criminali (CEPC), istituito nel 1996. Tale intervento normativo interno ha reso necessaria una serie di correttivi in *subiecta materia*[22].

Come emerge con estrema chiarezza dal suo preambolo, la questione preminente e ineludibile sottesa all'emanazione della Convenzione può dirsi coincidente con la creazione di una politica comune agli Stati dell'Unione in materia di reati informatici, finalizzata alla protezione della società contro questa tipologia di delitti. Ciò che ha reso necessario tale intervento comune è costituito dai profondi cambiamenti dipesi dall'introduzione della tecnologia digitale, nonché dalla costante e progressiva globalizzazione che ha caratterizzato le reti informatiche.

La Convenzione di Budapest si pone, dunque, a tutela delle condotte penalmente rilevanti mirate a ledere – o a porre in pericolo – la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati in essi contenuti, scongiurando, così, anche l'uso improprio di tali sistemi, reti e informazioni[23].

Uno dei punti chiave del testo normativo, che, come si vedrà, assume un ruolo centrale nella presente materia, è la ricerca di un doveroso bilanciamento – non sempre agevole – tra l'interesse sotteso all'azione repressiva delle predette condotte e il rispetto dei fondamentali diritti dell'individuo, i quali non possono essere oltremodo compromessi o anche soltanto compressi, neppure dinanzi alla straordinaria pervasività dei delitti *de*

[22] G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, cit.

[23] G. COSTABILE, Computer forensics *e informatica investigativa alla luce della Legge n. 48 del 2008*, cit.

quibus[24]. Per tali ragioni, come si è anticipato, sono stati posti in essere alcuni correttivi all'interno del codice penale e del codice di procedura penale[25].

Inoltre, la normativa in oggetto ha introdotto all'interno dell'ordinamento nazionale, segnatamente nel corpo del D.Lgs. 231/01, l'art. 24-*bis*, recante la previsione di nuove fattispecie di reato in materia di delitti informatici e, in generale, di trattamento illecito di dati.

Come è emerso nel corso della trattazione precedente, nell'art. 1 della Convenzione si rinvengono una serie di definizioni che assumono una notevole rilevanza nel presente ambito e ciò poiché, nell'anzidetta norma, più volte richiamata *supra*, viene chiarita per la prima volta, in maniera chiara, univoca, nonché accettata da tutti gli Stati membri che hanno ratificato il trattato, la definizione di "sistema informatico", di "programma informatico" e di "dato informatico".

La legge di ratifica della Convenzione di Budapest ha proseguito nello schema già tracciato dal legislatore con la L. 547/93: i *cyber crimes* sono stati collocati, ancora una volta, all'interno dei Capi e dei Titoli preesistenti, accanto alle tradizionali fattispecie incriminatrici previgenti.

Questo perché, com'è evidente anche da una sommaria lettura dei delitti di che trattasi, non è, in alcun modo, dato individuare un unico bene giuridico alla cui tutela siano poste le differenti fattispecie ivi disciplinate.

Le principali modifiche operate dalla Convenzione hanno riguardato l'art. 491-*bis* c.p. in tema di falso informatico, l'art. 495-*bis* c.p. con riferimento alla falsa dichiarazione o attestazione al certificatore di firma elettronica, il già analizzato art. 615-*quinquies* c.p. riguardante la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico, gli artt. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* c.p. relativamente alle già descritte condotte di danneggiamento

[24] S.v. G. BRAGHÒ, *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa*, in *Dir. inf. e informatica*, 2005.

[25] Per quanto riguarda le modifiche introdotte agli articoli del codice di procedura penale si segnalano, principalmente, quelle in materia di ispezioni, perquisizioni e sequestri, delle quali si tratterà *infra*.

informatico e l'art. 640-*quinquies* c.p. in materia di frode informatica del certificatore.

Mentre con riferimento alle citate modifiche all'art. 491-*bis* c.p. ci si può limitare ad affermare che il legislatore ha semplicemente abrogato il secondo periodo del comma 1, il quale stabiliva una definizione di "documento informatico", ormai ritenuta superata, maggiormente interessanti sono le considerazioni da svolgere relativamente alla nuova figura delittuosa prevista dall'art. 495-*bis* c.p.[26]

Ai sensi di tale previsione è punito chiunque renda al certificatore di firma elettronica dichiarazioni o attestazioni false, ideologicamente o materialmente, sull'identità o su qualità personali proprie o di altri. L'art. 7 della Convenzione, introducendo questa nuova fattispecie incriminatrice, pare, dunque, voler prevedere la disciplina di una norma volta alla tutela della firma digitale, la quale, per essere generata, necessita, appunto, di un soggetto certificatore.

Qui, infatti, risiede l'elemento specializzante di tale reato rispetto a quello – tradizionale – previsto dall'art. 495 c.p.: il destinatario della falsa dichiarazione o attestazione penalmente rilevante non è più il pubblico ufficiale redigente un atto pubblico, bensì un soggetto che presta servizi di certificazione delle firme elettroniche[27].

Analoga importanza assume la nuova previsione del delitto contenuto nella norma dell'art. 640-*quinquies* c.p., previsione resa indispensabile per coprire il *vulnus* lasciato dalla fattispecie di cui al citato art. 640-*ter* c.p., ove non potevano ritenersi rientranti determinate condotte, le quali restavano, pertanto, sprovviste di un adeguato profilo sanzionatorio[28].

---

[26] L. LUPARIA, *Sistema penale e criminalità informatica*, cit.

[27] In campo definitorio occorre rivolgersi al D.Lgs. 82/05, secondo il quale per "firma elettronica" s'intende l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica; e per "certificatore" s'intende il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

[28] La predetta esigenza emerge dall'art. 8 della Convenzione, dedicato alla frode informatica. Tale previsione impegna gli Stati aderenti ad attribuire rilevanza penale al fatto di