SERIE BUSSOLA: orientamenti legislativi 159

Paolo Scognamiglio

Criminalità informatica

Commento organico alla Legge 18 marzo 2008, n. 48

2008

EDIZIONI GIURIDICHE SIMONE®

Gruppo Editoriale Esselibri - Simone

Paolo Scognamiglio

Criminalità informatica

Commento organico alla Legge 18 marzo 2008, n. 48

2008

EDIZIONI GIURIDICHE SIMONE®

Gruppo Editoriale Esselibri - Simone

Ha collaborato alla revisione del testo il dott. Rocco Pezzano

---

Finito di stampare nel mese di maggio 2008
dalle «Arti Grafiche Italo Cernia» - Via Capri, n. 67 - Casoria (NA)
per conto della Esselibri S.p.A. - Via F. Russo 33/D - 80123 - Napoli

Grafica di copertina a cura di Giuseppe Ragno

PREMESSA

La legge 18 marzo 2008, n. 48 ratifica la Convenzione del Consiglio d'Europa sulla Criminalità informatica (cd. Convenzione di Budapest) del 23 novembre 2001.

La Convenzione di Budapest è entrata in vigore il 1 luglio 2004 ed ha rappresentato il primo accordo internazionale riguardante i crimini commessi attraverso le reti informatiche.

L'approvazione della Legge 48/2008, oltre che consentire al nostro Paese di assolvere agli obblighi assunti in sede internazionale, ha costituito l'occasione per adeguare la normativa del codice penale e del codice di rito in tema di reati informatici alle esigenze che si erano venute a manifestare dopo quasi quindici anni di applicazione della legge 547/1993 che rappresentò il primo intervento organico in tema di criminalità informatica.

La presente opera fornisce una prima lettura ragionata della riforma, con un commento articolo per articolo, che evidenzia le differenze tra la nuova formulazione e le norme sostituite e vuole rappresentare un piccolo aiuto a tutti gli operatori del diritto che nei prossimi mesi (ed anni) si troveranno ad applicare la nuova disciplina.

Lungi poi ogni pretesa di completezza, il volume comprende un capitolo finale dedicato ad alcune figure di reati informatici, già previste dal codice penale e non modificate dalla presente legge, nel quale ci si sofferma essenzialmente sui problemi di carattere interpretativo sorti in questi anni.

Completa il volume una appendice normativa e giurisprudenziale.

Si ringrazia il dott. Rocco Pezzano per la collaborazione prestata nella revisione del testo.

Capitolo Primo

La criminalità informatica

Sommario

1. L'ORIGINE DELLA TUTELA DEI BENI INFORMATICI: DAI PRIMI INTERVENTI ALLA LEGGE 547/1993

Il rilievo acquisito nella società contemporanea dai procedimenti di informazione automatizzata effettuati attraverso l'impiego di elaboratori elettronici, nonché delle reti di trasmissione telematica, già a partire dai primi anni ottanta, mise in evidenza la necessità di tutelare i cd. beni informatici, anche attraverso la predisposizione di un sistema di fattispecie penali *ad hoc* (i cd. computer crimes).

Nel nostro Paese vi furono primi timidi interventi settoriali quali il decreto legge 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978 n. 191, che, nel reintrodurre nel codice penale l'articolo 420 c.p. che sanzionava l'attentato ad impianti di pubblica utilità, menzionava espressamente anche gli impianti di elaborazione di dati o la legge 1º aprile 1981 n. 121, contenente il «Nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza», istitutiva di un Centro di elaborazione dati presso il Ministero dell'Interno, che introduceva il delitto di comunicazione od uso, da parte del pubblico ufficiale, di dati ed informazioni in violazione della disciplina o dei fini previsti dalla stessa normativa.

Altro più severo, ma sempre settoriale intervento, si registrò in campo tributario con la previsione dell'art. 2, 7° comma, l. 26 gennaio 1983, n. 18 sui cd. registratori di cassa, che introdusse la prima fattispecie penale esplicitamente incriminatrice delle falsificazioni o

manipolazioni informatiche, punendo fra l'altro la «manomissione ed alterazione di apparecchi misuratori fiscali (1)».

Mancava però un intervento di carattere organico ed in difetto di specifiche previsioni la giurisprudenza cercava di ricondurre le figure criminose che la realtà andava proponendo alle fattispecie tradizionali.

Ciò non creava particolari problemi per le condotte che avevano ad oggetto la parte fisica del sistema informatico (hardware), che poteva trovare facile riconoscimento nelle ipotesi classiche del danneggiamento, del furto, ecc., ma notevoli difficoltà si presentavano per l'incriminazione di condotte, quali ad esempio truffe commesse attraverso l'elaboratore nelle quali gli «artifizi e i raggiri» non erano volti ad indurre un soggetto in errore, quanto ad incidere sul funzionamento di una macchina, di un elaboratore (2).

Ugualmente appariva difficile ricomprendere il software, i dati e le informazioni custodite negli elaboratori tra i beni materiali tutelati dal delitto di danneggiamento o tra le cose mobili contemplate dall'art. 624 c.p., per i casi di furto; tra l'altro, dal momento che il «furto» di regola veniva realizzato attraverso la semplice duplicazione del software o dei dati, senza cancellazione dell'originale, non appariva comunque punibile ai sensi dell'art. 624 c.p., mancando, tra gli elementi essenziali del reato, lo «spossessamento» fisico del bene.

---

(1) V. PICOTTI, *I reati e gli illeciti amministrativi in materia di registratori di cassa, bilance e terminali elettronici,* in *Giurisprudenza sistematica di diritto penale. I reati in materia fiscale,* a cura di P.M. Corso e L. Stortoni, Torino, 1990, 433 ss.

(2) Non mancarono pronunce giurisprudenziali che riconducevano ugualmente tali condotte alle figure codicistiche: si veda Trib. Como, 21 settembre 1995, in *Informaz. prev.*, 1995, n. 12, 1545, che ritenne applicabili le norme relative al falso in atto pubblico (art. 476 c.p.) ed alla tentata truffa (art. 640 c.p.) ad alterazioni dell'archivio informatico dell'I.N.P.S commesse prima dell'emanazione della legge in esame ed ancora prima la giurisprudenza romana Trib. Roma, 20 giugno 1984, Testa ed altri che ritenne applicabile l'art. 640 c.p. nel caso di immissione nell'elaboratore elettronico dell'I.N.P.S. di dati non veritieri relativi a contributi in realtà non versati, ritenendosi, peraltro, che in tal modo fossero ingannati i dipendenti preposti al controllo del versamento dei contributi e all'esazione degli stessi, e non il computer.

Venne altresì ravvisato il delitto di truffa aggravata nel caso di un dipendente bancario che, inserendo falsi dati nell'elaboratore, aveva ottenuto che risultassero come avvenuti per contanti versamenti effettuati mediante assegni, al fine di occultare il maggior rischio assunto con la negoziazione di assegni prima che ne fosse stata confermata la copertura e per procurare il maggior lucro ai correntisti attraverso il riconoscimento della valuta liquida (Trib. Roma, 14 dicembre 1985, Manenti ed altri).

La giurisprudenza, con una opera ardua (3), aveva cercato di estendere le figure criminose tradizionali alle nuove condotte, ma certamente non appariva infondato il timore che tale *modus operandi* avrebbe potuto tradursi in un'inaccettabile violazione del principio di tassatività.

Ecco che quindi agli inizi degli anni novanta i tempi apparivano maturi per un intervento di carattere ampio e così il legislatore intervenne con L. 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».

Il legislatore italiano si mosse seguendo le indicazioni provenienti dal Consiglio d'Europa che aveva provveduto a suggerire alle nazioni aderenti due diverse liste di reati da considerare ed eventualmente introdurre nei rispettivi ordinamenti, una cd. minima, consistente nelle fattispecie ritenute necessarie (es.: la frode informatica, intesa, fra l'altro, quale ingresso, alterazione, cancellazione o soppressione di dati e programmi informatici, e l'intercettazione non autorizzata di comunicazioni inviate, provenienti o esistenti nell'interno di un sistema o di una rete informatica) ed un'altra, facoltativa, includente fattispecie ritenute non essenziali, ma opportune, la cui concreta introduzione avrebbe dovuto essere considerata da ciascuno Stato sulla base dell'armonizzazione con il proprio sistema penale preesistente (tale novero comprendeva ad es.: l'alterazione di dati o dei programmi informatici, da parte di chi non avesse diritto di intervenire su di essi) (4).

L'intervento si realizzò non con una legge *ad hoc* dedicata ai reati informatici, ma con l'inserimento delle nuove fattispecie penali all'interno del corpo del codice penale.

La scelta riflette indubbiamente la consapevolezza che non si trattava di introdurre fattispecie che tutelassero nuovi beni giuridici,

---

(3) Oltre alle pronunce citate alla nota precedente v. Pret. Torino 23 ottobre 1989 (in *Foro it.*, 1990, II, 462) che ritenne configurabile il delitto di danneggiamento nella condotta di chi, mediante una serie di istruzioni indirizzate al calcolatore elettronico, cancelli o alteri alcuni programmi applicativi contenuti in supporti magnetici, in quanto «la cancellazione dei nastri di *backup* e l'introduzione di istruzioni nel programma idonee a disabilitare il sistema informatico ad una data prestabilita, rendono inservibile il sistema stesso, comportandone l'alterazione strutturale e funzionale».

(4) V. AA.VV., *Temi & Percorsi di Diritto penale,* Napoli, 2007, p. 1079.

ma di introdurre delle tutele contro nuove forme di aggressione, portate cioè con modalità nuove, a beni in larga parte già penalmente rilevanti e tutelati con le norme codicistiche.

Del resto la creazione di una ennesima legge speciale avrebbe finito per confinare la materia in un settore non centrale dell'ordinamento (5).

Ecco quindi che si cercò soprattutto di estendere espressamente le vigenti previsioni codicistiche (es.: delitto di danneggiamento, truffa) alle nuove condotte che la realtà andava proponendo e vennero introdotte nel codice figure come la frode informatica, il delitto di danneggiamento di sistemi informatici, l'accesso abusivo ad un sistema informatico, ma pare inutile soffermarsi ulteriormente sulle figure criminose introdotte dalla legge 547/1993 sulle quali si ritornerà nel Capitolo III del presente lavoro.

2. LA CONVENZIONE DI BUDAPEST E LA LEGGE 48/2008

A distanza di quasi quindici anni dal precedente intervento è giunta la legge in commento che ratifica la Convenzione di Budapest 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica, convenzione che rappresenta il primo accordo internazionale riguardante i crimini commessi attraverso internet o le altre reti informatiche, con l'obiettivo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata che consenta di contrastare il crimine informatico in maniera coordinata.

Gli obiettivi fondamentali della Convenzione consistevano essenzialmente nell'armonizzazione degli elementi fondamentali delle fattispecie di reato previste dai singoli ordinamenti interni e nel dotare i singoli Paesi di una normativa efficace per lo svolgimento delle indagini ed il perseguimento dei crimini correlati all'area informatica.

La Convenzione aveva una portata piuttosto ampia, comprensiva di norme in tema di pornografia infantile, attentati contro la proprietà intellettuale, ma numerose disposizioni non sono state ade-

(5) Così BERGHELLA-BLAIOTTA, *Diritto penale dell'informatica e dei beni giuridici*, in *Cassazione Penale* 1995, pag. 2330 e PICOTTI, *Reati informatici* (voce)*, Enc. Giur.Treccani,* 1999, p. 5.

guate sulla base del presupposto che la nostra legislazione già prevedeva specifiche norme, ritenute in alcuni casi, anche più *avanzate* delle previsioni convenzionali.

La stessa Convenzione, all'articolo 15, sanciva inoltre in capo agli Stati firmatari l'obbligo di prevedere istituti di garanzia tali da assicurare che le misure processuali introdotte per l'accertamento e la repressione dei reati informatici venissero applicate nel rispetto dei diritti umani e delle libertà fondamentali.

Tale esigenza viene richiamata nella relazione al disegno di legge (6) che ha portato all'approvazione della legge 48/2008, ove si afferma che si è inteso salvaguardare il rispetto del principio di proporzionalità, *onde evitare di configurare incriminazioni caratterizzate da livelli sanzionatori che avrebbero potuto cagionare all'individuo ed alla società danni sproporzionatamente maggiori dei vantaggi ottenuti con la tutela dei beni e dei valori offesi dalle predette incriminazioni*.

Ciò posto, va osservato che il testo della legge 48/2008 si compone di quattordici articoli, suddivisi in quattro capi, di cui il capo I ed il capo IV contengono disposizioni sostanzialmente procedimentali (autorizzazione al Presidente della Repubblica a ratificare la convenzione, entrata in vigore della norma), mentre la parte centrale e pregnante del decreto è costituita dai capi II e III che comportano innovazioni al codice penale ed al codice di procedura penale ed è soprattutto su queste norme che concentreremo la nostra attenzione.

(6) V. relazione al disegno di legge C 2087, Camera dei deputati, ultima legislatura.

Capitolo Secondo

La legge 48/2008 articolo per articolo

Sommario

1. L'ESECUZIONE DELLA CONVENZIONE (ARTICOLI 1 E 2)

Capo I
Ratifica ed esecuzione

Art. 1
Autorizzazione alla ratifica

1. Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata «Convenzione».

Art. 2
Ordine di esecuzione

1. Piena e intera esecuzione è data alla Convenzione, a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall'articolo 36 della Convenzione stessa.

Commento

Gli articoli in commento regolano l'esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

Nonostante l'articolo 2 della presente legge affermi che viene data *piena ed intera esecuzione* alla Convenzione, in realtà la Convenzione non è stata recepita integralmente ed in particolare non sono state richiamate

quelle parti come l'articolo 1 che fornisce le definizioni tecniche di sistema informatico, dato informatico etc.…

Non sono stati altresì recepiti gli articoli della Convenzione in tema di cooperazione tra gli Stati nella repressione dei crimini informatici, giurisdizione etc….

Al riguardo nella relazione al disegno di legge si evidenza che la norma di riferimento è rappresentata dall'articolo 696 del codice di procedura penale in base al quale le norme delle convenzioni internazionali in vigore per lo Stato italiano sono di diretta applicazione.

Di qui la convinzione che non vi era necessità di introdurre nell'ordinamento norme che le riproducessero: anzi la relazione sottolinea che *l'apparato normativo contenuto nel libro undicesimo del codice di procedura penale è perfettamente idoneo ad attuare le disposizioni di cooperazione internazionale contenute nella Convenzione, tanto più che si tratta di disposizioni di tipo tradizionale, comuni a molte altre convenzioni.*

Analogamente la relazione premette che *la portata dell'adeguamento normativo da realizzare nel settore del diritto penale sostanziale è risultata modesta, essendo, in molti casi, in vigore una disciplina esaustiva, addirittura più incisiva di quella richiesta dalle disposizioni della Convenzione.*

Ha suscitato invece alcune perplessità il mancato recepimento dell'art. 10, comma 2, della Convenzione che regola l'infrazione legata agli attentati alla proprietà intellettuale ed ai delitti commessi deliberatamente a livello commerciale mediante sistemi informatici (1).

La violazione del diritto d'autore, in base alle disposizioni della Convenzione, deve essere sanzionata penalmente se tali atti sono commessi deliberatamente, su scala commerciale ed attraverso l'utilizzo di un sistema informatico, ma lo Stato può riservarsi di non imporre sanzioni penali se altri rimedi efficaci sono disponibili e se non si violano gli impegni internazionali.

Si è pertanto osservato che il legislatore avrebbe potuto cogliere l'occasione per modificare l'art. 171, comma 1, lett a-bis), legge 633/1941 che punisce, con la sanzione penale della multa da euro 51 ad euro 2.065,00, «*chiunque, senza averne diritto, a qualsiasi scopo ed in qualsiasi forma, mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere un'opera dell'ingegno protetta, o parte di essa».*

La norma infatti sanziona penalmente anche condotte che non avvengono a livello commerciale, con una disciplina più severa rispetto a quanto previsto dalla Convenzione.

---

(1) MICOZZI-ATERNO, *Commento alla legge di ratifica della Convenzione di Budapest del 23 novembre 2001*, p.4., rinvenibile sul sito www. *Giuristi telematici.it.*

La critica appare condivisibile anche se va osservato che la presente legge si è limitata a modificare i *computer crimes* in senso stretto e la materia del diritto d'autore necessita probabilmente di una rivisitazione completa con una legge *ad hoc*.

2. I DELITTI DI FALSO (ARTICOLO 3)

Capo II
Modifiche al codice penale
e al decreto legislativo 8 giugno 2001, n. 231

ART. 3
Modifiche al titolo VII del libro secondo del codice penale

1. All'articolo 491bis del codice penale sono apportate le seguenti modificazioni:

a) al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»;

b) il secondo periodo è soppresso.

2. Dopo l'articolo 495 del codice penale è inserito il seguente:

«Art. 495bis. Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri. – Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno».

COMMENTO

L'articolo 3 della legge in commento si compone di due commi, dei quali, il primo modifica l'articolo 491bis che aveva previsto una nozione di documento informatico, mentre il secondo istituisce una nuova figura di reato all'articolo 495bis c.p.

È da premettere che ipotesi di falso, sia ideologico che materiale, possono aversi anche con riguardo al documento informatico.

Ora, le ipotesi di falsità ideologica non comportano significative peculiarità rispetto alle analoghe situazioni di falsi ideologici «cartacei», atteso che la falsità prescinde dalla forme dell'atto, riguardando solo la rispondenza al vero del contenuto del medesimo.

Al contrario, il falso informatico materiale, nella duplice prospettiva dell'alterazione o della contraffazione, si presenta, tendenzialmente, come una forma più insidiosa di aggressione alla veridicità e genuinità di un documento e delle notizie riservate in esso contenute.

Infatti, mentre il falso «ordinario» consiste in una modificazione della realtà pregressa del documento stesso o nella formazione dell'atto che può «tendere» alla somiglianza, ma che può anche significativamente discostarsene, presentandosi quindi come fenomeno percepibile da parte di terzi, il falso «informatico» è un documento che si presenta nella sua materialità, ossia nelle sue forme esteriori, come assolutamente identico all'originale: la sua individuazione presuppone necessariamente l'intervento di un tecnico del settore.

Pertanto, il privato cittadino mentre, salvo casi eccezionali, sarebbe in grado autonomamente di disconoscere con certezza un documento non redatto di proprio pugno, potrebbe trovarsi nella condizioni di non poter fare altrettanto con un documento informatico utilizzato, ad esempio, nell'ambito di una contrattazione (2).

Di qui la necessità di una specifica disciplina del falso in documento informatico.

Ebbene, nel testo antecedente alla presente riforma, l'articolo 491 bis, come introdotto dall'articolo 3 della legge 547/1993, statuiva «Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine *per documento informatico si intende qualunque supporto informatico contenente dati od informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarla.*

Tale nozione era criticata in quanto legata al concetto di supporto informatico e sembrava attribuire rilevanza, più che al dato informatico, all'elemento materiale sul quale era contenuto.

Inoltre, come detto, l'articolo 491bis testo previgente legava il concetto di documento a quello di programma rilevando che per documento doveva intendersi qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Orbene anche tale riferimento appariva poco lineare dal momento che il programma è uno strumento operativo e non un documento: del resto la manipolazione dei programmi informatici trova tutela nelle figure di dan-

(2) V. le considerazioni di CALICE, *I computer crimes nell'ordinamento giuridico italiano: inquadramento sistematico ed efficacia della risposta sanzionatoria»* al corso «Criminalità informatica e protocolli investigativi», Csm, Roma, 23-25 gennaio 2006, p. 24 ss.

neggiamento, di cui agli articoli 635bis e 635ter che puniscono appunto la distruzione, il deterioramento, l'alterazione o la cancellazione dei programmi informatici (3).

Vi è da dire che poi tale nozione appariva anacronistica dal momento che l'articolo 1, lett. b), D.P.R. 28-12-2000, n. 445 come sostituito dal D.P.R. 7-4-2003, n. 137, ora riprodotto nell'articolo 1, lett. p) del decreto legislativo 7-3-2005, n. 82, contenente il Codice dell'amministrazione digitale, definiva «documento informatico» la *rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*

Ci si chiedeva quindi se ai fini penalistici dovesse valere una nozione di documento informatico diversa da quella rilevante per l'ordinamento in generale.

Con la previsione in commento si elimina il legame tra l'esistenza del documento informatico e la necessaria sussistenza di un supporto: del resto già nei lavori preparatori alla presente legge si evidenzia che «*l'equiparazione tra documento e supporto rischia di apparire in qualche misura fuorviante perché attribuisce al documento informatico una pretesa dimensione materiale da cui esso, a ben vedere, proprio per le sue intime caratteristiche, prescinde*».

Di qui l'eliminazione della definizione di documento dal codice penale e dunque, allo stato, la nozione di documento, rilevante per l'ordinamento, si ricava dalla citata definizione che ne dà il Codice dell'amministrazione digitale che prescinde, come detto dalla nozione di supporto materiale.

L'articolo 491bis, 2ª parte, statuiva però che intanto il falso nel documento informatico era rilevante in quanto lo stesso avesse efficacia probatoria e l'eliminazione del secondo periodo avrebbe comportato anche l'eliminazione del requisito dell'efficacia probatoria.

Così il legislatore ha opportunamente inserito le parole «avente efficacia probatoria» nella prima parte dell'art. 491bis che, nel nuovo testo coordinato, così recita «*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private».*

Nulla la legge dice su cosa debba intendersi per efficacia probatoria del documento informatico ed al riguardo occorrerà rifarsi all'articolo 20 del Codice dell'amministrazione digitale che attribuisce rilevanza probatoria ai documenti informatici laddove siano formati nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore e l'integrità del documento.

(3) V. le considerazioni di G. AMATO, *Incerta l'efficacia probatoria del documento, Guida al diritto,* 2008, n. 16, p. 55.

Il nuovo testo dell'articolo 491bis punisce le falsità nei documenti informatici pubblici o privati attraverso un rinvio alle norme che incriminano le falsità in atti pubblici o scritture private.

Si pone naturalmente la necessità di comprendere quando si sia in presenza di un documento informatico pubblico o privato.

La questione, come è evidente, ha una notevole rilevanza pratica: si consideri ad esempio che se la falsità riguarda un documento informatico privato, i reati configurabili sono perseguibili a querela della persona offesa e per la punibilità, almeno nell'ipotesi di cui all'articolo 485 codice penale, occorre il dolo specifico, giacchè l'azione falsificatoria del colpevole deve essere determinata dalla finalità di procurare a sé od altri un vantaggio o recare ad altri un danno.

Nel caso di falso riguardante documenti informatici pubblici è invece sufficiente il dolo generico (4).

In sintonia con la costante giurisprudenza in tema di atti pubblici, dovrà ritenersi che non ogni documento proveniente dalla pubblica amministrazione sia pubblico dal momento che saranno tali solo quei documenti la cui redazione risulti espressione dell'esercizio della pubblica funzione o del pubblico servizio.

Ne consegue che ad esempio non si applicherà la normativa sui falsi in atto pubblico alle manipolazioni riguardanti le modalità di registrazione informatica dei pubblici dipendenti, registrazioni che attendono al rapporto privatistico di lavoro, senza coinvolgere l'esercizio di poteri pubblicistici (5).

Sempre in tema di falso l'articolo 3 della legge 48/2008 inserisce nel corpo del codice l'articolo 495bis che punisce con la reclusione fino ad un anno «*Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona».*

La norma è modellata sull'articolo 495 del codice penale che punisce la falsa attestazione o dichiarazione ad un pubblico ufficiale sulla identità o qualità personali proprie o di altri.

Essa si caratterizza per il fatto che la falsa dichiarazione deve essere resa ad un soggetto che presta servizi di certificazione di firma elettronica ed a titolo esemplificativo tenderà ad incriminare quelle false indicazioni concernenti le qualifiche soggettive del richiedente, la sussistenza ed i li-

---

(4) È da segnalare che l'articolo 7 della Convenzione invitava gli Stati membri a valutare la possibilità di sanzionare i delitti di falso solo se commessi «fraudolentemente o con altro analogo intento delittuoso».

(5) V. AMATO G., *Incerta. cit,* p. 16. V. in giurisprudenza Cass. Sez. un. 10-5-2006, n. 15983, rv. 233423.

miti del potere di rappresentanza e, soprattutto, i limiti d'uso del certificato elettronico necessario per l'ottenimento della firma elettronica qualificata o della firma digitale (6).

3. IL NUOVO ARTICOLO 615QUINQUIES C.P. (ARTICOLO 4)

ART. 4

Modifica al titolo XII del libro secondo del codice penale

1. L'articolo 615quinquies del codice penale è sostituito dal seguente:

«Art. 615quinquies. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

COMMENTO

L'articolo 4 della legge 48/2008 riformula il testo dell'art. 615 quinquies che, nella sua formulazione originaria, puniva «*chiunque diffonde, comuni-*

(6) L'art. 1 del Decreto legislativo 7-3-2005, n. 82 (Codice amministrazione digitale) definisce la «firma elettronica» come «l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica»; la «firma elettronica qualificata» come «la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma»; la «firma digitale» come «un particolare tipo di firma elettronica 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».

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

La norma mirava e mira tuttora, come si vedrà, a reprimere la diffusione dei *virus* informatici, quei programmi, cioè, che si attivano da soli ad un dato momento temporale od al verificarsi di una certa condizione e sono forieri di gravi danni ai sistemi informatici e telematici, utilizzati spesso per scopi di sabotaggio (7).

L'art. 615quinquies c.p. costituisce uno strumento di tutela giuridica diretto a «prevenire», prima ancora che reprimere, una serie di condotte oggettivamente valutate come particolarmente insidiose ed intrinsecamente nocive per la funzionalità di sistemi, dati o programmi.

Prima di esaminare nello specifico la nuova disposizione non pare inopportuno soffermarsi brevemente sul concetto di sistema informatico.

Ora, l'articolo 1 della Convenzione definiva «sistema informatico» qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati.

Il nostro legislatore, rifuggendo da qualsiasi tecnica definitoria, non ha recepito la previsione ed occorre quindi rifarsi inevitabilmente all'opera interpretativa della giurisprudenza ed in particolare della Suprema Corte che ha precisato come deve ritenersi «sistema informatico», secondo la ricorrente espressione utilizzata nella L. 547/93 «*un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate — per mezzo di un'attività di «codificazione» e «decodificazione» — dalla «registrazione» o «memorizzazione», per mezzo di impulsi elettronici, su supporti adeguati, di «dati», cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare «informazioni», costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente*» (8).

Non dissimile è la posizione di chi ha affermato che per sistema informatico deve intendersi un sistema costituito, di regola, da più elaboratori

(7) PICA, *Reati informatici e telematici, Digesto delle discipline penalistiche - Aggiornamento,* Torino, 2000, pag. 533.

(8) Così espressamente Cass. 14-12-1999, n. 3067. Tale definizione è stata ripetuta recentemente da Cass. 31-7-2007, n. 31135.

collegati tra loro per scambiare dati oppure da ogni macchina elettronica che presenti una connessione organica di elementi funzionale ad uno scopo e che utilizzi un microprocessore per l'elaborazione di dati binari (BIT), purchè sia dotata di propria autonomia, cioè in grado di svolgere il lavoro comandato senza ricorrere all'ausilio di altri sistemi (es., pc. collegato alla stampante per elaborazione testi). Si ritiene, inoltre, che più sistemi informatici possano occasionalmente collegarsi tra loro per ottenere informazioni o scambiare e prelevare dati.

Con l'espressione sistema telematico si intende invece un insieme combinato di apparecchiature idoneo alla trasmissione a distanza di dati ed informazioni, attraverso l'impiego di tecnologie dedicate alle comunicazioni (9).

Ciò posto, nel ritornare all'articolo 4, legge 48/2008, va osservato che l'originaria formulazione dell'articolo 615quinquies era apparsa sin dall'inizio poco felice dal momento che il legislatore aveva equiparato, a fini penali, la destinazione «intenzionale» di un programma al danneggiamento ovvero all'alterazione del funzionamento di sistemi, dati o programmi con la semplice possibilità che tali eventi si verifichino «per effetto» di un programma.

Se poi si aggiunge che veniva punita anche la consegna di un programma che aveva per effetto il danneggiamento di un sistema informatico, si aveva la conseguenza paradossale che si sarebbe dovuto ritenere punibile ad esempio anche chi avesse consegnato un dischetto contenente il programma che aveva cagionato il danno, al tecnico che deve riparare il computer rovinato dal *virus*.

Dinanzi a tali conseguenze si era sostenuto in dottrina, del tutto plausibilmente, che la *consegna* doveva ritenersi penalmente illecita solo se effettuata con l'intenzione di comunicare il *virus* al sistema di chi riceve il supporto contenente il programma nocivo e, dunque, con la piena coscienza di chi lo consegna e nell'inconsapevolezza del ricevente (10).

Del resto la stessa lettera della norma consentiva di limitare la rilevanza penale dell'attività di consegna che fosse effettuata allo scopo di danneggiare un sistema informatico.

Comunque, stante l'oggettiva incertezza del testo normativo, è apparsa quanto mai opportuna la riformulazione dell'615quinquies che, nel testo attuale, punisce solo le condotte poste in essere*, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione totale o parziale, o l'alterazione del suo funzionamento*.

(9) CALICE, op. cit., pag. 5.
(10) PICA, op. cit. pag. 534.

L'elemento soggettivo del reato è stato, dunque, circoscritto al dolo specifico, con la conseguenza che dovrebbero essere risolti i problemi interpretativi sopra esposti.

Nei primi commenti alla norma si è però rilevato che anche l'attuale formulazione si presta a qualche considerazione critica: infatti in precedenza si considerava pacifico che dovesse essere il software medesimo a dover possedere la caratteristica obiettiva di avere per scopo o per effetto il danneggiamento di un sistema informatico e telematico.

Con la nuova disposizione, si è osservato, l'attenzione si sposterebbe non più sul fatto oggettivo della potenzialità dannosa del programma (o del dispositivo), ma sul profilo soggettivo, ossia sullo scopo per cui un soggetto agente acquisisca, produca, si procuri o diffonda il programma stesso, con il rischio, non meramente ipotetico, di criminalizzare la detenzione di programmi che, pur pienamente leciti, abbiano comunque l'effetto di danneggiare un sistema informatico o i dati in esso contenuti, quali ad esempio i programmi di partizionamento dell'hard disk che, se usati in maniera non appropriata, possono portare ad estesi danneggiamenti dei dati, ovvero ad alterazioni del funzionamento di un sistema informatico (11).

La critica non convince: innanzitutto il testo, per come riformulato, incrimina la condotta del *procurarsi* che appare essere qualcosa di diverso dalla mera detenzione.

Ma quand'anche si volesse ritenere che la detenzione sia ricompresa nel procurarsi, è indubbio che tale condotta in tanto è punibile in quanto il soggetto agisca allo scopo di danneggiare illecitamente sistemi altrui, il che appare meritevole di sanzione penale.

Del resto la formulazione precedente era infelice proprio perché sembrava prescindere dall'intenzione dell'agente e la stessa Convenzione di Budapest, all'articolo 6, imponeva la punibilità dell'*approvvigionamento per l'uso.*

Anzi va osservato che la stessa Convenzione consentiva agli Stati membri di incriminare la condotta di possesso solo nel caso in un soggetto disponesse di un certo numero di apparecchiature, dispositivi e programmi informatici atti a danneggiare un sistema informatico o telematico.

In ogni caso la mancata previsione di una soglia numerica non esclude che il numero (specie se consistente) degli apparecchi o dispostivi possa essere preso in considerazione per la dimostrazione della finalità illecita del possessore e quindi rilevare come elemento di prova al fine della sussistenza del dolo specifico (12).

---

(11) V. CUNIBERTI-GALLUS-MICOZZI-ATERNO, *Commento, cit,* p. 8.

(12) G. AMATO, *Contrasto specifico all'uso di dispositivi, Guida al diritto,* 2008, p. 58.

Accanto alla sopra esaminata rivisitazione dell'elemento soggettivo del reato, la norma ha inciso anche sull'elemento materiale della condotta, estendendo il raggio delle condotte punibili.

Infatti, in ossequio a quanto previsto dall'articolo 6 della Convenzione di Budapest, la norma sanziona non soltanto le condotte afferenti i «programmi informatici», ma anche «le apparecchiature» e i «dispositivi», il cui funzionamento sia idoneo a danneggiare un sistema informatico, ovvero ad alterarne il funzionamento.

Inoltre mentre il previgente testo dell'art. 615quinquies mirava alla punizione di chiunque *diffonde, comunica o consegna,* il nuovo testo punisce anche le condotte di chi *procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici,* aventi lo scopo di danneggiamento.

Anche tale estensione è quanto mai opportuna dal momento che la precedente formulazione poteva lasciare impunite condotte di riproduzione, etc.. ugualmente pericolose, perché accrescono il mercato illecito attraverso l'immissione *ex novo* di dispositivi o programmi illeciti.

Si è poi introdotto l'avverbio *illecitamente*: l'aggiunta appare pleonastica dal momento che appare evidente che il danneggiamento in tanto è punibile in quanto illecito, commesso cioè al di fuori di qualsiasi norma che lo autorizza o lo impone.

Anche nel nuovo testo continua a non essere penalmente rilevante la semplice *creazione* dei programmi nocivi: tale scelta appare dettata oltre che da considerazioni pratiche di accertamento e di prova del fatto, che avrebbero vanificato l'efficacia di un tale divieto, anche dall'intento di non incidere negativamente su momenti creativi dell'attività umana, fin quando restano nella sfera privata di libertà dell'agente, senza assumere pericolosità sociale.

È rimasta inalterata la pena: reclusione sino a due anni e la multa sino ad euro 10.329.

4. I DANNEGGIAMENTI (ARTICOLI 5 E 6)

Art. 5

Modifiche al titolo XIII del libro secondo del codice penale

1. L'articolo 635bis del codice penale è sostituito dal seguente:

«Art. 635bis. Danneggiamento di informazioni, dati e programmi informatici. – Salvo che il fatto costituisca più grave reato, chiunque

distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».

2. Dopo l'articolo 635bis del codice penale sono inseriti i seguenti:

«Art. 635ter. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. – Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635quater. Danneggiamento di sistemi informatici o telematici. – Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635quinquies. Danneggiamento di sistemi informatici o telematici di pubblica utilità. – Se il fatto di cui all'articolo 635quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

3. Dopo l'articolo 640quater del codice penale è inserito il seguente:

«Art. 640quinquies. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica. – Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

ART. 6

Modifiche all'articolo 420 del codice penale

1. All'articolo 420 del codice penale, il secondo e il terzo comma sono abrogati.

COMMENTO

L'articolo 5 viene ad operare un complessivo riordino delle fattispecie di danneggiamento.

In particolare si sono accorpate e riunite sotto le figure degli articoli 635 bis a 635quinquies le varie figure di danneggiamento informatico, provvedendo ad abrogare contestualmente il secondo e terzo comma dell'articolo 420 c.p. che disciplinavano ipotesi di attentato a sistemi di pubblica utilità ora sanzionati dagli articoli 635ter e quinquies.

La riclassificazione delle varie figure di danneggiamento informatico si giustifica con la necessità di sanzionare in maniera differenziata condotte dalla potenzialità lesiva piuttosto diversa (si pensi alla differenza tra la condotta di chi danneggia un singolo documento informatico appartenente a soggetto privato e chi, invece, distrugge sistemi informatici rilevanti per la collettività), oltre che con esigenze di simmetria rispetto alle previsioni della Convenzione di Budapest, la quale, agli artt. 4 e 5 distingue nettamente fra condotte di «attentato all'integrità dei dati» e condotte di «attentato all'integrità di un sistema».

Con la norma in commento, inoltre, il legislatore ha realizzato una nuova disciplina delle aggravanti seguendo la duplice direttrice: eliminazione del generico rinvio alle aggravanti di cui all'articolo 635

c.p. che ricomprendeva anche aggravanti del tipo *sopra piante di viti, di alberi,* ontologicamente inconfigurabili con un reato informatico e previsione di due aggravanti per tutti i reati (danneggiamento con violenza alla persona o minaccia; commissione del fatto con abuso della qualità di operatore del sistema).

Ma esaminiamo più da vicino le singole disposizioni.

a) *L'articolo 635bis: il danneggiamento di dati, informazioni e programmi non di pubblica utilità*

L'articolo 5, 1° comma, legge in commento modifica il precedente testo dell'art. 635bis codice penale, introdotto dall'articolo 9 della legge 547/1993 che puniva «*chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui*».

La norma era ricalcata sostanzialmente sulla figura di cui all'articolo 635 codice penale in tema di beni materiali e appariva poco adattabile alle fenomenologie proprie del mondo virtuale dell'informatica (13).

Infatti il nuovo testo dell'articolo 635bis codice penale punisce, a querela della persona offesa, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

La novità più significativa consiste nel fatto che la previsione normativa è stata limitata al danneggiamento di *dati e programmi informatici,* con l'esclusione dei *sistemi informatici o telematici* che sono ora oggetto di una autonoma tutela agli articoli 635quater e quinquies.

Il legislatore ha poi precisato meglio le modalità della condotta di danneggiamento, includendovi anche la cancellazione, alterazione o soppressione di informazioni, dati e programmi, attività che, in via interpretativa, comunque potevano ritenersi penalmente sanzionate dall'articolo 635bis testo previgente, rientrando nella condotta del «rendere inservibili in tutto o in parte».

Particolarmente significativa è poi l'introduzione della perseguibilità a querela del delitto di cui all'art. 635bis c.p. non aggravato.

Mentre infatti, sotto la precedente formulazione, ogni danneggiamento di dati informatici era perseguibile d'ufficio nella convinzione, espressa nella

(13) In giurisprudenza (Cass. Sez. un. 13-2-1997, n. 1282) si era tuttavia sostenuto, che anche prima della legge 547/1993, 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'articolo 635 del codice penale, in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore.