COMMENTO ALLA LEGGE DI RATIFICA
DELLA CONVENZIONE DI BUDAPEST
del 23 NOVEMBRE 2001

avv. Marco Cuniberti
avv. Giovanni Battista Gallus
avv. Francesco Paolo Micozzi
avv. Stefano Aterno

Indice

1 PREMESSA

E' stata ratificata, con legge approvata dal Senato in data 27.02.2008, la Convenzione di Budapest 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica, il primo accordo internazionale riguardante i crimini commessi attraverso internet o 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 combattere il crimine informatico in maniera coordinata.

Detta legge, che curiosamente non è ancora stata pubblicata sulla Gazzetta Ufficiale, introduce importanti modifiche al Codice penale, al Codice di procedura penale, al D. Lgs. 231/2001 (sulla responsabilità amministrativa delle persone giuridiche) e al cd. Codice Privacy.

Dopo un'appassionata ed elaborata analisi della normativa davanti alle Commissioni riunite di Giustizia e Senato, si è approdati in aula alla fine di febbraio con una serie di emendamenti al testo del disegno di legge del Governo.
Va dato merito al Relatore del testo legislativo e agli altri componenti della Commissione Giustizia che hanno avuto l'accortezza, e se vogliamo l'umiltà, di rivolgersi ad un "gruppo di giovani studiosi" (vedansi le parole pronunciate nella Relazione di presentazione) per risolvere i problemi applicativi e interpretativi di alcune norme dello schema di disegno di legge (schema disegno di legge dell'11 maggio 2007) che presupponevano infatti una conoscenza approfondita dei metodi investigativi sulle cd *digital evidence*.

In attesa della pubblicazione, ecco un primo analitico commento delle nuove norme: trattasi di 14 articoli, divisi in quattro capi.

2 Capo I: RATIFICA ED ESECUZIONE

2.1 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».

2.2 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.

Gli articoli 1 e 2 della legge dichiarano l'intenzione di dare piena ed intera esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica: ma, come verrà evidenziato, la convenzione non viene recepita integralmente.
La legge non ne ratifica, ad esempio, l'art. 1 relativo alle definizioni tecniche. Analizzando sia il dossier del Servizio Studi della Camera dei Deputati, sia la relazione al DDL, sembra evidente che tale omissione sia consapevole e voluta, , in quando vi si trovano i riferimenti alle normative speciali contenenti tali definizioni,

nonché alle elaborazioni terminologiche dottrinali e giurisprudenziali. La più importante questione si pone per la definizione di sistema informatico e/o telematico, abbondantemente utilizzata dal nostro codice penale per i cosiddetti "reati informatici". La Convezione parla espressamente solo di sistema informatico (non di sistema telematico), così definendo "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". Si rileva quindi che:

- è definito SISTEMA anche una singola apparecchiatura, il che potrebbe aiutare l'interpretazione del concetto;
- ben si ricomprende anche il concetto di sistema telematico, visto che si intende come sistema informatico anche un "*gruppo di apparecchiature* (COMUNQUE) *interconnesse o collegate*".

Al contrario, con la legge si è preferito continuare a non fornire una definizione positiva (e, ciò che maggiormente si nota, non vi sono considerazioni in merito alla questione né nella relazione introduttiva, né nel citato dossier).
Pare comunque sicuramente una scelta (non certo una dimenticanza), dovuta probabilmente al non rischiare di incorrere nel rigido limite rappresentato dal principio di tassatività, per cui sarebbe più opportuno lasciare la definizione alla giurisprudenza (che magari potrà far propria la definizione di cui alla stessa convenzione, specie per la suesposta osservazione sul concetto di "sistema"), che la adegui al concetto di sistema informatico e valga anche nel caso in cui questo tecnicamente cambi e possa non corrispondere più alla definizione (risalente oltretutto al 2001). D'altro canto resta l'annoso problema (che si pone sin dalla novella codicistica del '93) della minore certezza del diritto, lasciando totalmente al magistrato la responsabilità (e la libertà) di decidere se, nel caso concreto, si sia o meno in presenza di un sistema informatico o telematico.
Non è stato recepito neppure l'art. 10, comma II, della convenzione, che, come sottolineato anche dalla relazione al DDL, prevede l'infrazione legata agli attentati alla proprietà intellettuale e ai delitti commessi deliberatamente a livello commerciale mediante sistemi informatici (articolo 10).
La violazione del diritto d'autore va sanzionata penalmente se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico. Lo Stato può anche riservarsi di non imporre sanzioni penali se altri rimedi efficaci siano disponibili e se non si violano gli impegni internazionali.
Sarebbe quindi potuta cogliersi l'occasione di rivedere una tra le più controverse norme del nostro ordinamento, cioè l'art. 171, comma 1, lett a-bis della LDA: "*Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa […] chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma […]a-bis) 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*".
Si tratta di una norma, introdotta in sede di conversione del DL 31/1/2005, n. 7, che ha criminalizzato (ancorché sanzionandolo con una multa) le condotte rientranti nella distribuzione di opere protette attraverso reti "peer to peer". La norma sanziona anche condotte che non avvengono a livello commerciale, o, per utilizzare la terminologia del Legislatore italiano, per scopo commerciale, e dunque criminalizza anche delle condotte ulteriori, rispetto a quanto previsto dalla Convenzione.
Il Legislatore avrebbe quindi potuto modificare il trattamento sanzionatorio di

quelle condotte che, pur provocando detrimento patrimoniale agli intermediari dei diritti d'autore, non siano compiute a scopo commerciale o imprenditoriale, ovvero a fini di lucro, nonché per modificare l'art. 171 bis L.d.A. che, a seguito della modifica operata dalla l. 248/2000, sanziona ora anche le condotte di importazione, distribuzione vendita etc. di programmi per elaboratore e banche dati, qualora la condotta sia posta in essere "per trarne profitto", mentre l'originaria dizione (come peraltro l'art. 171 ***ter***, nella sua attuale formulazione) prevedeva il fine di lucro.
Poiché la Corte di Cassazione ha avuto varie volte occasione di chiarire come il profitto possa essere costituito da un vantaggio anche non direttamente patrimoniale, il ripristino dell'originaria dizione, oltre che conforme al dettato della Convenzione, avrebbe consentito di restringere l'area dell'illecito penale alle condotte più marcatamente lesive dell'interesse protetto, e sanerebbe la distonia attualmente sussistente tra le fattispecie di cui all'art. 171 *bis* (ove è richiesto il fine di profitto), con quelle di cui all'art. 171 *ter* (ove al contrario è richiesto il fine di lucro).

3 Capo II: MODIFICHE AL CODICE PENALE E AL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

3.1 Art. 3. (Modifiche al titolo VII del libro secondo del codice penale)

1. All'articolo 491-bis 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 aggiunto il seguente:

"Articolo 495–bis (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."

Il primo comma modifica l'art. 491 *bis*, eliminando il secondo periodo del primo e unico comma (che recita "A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli"). Da un lato, la modifica si rivela assolutamente opportuna, in quanto "sgancia" il documento informatico dall'ormai anacronistica necessità di un eventuale supporto e rinvia chiaramente (ma solo nella prefazione al DDL) alla definizione di "documento informatico" di cui al C.A.D. (d.lgs. 82/2005: il riferimento è erroneamente alla definizione del DPR 513/97, che, malgrado sia stato già superato da numerose altre leggi – in ultimo appunto dal C.A.D. – fornisce comunque la medesime definizione

di documento informatico).
Lo scopo è apprezzabile: si cerca di ricondurre ad un'unicità di concetto per il documento informatico e, come già osservato, si elimina il legame tra l'esistenza del documento informatico e la necessaria sussistenza di un supporto: come infatti rilevato nel dossier del Servizio Studi della Camera dei Deputati, "*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. In realtà, come rilevato in dottrina, il rilievo ha carattere più generale: nel tentativo, infatti, di disciplinare secondo regole e schemi tradizionali un fenomeno ad essi irriducibile, se non, appunto, attraverso costose forzature, il legislatore non ha considerato alcune fondamentali peculiarità del sistema tecnologico; con riguardo al documento informatico tale atteggiamento ha finito col trascurare la capacità dei mezzi tecnologici informatici di garantire «la perfetta autonomia strutturale e funzionale del dato rispetto al supporto che lo ospita»*".
Occorre però fare attenzione a un altro aspetto: la "vecchia" seconda parte dell'unico comma dell'art. 491 *bis* c.p. disponeva infatti anche che il documento informatico, per ottenere la medesima tutela penale di quello cartaceo, dovesse comunque avere una qualche efficacia probatoria: cancellando tale seconda parte, anche quest'ultimo requisito sarebbe stato eliminato.
Rispetto al DDL, che prevedeva appunto l'eliminazione di tale "vecchia" seconda parte, in sede di Commissione è stato recuperato il requisito della necessaria efficacia probatoria del documento informatico oggetto del reato, inserito ora nella prima parte dell'articolo.
Per il C.A.D. (art. 1, lett. P), il documento informatico è infatti semplicemente "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:
- se non è sottoscritto con una firma elettronica (art. 1, lett. Q), non può avere alcuna efficacia probatoria, ma può al limite, a discrezione del Giudice, soddisfare il requisito legale della forma scritta (art. 20, c. 1 bis);
- anche quando sia firmato con una firma elettronica "semplice" (cioè non qualificata) può non avere efficacia probatoria (il giudice dovrà infatti tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento informatico).

E' quindi chiaro che, poiché ben può darsi che un documento informatico possa non avere alcuna efficacia probatoria (anzi, in certi casi può non soddisfare neppure il requisito legale della forma scritta), la sua offensività può essere molto minore rispetto ai documenti "tradizionali (e di cui alle norme del capo III, libro secondo, titolo VIII, c.p.), se non addirittura nulla.
In tali casi, prevedere la medesima tutela penale sarebbe stato quindi sproporzionato, se non addirittura ingiustificato (con possibili profili di incostituzionalità).

Il secondo comma introduce invece il "nuovo" Art. 495–*bis* c.p..
Rispetto al DDL, che parlava genericamente di "certificatore", la versione definitiva della legge fa maggior riferimento alla definizione del C.A.D., facendo ora riferimento, nella rubrica, al "certificatore di firme elettroniche" e nell'articolo al "soggetto che presta servizi di certificazione delle firme elettroniche".
Il nostro ordinamento (ed in particolare il C.A.D.) conosce però più tipi di certificatore, tra cui il certificatore qualificato e quello accreditato.

Ma poiché la firma elettronica è anche, sempre a mente del C.A.D. "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica" (cd. "firma elettronica semplice") e poiché ai sensi dell'art. 21 dello stesso C.A.D. il documento informatico sottoscritto con firma elettronica è sul piano probatorio liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (per cui ben può non essergli riconosciuta alcuna efficacia probatoria), mentre il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, ha necessariamente l'efficacia prevista dall'articolo 2702 del codice civile (ha valenza di scrittura privata), è evidente la diversa portata offensiva tra le dichiarazioni effettuate a un certificatore non qualificato, e quelle rese ai certificatori abilitati a rilasciare una firma digitale qualificata.

3.2 Art. 4. (Modifica al titolo XII del libro secondo del codice penale)

1. L'articolo 615-quinquies del codice penale e` sostituito dal seguente:

«Art. 615-quinquies. – (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, e` punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

Il testo definitivamente approvato opera una significativa riforma del "vecchio" art. 615 *quinquies* del codice penale, che puniva (con identica sanzione) "Chiunque diffonde, comunica 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".
Vengono introdotte svariate novità: in primo luogo, in ossequio a quanto previsto dall'art. 6 della Convenzione di Budapest, la norma sanziona non soltanto le condotte afferenti i "programmi informatici", ma anche le "apparecchiature" e i "dispositivi".
La norma quindi include non solo il software, ma anche l'hardware, comprendendo tutte quelle apparecchiature e dispositivi il cui funzionamento sia idoneo a danneggiare un sistema informatico, ovvero ad alterarne il funzionamento.
Integrerà quindi il "nuovo" delitto di cui all'art. 615 quinquies non solo il procurarsi virus e malware in genere, ma anche la produzione, importazione, etc. di dongle, smart card, skimmer e così via, laddove, naturalmente, si prestino ad un utilizzo illecito, al fine appunto di danneggiare o alterare un sistema informatico, ovvero i dati e programmi ivi contenuti.

In secondo luogo, la norma amplia nettamente le condotte sanzionabili: mentre con la precedente dizione era pacifico che la mera detenzione non fosse punibile, richiedendosi che il programma venisse quantomeno "diffuso comunicato o consegnato", la norma così riformulata sanziona non solo chi diffonda, comunichi, consegni o, comunque, metta a disposizione programmi, apparecchiature o dispositivi, ma anche chi produca, importi, si procuri ovvero riproduca tali software o hardware.
Diventano pertanto sanzionabili, in astratto, anche delle condotte di mera detenzione di malware, coerentemente con l'impianto della Convenzione, che impone la punibilità, all'art. 6, anche dell'"approvvigionamento per l'uso".
All'estensione della portata della norma sotto il profilo oggettivo ha fatto riscontro la riformulazione dell'elemento soggettivo richiesto, nei termini del dolo specifico.
Se infatti la precedente formulazione richiedeva pacificamente il solo dolo generico, ovverosia la consapevolezza che il malware fosse in grado di danneggiare o alterare il funzionamento di un sistema informatico o telematico, e la consapevolezza della diffusione, comunicazione o consegna, con la riforma l'elemento soggettivo viene ad essere circoscritto al solo dolo specifico, in quanto il fatto è punibile soltanto laddove sia commesso "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".
Il DDL, nella sua redazione originaria, conteneva una dizione diversa, e ben più ampia, prevedendo che il fatto dovesse essere commesso "al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno", anche se soggiungeva che software e dispositivi dovessero comunque avere per scopo o per effetto il danneggiamento, l'alterazione etc. del sistema, dei dati e dei programmi.
In effetti, è sicuramente opportuno che il Legislatore abbia ristretto significativamente l'ambito delle condotte punibili. In sede di approvazione definitiva, era stato infatti rilevato dalla VII Commissione (Cultura) che, con l'originaria formulazione, tra l'altro "si andrebbero così a rendere illegale e finanche penalmente rilevante alcune attività di verifica della sicurezza informatica, attraverso strumenti commerciali e, in potenza, anche gratuiti, questi ultimi spesso sviluppati da programmatori esperti che intendono mettere a disposizione del pubblico programmi informatici atti a tentare danneggiamento o intrusione nel sistema allo scopo di testarne l'effettiva vulnerabilità; con particolare preoccupazione va valutata questa previsione in riferimento allo studio e la ricerca nell'ambito della sicurezza informatica, materia di sempre maggiore rilevanza nei corsi universitari e di specializzazione, e che in modo crescente interessa l'ambito di ricerca tecnologica e teorica della scienza informatica".
Se infatti fossero stati sanzionabili i fatti commessi semplicemente a fine di profitto o di danno, si sarebbe corso il serio rischio di ritenere punibile, in astratto, la mera creazione di malware a scopo di ricerca, o di attività commerciale (si pensi alle software house che si occupano di sicurezza informatica).
Anche l'attuale formulazione della norma si presta a qualche considerazione critica: mentre prima era infatti pacifico che fosse il software medesimo a dover possedere la caratteristica obbiettiva di avere per scopo o per effetto il danneggiamento di un sistema informatico o telematico, e dunque occorresse l'accertamento positivo che il programma avesse tali effetti, ora l'analisi si potrebbe spostare non più sul fatto oggettivo della potenzialità dannosa del programma (o del dispositivo), ma sul profilo soggettivo, vale a dire sullo scopo per cui il

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.
Basti pensare, infatti, agli effetti potenzialmente devastanti che possono avere dei banali tool di partizionamento dell'hard disk, ovvero dei software di accesso remoto e simili, che, certamente, se usati in maniera non appropriata, possono portare ad estesi danneggiamenti dei dati, ovvero ad alterazioni del funzionamento di un sistema informatico.
Occorrerà quindi verificare accuratamente l'applicazione pratica della norma, che, nella formulazione attualmente vigente, è stata oggetto di contestazione giudiziale in pochissime occasioni.

3.3 Articolo 5 (Modifiche al Titolo XIII del libro secondo del codice penale)

1. L'articolo 635 - bis del codice penale è sostituito dal seguente: "Articolo 635 – bis (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 e` 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 e` commesso con abuso della qualita` di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio»."

2. Dopo l'articolo 635 - bis del codice penale sono aggiunti i seguenti articoli:

"Articolo 635 – ter (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 e` commesso con abuso della qualita` di operatore del sistema, la pena è aumentata."

Articolo 635 – quater (Danneggiamento di sistemi informatici e telematici) - Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635- bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, 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 e` commesso con abuso della qualità di

operatore del sistema, la pena è aumentata."

Art. 635-quinquies. – (Danneggiamento di sistemi informatici o telematici di pubblica utilità) – Se il fatto di cui all'articolo 635-quater 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 e` 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 e` reso, in tutto o in parte, inservibile, la pena e` 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 e` commesso con abuso della qualità di operatore del sistema, la pena e` aumentata."

3. Dopo l'articolo 640-quater del codice penale e` inserito il seguente:

«Art. 640-quinquies. – (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 se´ 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, e` punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

3.4 Art. 6. (Modifiche all'articolo 420 del codice penale)

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

Il Legislatore ha, in sede di ratifica della Convenzione, operato un complessivo riordino delle fattispecie di danneggiamento informatico.
In generale, si è scelto, seguendo l'impianto degli artt. 4 e 5 delle Convenzione di Budapest, di distinguere nettamente tra il danneggiamento dei dati programmi e informazioni da un lato, ed il danneggiamento dei sistemi informatici dall'altro.
In secondo luogo, si è optato (con una serie di emendamenti presentati in sede di approvazione definitiva, il 20/2/08) per l'accorpamento di tutte le fattispecie di danneggiamento, includendovi anche quelle di attentato a sistemi di pubblica utilità, prima contenute nell'art. 420 del Codice penale (i cui commi II e III sono stati, infatti, abrogati).
Si è, infine, proceduto a rimodulare le aggravanti.
In particolare, tutte le fattispecie sono aggravate se "ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema".
La vecchia norma, infatti, prevedeva il danneggiamento fosse aggravato laddove ricorresse "una o più delle circostanze di cui al secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema": aldilà delle aggravanti palesemente inapplicabili e certamente poco pertinenti (basti pensare ad un danneggiamento informatico "sopra opere destinate all'irrigazione", ovvero sopra piante di viti, di alberi, o ancora su vivai...- art. 635, comma II, nn. 4 e 5) è significativa l'eliminazione del richiamo all'art. 625, n. 7 c.p., che rendeva il danneggiamento informatico aggravato laddove fosse commesso "su cose esistenti in uffici o stabilimenti pubblici, o sottoposte a sequestro o a pignoramento, o

esposte per necessità o per consuetudine o per destinazione alla pubblica fede, o destinate a pubblico servizio o a pubblica utilità".
Aldilà delle fattispecie introdotte *ex novo* ai successivi articoli, tutte le ipotesi di danneggiamento saranno pertanto da considerarsi aggravate laddove ricorra una delle seguenti ipotesi: 1) quando il danneggiamento sia commesso con violenza alla persona o minaccia (art. 635, comma II, n. 1); 2) quando il fatto sia commesso con abuso della qualità di operatore del sistema.
Si sarebbe peraltro potuto cogliere l'occasione per definire meglio l' "operatore di sistema" (figura introdotta dalla L. 547/93), al fine di delineare più precisamente il suo ambito di applicazione, per circoscrivere l'operatività della circostanza aggravante soltanto a quei soggetti le cui condotte, in forza della proprie competenze tecniche, e della loro posizione quali amministratori di rete o di sistema, abbiano un potenziale offensivo maggiore.

3.4.1 Il danneggiamento di dati, informazioni e programmi non di pubblica utilità

Il "vecchio" art. 635 *bis* del Codice Penale, rubricato "danneggiamento di sistemi informatici o telematici" così disponeva: " Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".
Le modifiche apportate, come anticipato, sono abbastanza incisive.
In primo luogo, viene introdotta la punibilità a querela della persona offesa del danneggiamento di dati programmi e informazioni, non aggravato (art. 635 *bis,* comma 1), mentre prima si procedeva d'ufficio, in quanto, come si sottolineava nella relazione alla L. 23/12/93, n. 547, "il regolare funzionamento dei sistemi informatici e telematici, anche privati, è di interesse non strettamente singolare, ma della collettività intera": a distanza di quasi quindici anni dall'emanazione della L. 547/93, il Legislatore ha evidentemente ritenuto non più necessaria la procedibilità d'ufficio per il mero danneggiamento di dati, informazioni e programmi "privati".
In altre parole, il Legislatore ha introdotto una condizione di procedibilità (la proposizione della querela), in armonia al danneggiamento "comune", di cui all'art. 635 del Codice Penale, che è procedibile d'ufficio soltanto in determinate ipotesi aggravate.
Occorrerà pertanto una maggior cautela da parte della persona offesa, che dovrà procedere a sporgere rituale querela, entro il termine di legge (tre mesi), decorrente dalla notizia del fatto, pena l'improcedibilità dell'azione penale.
In secondo luogo, il Legislatore precisa meglio le modalità della condotta di danneggiamento, includendovi anche la cancellazione, alterazione o soppressione di informazioni dati e programmi (attività che avrebbero comunque potuto essere ricomprese, in via interpretativa, tra le condotte penalmente sanzionate).

3.4.2 Il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Anche il danneggiamento di dati, informazioni e programmi "pubblici" è stato profondamente rimaneggiato.
Occorre in primo luogo precisare come tali condotte fossero sanzionate dall'art. 420, comma II del Codice penale (ora abrogato), ove il delitto era delineato quale reato a consumazione anticipata, in termini di attentato a impianti di pubblica utilità (ed alle informazioni ivi contenute).
Il Legislatore, all'esito dei lavori parlamentari, e a seguito di una proposta emendativa presentata in sede di approvazione definitiva, ha ritenuto di mantenere sostanzialmente invariata detta qualità.
Il disegno di legge originario, al contrario, prevedeva che anche il danneggiamento di dati informazioni e programmi pubblici o di pubblica utilità fosse un reato di evento, e dunque richiedeva (salva naturalmente la punibilità del tentativo) che vi fosse una effettiva alterazione delle informazioni.
Si è ritenuto, invece, di modificare l'originaria dizione, mantenendo la natura di reato a consumazione anticipata, nonostante la Convenzione non lo richiedesse es*pressamente.*
*Il testo inglese parla infatti di "Data interference" e di "*System interference", mentre il testo francese fa riferimento, in effetti, a "*Atteinte à l'intégrité des données*" e "*Atteinte à l'intégrité du système*": in ogni caso, in entrambe le traduzioni, è pacifico che le fattispecie descritte dalla Convenzione richiedano l'effettivo danneggiamento del sistema o dei dati.
L'attuale norma prevede invece un reato aggravato dall'evento, che punisce i fatti diretti a distruggere, deteriorare etc. informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
Anche in questo caso, si assiste ad un ampliamento evidente delle condotte punibili, in primo luogo sotto il profilo dell'oggetto materiale.
La precedente dizione normativa, difatti, sanzionava soltanto i danneggiamenti riguardanti i dati contenuti o pertinenti a "sistemi informatici o telematici di pubblica utilità", mentre ora è sufficiente che i dati siano "utilizzati dallo Stato o da altro ente pubblico".
Sono ricomprese pertanto le condotte 1) riguardanti dati, informazioni e programmi utilizzati dagli enti pubblici; 2) riguardanti dati informazioni e programmi di pubblica utilità (e dunque sia pubblici che privati, purché siano destinati a soddisfare un interesse di natura pubblica).
Trattandosi di reato aggravato dall'evento, il fatto sussiste anche in assenza di qualunque effettivo deterioramento o soppressione dei dati, pur dovendosi necessariamente richiedere l'idoneità dell'azione a produrre tale effetto.
L'effettiva distruzione, deterioramento, cancellazione o alterazione è invece contemplata come circostanza aggravante (art. 635 *ter*, comma II).

3.4.3 Il danneggiamento di sistemi informatici e telematici non di pubblica utilità

Il danneggiamento di sistemi informatici o telematici non di pubblica utilità ha mantenuto (per fortuna) la sua caratteristica di reato di evento, e pertanto si

richiede espressamente che il sistema venga danneggiato, reso in tutto o in parte inservibile, ovvero ne venga ostacolato gravemente il funzionamento.
In sede di riforma, peraltro, si è meglio precisata la condotta.
Sarà integrata la fattispecie di cui all'art. 635 *quater*, laddove il danneggiamento del sistema sia cagionato 1) mediante la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi; ovvero 2) mediante l'introduzione o la trasmissione di dati, informazioni o programmi.
Le condotte punibili sono inoltre ampliate rispetto all'originaria dizione (il reato era sempre previsto dall'art. 635 *bis* c.p.), in quanto è sufficiente la prova che la condotta abbia alterato (ancorché gravemente) il funzionamento del sistema, mentre fino a oggi era necessaria la dimostrazione della distruzione, del deterioramento, ovvero del fatto che il sistema fosse reso, in tutto o in parte, inservibile.
D'altronde, tale ampliamento era necessitato dal dettato della Convenzione, che imponeva la punibilità di qualsiasi condotta che provocasse "*the serious hindering without right of the functioning of a computer*".
La distinzione tra il danneggiamento di dati e il danneggiamento del sistema è pertanto legata alle conseguenze che la condotta assume: laddove la soppressione o l'alterazione di dati informazioni e programmi renda inservibile, o quantomeno ostacoli gravemente il funzionamento del sistema, ricorrerà la più grave fattispecie del danneggiamento di sistemi informatici o telematici, prevista appunto dall'art. 635 quater.
Si porranno pertanto, in sede di giudizio, dei complessi problemi circa la prova del danno, e soprattutto delle sue conseguenze sul funzionamento del sistema.
E' stato previsto, peraltro, un sensibilissimo inasprimento delle sanzioni, poiché la pena massima, per l'ipotesi non aggravata, è stata portata da tre a cinque anni: quest'aumento ha portato il danneggiamento di sistemi informatici ad essere punito con una sanzione più severa rispetto anche alla frode informatica non aggravata.
Le aggravanti sono le stesse previste per il danneggiamento di dati.

3.4.4 Il danneggiamento di sistemi informatici o telematici di pubblica utilità

L'art. 635 *quinquies* corrisponde al "vecchio" reato di attentato a sistema informatico o telematico di pubblica utilità, anche per quanto riguarda la pena.
Si è scelto, anche per tale reato di ampliare la sfera delle condotte punibili, prevedendo che il fatto possa essere diretto non solo a danneggiare o a distruggere il sistema, ma anche a renderlo inservibile, ovvero a ostacolarne gravemente il funzionamento.
Si tratta (come già visto per il danneggiamento di dati di cui all'art. 635 *ter*) di un reato a consumazione anticipata, che non richiede l'avverarsi dell'evento di danneggiamento.
L'effettivo danneggiamento del sistema, la sua distruzione, o il fatto che venga reso in tutto o in parte inservibile, è considerato un'ulteriore circostanza aggravante, che aumenta significativamente la sanzione (reclusione da tre a otto anni): non è, peraltro, indicato tra le circostanze aggravanti il fatto che il funzionamento del sistema venga gravemente ostacolato.Non è parimenti più ricompresa nella fattispecie aggravata la circostanza che dal fatto derivi l'interruzione (anche parziale) del funzionamento, prevista dall'art. 420, comma III (ora abrogato).

Vi è poi da notare come la scelta appunto di abrogare tout court il terzo comma dell'art. 420, possa portare a delle soluzioni paradossali: mentre infatti l'attentato a sistemi informatici di pubblica utilità è rimasto un reato aggravato dall'evento, l'attentato a sistemi (non informatici) di pubblica utilità non ha più tale natura, proprio per l'intervenuta eliminazione della circostanza aggravante.
Occorre poi rilevare che, mentre per quanto riguarda l'art. 635 *ter*, il danneggiamento può riguardare dati o programmi informatici utilizzati dagli enti pubblici o ad essi pertinenti, o comunque di pubblica utilità, il delitto di cui all'art. 635 *quinquies* sussiste soltanto laddove la condotta di danneggiamento di sistema informatico sia diretta a danneggiare, distruggere etc. dei sistemi informatici o telematici di pubblica utilità.
Non è sufficiente quindi, per la sussistenza del reato, che i sistemi siano utilizzati dagli enti pubblici, ma occorre che gli stessi siano di pubblica utilità.

3.4.5 La truffa del certificatore di firma elettronica qualificata

L'aggiunta dell'articolo 640–quinquies sembra essere opportuna, stante la potenziale maggiore offensività della condotta compiuta dal certificatore, ed il ruolo svolto. La condotta sembrerebbe rientrare, comunque, nella fattispecie di cui all'art. 640 c.p., con cui si porrebbe quindi in rapporto di specialità.
Nell'originario DDL la sanzione era incomprensibilmente prevista in via alternativa (reclusione o multa), diversamente dalla truffa "ordinaria": tale situazione è poi stata "corretta" in sede di approvazione con la previsione "cumulativa" delle pene.
Queste paiono comunque troppo basse per essere dissuasive, tenendo anche presente che, proprio perché è norma speciale rispetto all'art.640 e relativa ad una condotta evidentemente più grave di una normale truffa, detta sanzione si troverebbe comunque ad essere ben più bassa (nel minimo edittale) di quella base prevista dallo stesso art. 640.
Stante la violazione degli obblighi incombenti sul certificatore, sarebbe stata opportuna anche l'introduzione di una sanzione accessoria, quale la sospensione dell'attività di certificazione, ovvero la pubblicazione della sentenza di condanna (la sanzione interdittiva sarebbe comunque applicabile laddove ricorresse un'ipotesi di responsabilità amministrativa delle persone giuridiche, ai sensi del D.lgs 231/2001).
Si osserva infine che, a differenza del "nuovo" art. 495 bis c.p., in questo caso, la condotta punita riguarda solo il certificatore "qualificato" (o meglio, il soggetto che presta servizi di certificazione di firma elettronica qualificata).

3.5 Art. 7. (Introduzione dell'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231)

1. Dopo l'articolo 24 del decreto legislativo 8 giugno 2001, n. 231, inserito il seguente: «Art. 24-bis. – (Delitti informatici e trattamento illecito di dati). – 1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».

Sulla scorta degli articoli 12 e 13 (secondo comma) della Convenzione di Budapest l'Italia ha introdotto misure legislative volte a consentire la "responsabilizzazione" delle "*personnes morales*" (fr.) per la commissione dei crimini previsti ed introdotti dalla Convenzione. Con l'art. 7 del testo definitivamente approvato dal Parlamento si è pensato, così, di novellare il **d.lgs. 231/2001**, disciplinante le ipotesi di illeciti amministrativi degli enti per i reati posti in essere da soggetti che si trovino in posizione apicale o dipendente nell'interesse o a vantaggio dell'ente stesso.
Prima della ratifica della Convenzione di Budapest, il d.lgs. 231/01 conosceva, quale reato c.d. informatico presupposto per la responsabilità dell'ente, unicamente la fattispecie descritta dall'art. 640 *ter* del codice penale (frode informatica).
In sede di audizione informale alla Camera dei Deputati, era stata avanzata la proposta di modificare il testo della rubrica dell'articolo 24-*bis* (già 25-*septies*) eliminando anche il riferimento all'inciso "trattamento illecito dei dati". Un testo siffatto, infatti, porta l'attenzione del primo lettore verso la normativa nazionale in tema di privacy ed, in particolare, verso l'art. 167 del Codice della privacy (d.lgs. 196/2003) che prevede, appunto, la fattispecie penale dell'illecito trattamento dei dati personali. Il corpo dell'articolo in questione, però, non fa alcun riferimento alla disciplina relativa al trattamento illecito dei dati personali. Sarebbe stato, pertanto, utile ai fini di una maggiore lucidità e coerenza sistematica elidere quest'inciso (anche se, ad ogni modo, "*rubrica legis non est lex*").
Il Legislatore, tuttavia, ha modificato la rubrica originariamente prevista nel disegno di legge rimuovendo il riferimento all'"attentato ad impianti di pubblica utilità" (previsto dal II e III comma dell'art. 420 c.p., ora abrogato), ed ha preferito mantenere intonso il riferimento al "trattamento illecito dei dati".
Ciò che desta maggiore interesse è, comunque, il contraccolpo che tale disciplina sortirà nei confronti degli enti soggetti al d.lgs. 231/2001 (soprattutto in considerazione della ridotta *vacatio legis*). Tale normativa si sostanzia e culmina nella richiesta di un maggiore sforzo organizzativo nei confronti degli enti, e nell'esposizione degli stessi ad una responsabilità talmente incisiva da poter determinare la cessazione dell'attività dell'ente (anche nelle ipotesi di commissione dei reati informatici).

Occorre notare, innanzitutto, che dall'adozione della disciplina di cui al d.lgs. 231/2001 per l'adeguamento della normativa nazionale al contenuto degli artt. 12 e 13 della Convenzione di Budapest può derivare una conseguenza non-voluta (dalla Convenzione): ossia l'introduzione di una zona d'ombra con riferimento ai soggetti richiamati dall'art. 1, terzo comma, del d.lgs. 231/01.
In base a tale ultima norma, infatti, la disciplina della 231 non si applica allo Stato, né agli enti pubblici territoriali, né agli altri enti pubblici non economici né, infine, agli "enti che svolgono funzioni di rilievo costituzionale". E' comunemente riconosciuto che in tale zona d'ombra possano agevolmente rientrare anche i partiti politici, le imprese individuali (Cass., Sez VI pen., sent. n. 18941 del 3 marzo 2004), i sindacati, le aziende ospedaliere, gli ordini professionali e via dicendo. Si tratta, in sostanza, di una nutrita serie di enti che, di per se stessi, non saranno assoggettabili alle sanzioni previste dal nuovo art. 24-*bis*della legge di ratifica.
Questo *genus* anomalo di responsabilità concepita dal Legislatore del d.lgs. 231/2001 – amministrativa da reato – non assorbe, tuttavia, la responsabilità penale del soggetto che abbia materialmente posto in essere le condotte criminose descritte dall'art. 24-*bis*, ma ad essa si affianca predisponendo una sanzione pecuniaria e, per alcune ipotesi, anche interdittiva.
L'entità della sanzione penale che viene, volta per volta, applicata è determinata sulla base di un duplice criterio di calcolo: per numero di quote e per valore delle medesime. Il valore (la cui forbice tra minimo e massimo è predeterminata per legge) di ogni singola quota dipende dalle condizioni economiche e patrimoniali dell'ente, mentre il numero di quote che il giudice deciderà di comminare varia in considerazione della gravità del fatto, del grado della responsabilità dell'ente e dell'impegno dell'ente nella rimozione o nell'attenuazione delle conseguenze negative del reato. Ovviamente (art. 8) l'ente sarà responsabile anche quando l'autore del reato non sia stato identificato o non sia imputabile o, ancora, quando il reato si estingua per una causa diversa dall'amnistia.
Il d.lgs. 231, tuttavia, pur distinguendo tra i casi in cui il reato sia stato commesso da persona in posizione apicale o soggetto ad altrui direzione, conferisce un notevole rilievo (anche di effetto liberatorio per l'ente) al modello di organizzazione dell'ente sia idoneo a prevenire i reati della specie di quello verificatosi.
Questi modelli (comunemente detti "*modello 231*") – lasciando per un attimo da parte il discorso sulla loro obbligatorietà o facoltatività – dovranno essere elaborati con una specifica analisi delle procedure di accesso e di utilizzo dei sistemi informatici aziendali: ad esempio modalità di utilizzo di strumenti informatici o telematici dell'ente o personali del dipendente o del soggetto posto in posizione apicale; *security policies* per filtri di traffico di rete, e così via discorrendo.
Questo documento (che per alcuni aspetti pratici ricorda il DPS prescritto quale misura minima obbligatoria dall'all. B del Codice della Privacy) deve risultare oggettivamente – *ex antea* (in caso contrario il modello di organizzazione non avrebbe alcun senso posto che alla commissione del reato conseguirebbe, necessariamente, la qualifica di "inidoneità" del modello adottato) – idoneo a rimuovere il rischio della commissione dei reati tassativamente elencati dal d.lgs 231.
Il difficile compito al quale saranno chiamati gli enti soggetti al d.lgs. 231/2001, a partire dall'entrata in vigore della disciplina di cui all'art. 24-*bis*, è quello di redigere puntuali documenti contenenti valutazioni prognostiche in grado di eliminare anche il rischio della commissione dei reati "informatici" di cui all'art.

24-*bis*. Si comprende, pertanto, quale importanza rivestano i di organizzazione dell'ente.
Oltre alle sanzioni pecuniarie, l'art. 24-*bis* la possibilità di comminare all'ente le sanzioni interdittive descritte dall'art. 9.
In particolare si prevede che nell'ipotesi di condanna dell'ente a seguito della commissione del reato – di accesso abusivo a sistema informatico o telematico (615-*ter* c.p.), di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-*quater* c.p.), di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico(617-*quinquies*c.p.), di danneggiamento di informazioni, dati e programmi informatici (635-*bis* c.p.), di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-*ter* c.p.), di danneggiamento di sistemi informatici o telematici (635-*quater* c.p.) e di ddi sistemi informatici o telematici di pubblica utilità (635-*quinquies* c.p.) - saranno applicabili le sanzioni dell'interdizione dall'esercizio dell'attività, della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e, infine, del divieto di pubblicizzare beni o servizi.
Si applicheranno, invece, le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito in caso di commissione del reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-*quater* c.p.) e di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (615-*quinquies* c.p.).
Infine per i reati previsti dal terzo comma dell'art. 24-*bis* applicheranno le sanzioni interdittive del divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un servizio pubblico); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi ed, ancora, il divieto di pubblicizzare beni o servizi.

4 CAPO III: MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

4.1 Art. 8. (Modifiche al titolo III del libro terzo del codice di procedura penale)

1. All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

2. All'articolo 247 del codice di procedura penale, dopo il comma 1 e` inserito il seguente:

«1-bis. Quando vi e` fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne

e` disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

3. All'articolo 248, comma 2, primo periodo,del codice di procedura penale, le parole:

«atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti:«presso banche atti, documenti e corrispondenza nonchè dati, informazioni e programmi informatici».

4. All'articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 1 è sostituito dal seguente:

«1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;

b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti:

«o alterarli».

5. Dopo l'articolo 254 del codice di procedura penale e` inserito il seguente:

«Art. 254-bis. – (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). – 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso e`, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

6. All'articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così e` ordinato,» sono inserite le seguenti:

«nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,».

7. All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo e` inserito il seguente:

«Quando la custodia riguarda dati, informazioni o programmi informatici, il custode e` altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».

8. All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti:

«, anche di carattere elettronico o informatico,»;

b) al comma 2 e` aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali puo` essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

4.2 Art. 9. (Modifiche al titolo IV del libro quinto del codice di procedura penale)

1. All'articolo 352 del codice di procedura penale, dopo il comma 1 e` inserito il seguente:

«1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

2. All'articolo 353 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 2 sono aggiunte, in fine, le seguenti parole: «e l'accertamento del contenuto».

b) al comma 3, primo periodo, le parole: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» sono sostituite dalle seguenti: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica,» e dopo le parole: «servizio postale» sono inserite le seguenti: «, telegrafico, telematico o di telecomunicazione».

3. All'articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente:

«In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

La legge di recepimento ha introdotto e modificato anche diverse disposizioni del codice di procedura penale.

Tra le più importanti si segnalano quelle relative alle ispezioni e quelle in materia di sequestro di dati informatici che hanno positivizzato alcune prassi consolidate in tema di investigazioni informatiche.
Dopo un appassionata ed elaborata analisi della normativa davanti alle Commissioni riunite Giustizia e Senato si è approdati in aula alla fine di febbraio con una serie di emendamenti al testo del disegno di legge del Governo.
Come già accennato, pur avendo il legislatore ascoltato l'opinione di tecnici ed esperti (e quindi modificato in alcune parti l'originario DDL), introdurre una norma processuale relativa alla "perquisizione del computer"[1] crea comunque seri problemi, vista la delicatezza della *computer forensics*[2] e il suo stretto legame con le garanzie processuali e l'inalterabilità del dato informatico.
In materia di acquisizione dei dati informatici e quindi di elementi di prova, tali modifiche si sono rese opportune, non solo per correggere errori dello schema di disegno di legge, ma anche per disciplinare un settore fino ad oggi governato dalla prassi investigativa.
Importanti emendamenti, apportati nell'ambito delle norme che disciplinano la materia delle ispezioni (art. 244 cpp), delle perquisizioni (art. 247 e art. 352 cpp) e del sequestro, hanno introdotto disposizioni correttive circa l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, e in altri casi l'adozione di procedure che assicurino la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.
Se questo non è altro che un commento a caldo, non vi è dubbio che nel prossimo futuro s'imporrà senz'altro un'analisi più approfondita e meditata di tutte le norme della legge di ratifica della Convenzione sul Cybercrime che non potrà non tenere in debito conto delle molte pronunce giurisprudenziali (di legittimità e di merito), in parte già pubblicate, ma che si attendono nei prossimi mesi ancor più numerose in questa materia.
La prossima pubblicazione su Gazzetta Ufficiale di queste norme è l'ultimo segnale in ordine di tempo che indica come la computer forensics in Italia stia passando da una fase "primitiva" o meglio "adolescenziale" ad una fase di maturità. Senza dubbio i prossimi anni saranno caratterizzati da importanti novità in ambito applicativo e giurisprudenziale e sarà interessante cogliere da vicino la direzione evolutiva.

4.3 Art. 10. (Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196)

1. Dopo il comma 4-bis dell'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sono inseriti i seguenti:

«4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici

[1] Si veda l'art. 7 del disegno di legge dell'11 maggio 2007 prima di essere modificato dagli emendamenti suggeriti e approvati nell'aula della Camera.
[2] La computer forensics è l'applicazione del metodo investigativo ai media digitali per ricavare elementi, informazioni, prove da portare in giudizio. Questo processo indaga sui sistemi informativi per determinare se essi siano stati impiegati in attività illegali o non autorizzate. (fonte: en.wikipedia.org)

centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonche´ gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorita` investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalita` indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalita` di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, puo` prevedere particolari modalita` di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attivita` conseguentemente svolte per il periodo indicato dall'autorita`. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca piu` grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

L'articolo 10 introduce un'importante modifica all'articolo 132 del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
Si tratta di una modifica che introduce il cd congelamento dei dati per ragioni urgenti.
In un articolo 132 che molto probabilmente tra qualche mese non sarà più com'è oggi (si prevede anche la presenza di un articolo 132 bis, con un art. 132 con i comma 4 ter, quater e quinquies che verranno risistemati in seguito all'entrata in vigore del decreto legislativo che recepirà la direttiva Frattini) l'articolo 10 della legge, che recepisce la Convenzione di Budapest, introduce delle disposizioni che conferiscono un potere non di poco conto alle forze di polizia ed ai servizi segreti.
Questo potere sembra limitato a casi eccezionali ed urgenti come quelli che determinano lo svolgimento delle indagini e delle intercettazioni preventive di cui all'art. 226 del decreto legislativo n. 271 del 1989. Sembra appunto, ma non siamo così sicuri.
La norma sul punto, in realtà aggiunge anche una formula forse ambigua che in sede Parlamentare si è cercato di modificare (senza successo) proprio per la sua

imprecisione, ovvero, *" ... di cui all'art. 226 del decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati"*.
E' di tutta evidenza che *accertamento e repressione di specifici reati* è una valvola di apertura che stona in una norma di carattere eccezionale com'è il comma 4 ter. L'apertura, appunto, ad ipotesi di reato non espressamente indicate significa poter applicare di fatto il comma 4 *ter* anche a reati diversi da quelli di cui alla convenzione sul cybercrime, diversi da quelli previsti dal 132 codice privacy e appunto specifici in quanto specificati a posteriori. Ciò non è proprio tranquillizzante sotto il profilo della chiarezza e della precisione normativa se si considera la portata internazionale della norma stessa in relazione ai rapporti che essa prevede con le autorità investigative straniere.
La circostanza che non si tratta di una norma che stabilisce il potere di "acquisizione" fuori dai termini del primo comma dell'art 132 bensì un potere meramente di "conservazione e protezione del dato" e tra l'altro con breve scadenza (sei mesi massimo), la circostanza che tutto ciò avviene vincolando al segreto assoluto (e punito) il gestore e con la massima indisponibilità del dato da parte dello stesso, la circostanza che i provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida e in caso di mancata convalida, i provvedimenti assunti perdono efficacia, non è sufficiente per lasciare questa norma esente da dubbi e da critiche.
Come non è sufficiente la circostanza che siamo in ambito di conservazione dei soli dati relativi al traffico telematico escluso il contenuto delle comunicazioni.
Innanzitutto non appare chiaro il perché si punisce così severamente, in linea potenziale, il gestore in caso di violazione degli obblighi di cui all'art. 4 *quater* quando altri e ben più pericolosi soggetti-agenti potrebbero trattare illecitamente il dato senza rispondere di alcun reato. Inoltre non è chiaro se il congelamento per complessivi 6 mesi può derogare il limite massimo di tempo di conservazione del file di LOG informatico (12 mesi nella stesura finale del 132 codice privacy che attua la direttiva Frattini).
Purtroppo non è passata in aula parlamentare la modifica suggerita con una certa insistenza e riguardante la necessità di affidare la convalida del provvedimento di cui al comma 4 *ter* al giudice del luogo dell'esecuzione anziché al pubblico ministero. Trattandosi del luogo di esecuzione del congelamento dei dati ovvero del luogo dove i dati sono conservati dal gestore, e considerato che SE trattasi di indagini (intercettazioni) preventive ex art. 226 norme coord. è evidente non vi è alcun procedimento penale e quindi nessun PM competente in virtù di un'indagine assegnata, la convalida del provvedimento affidata comunque al pubblico ministero del luogo fa sorgere il legittimo dubbio di un facile e spesso ricorrente "involontario appiattimento" del PM a tutte le richieste delle forze di polizia di cui al comma 4 ter. Indubbiamente meglio sarebbe stato, viste anche le sopra richiamate (e se vogliamo più preoccupanti) richieste avanzate dalle autorità investigative straniere, l'intervento di un giudice per le indagini preliminari.
Tutto l'articolo 10 della legge di ratifica (e quindi i comma 4 ter, quater e quinquies) investe, amplia e non risolve aspetti importanti relativi alla *data retention.* Ciò non fa che aumentare alcune perplessità sorte in questi ultimi mesi intorno a tutto il discorso della *data retention*.
Visti gli ultimi orientamenti dall'Autorità Garante, la sua grande e più volte manifestata attenzione per il problema *data retention*, l'animosità e la tenacia con

la quale si è battuto per far attuare la direttiva Frattini (direttiva 2006/24/CE) la battaglia sull'IP = contenuto di comunicazione (sempre e comunque ?) = pericolo del Grande Fratello, non si comprende come possa essere passata indenne al parere della stessa Autorità Garante e dello stesso e attentissimo Senato della Repubblica (anch'egli così attento al rischio di Grande Fratello tanto da modificare in sordina….il termine del 31.12.2008 del famoso Decreto Pisanu sulla *data retention* " complessiva") un siffatto art. 10 con i suoi tre commi ricchi di macroscopiche contraddizioni se letti nel quadro complessivo.
In tutta la materia della *data retention* si è notata troppo spesso negli ultimi tempi una certa schizofrenia interpretativa e normativa alla quale si sperava di non assistere vista l'importanza e soprattutto l'equilibrio che la materia deve mantenere tra esigenze di indagini antimafia (e antiterrorismo) e esigenze di riservatezza degli individui.

4.4 Art. 11. (Competenza)

1. All'articolo 51 del codice di procedura penale e` aggiunto, in fine, il seguente comma:

«3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

L'articolo 11 della legge di ratifica amplia il novero dei reati le cui indagini sono affidate agli uffici del pubblico ministero presso il tribunale del capoluogo del distretto di corte d'appello.
Questo soluzione "accentratrice" era stata originariamente (1991) pensata con riferimento al contrasto dei reati commessi dalla criminalità organizzata (mafiosa o terroristica), al fine di ottenere un effettivo coordinamento nelle indagini tra le diverse procure della Repubblica.
Tuttavia l'obiettivo del coordinamento tra procure della Repubblica anche per i reati contemplati dall'art. 11 appare di difficile realizzazione. E ciò in considerazione dell'assenza, in quest'ipotesi, di un organo omologo alla Direzione Nazionale Antimafia.
E' evidente, pertanto che obiettivo principale del novellando comma 3-*ter* dell'art. 51 c.p.p. sia rappresentato dalla formazione di appositi "pool" di magistrati inquirenti specializzati. E questo obiettivo pareva maggiormente raggiungibile all'interno delle procure con più alto numero di sostituti procuratori.
Questa scelta legislativa deve essere attentamente vagliata e ne devono essere soppesati gli effettivi benefici (in termini, quantomeno, di economia processuale).
E' ben vero che grazie a questa modifica delle competenze i procuratori della Repubblica presso il tribunale del capoluogo del distretto di corte d'appello potrebbero acquisire una notevole esperienza "sul campo". Tuttavia si tratterebbe di competenze non immediatamente tecnico-informatiche. I magistrati, si

troveranno – pur sempre – a dover disporre di consulenti tecnici, esperti informatici, che ricavino dai fatti concreti, concreti risultati. L'unica specializzazione – ma forse sarebbe meglio parlare unicamente di esperienza – che si avrebbe non sarebbe certo prerogativa di una casta di centauri, mezzo magistrati e mezzo tecnici informatici. Sarebbe sufficiente, infatti, prevedere semplici eventi formativi e di aggiornamento – questi si – a livello distrettuale.
E' vero, inoltre, che ulteriore conseguenza di quest'operazione accentratrice sarebbe quella di incrementare il carico delle procure distrettuali. Senza lo stanziamento di fondi a sostegno delle procure distrettuali, già notevolmente affaticate da carenza di strumenti e personale (amministrativo e giudiziario), sarà quindi difficile prevedere gli auspicati risultati di un miglior coordinamento. Sarebbe stato forse più opportuno dirottare lo stanziamento di fondi previsto al successivo art. 12 all'adeguamento di uomini e mezzi a disposizione delle procure distrettuali.
Secondo alcuni commentatori l'art. 11 suscita perplessità in ordine alla violazione dell'art. 25, primo comma, della Costituzione, in quanto determinerebbe un irragionevole sconvolgimento del preesistente ordine di competenza dei pubblici ministeri, e quindi, una violazione del principio del giudice naturale precostituito per legge.
Personalmente ritengo il problema un falso problema. Il principio costituzionalmente garantito del "giudice naturale precostituito per legge", infatti, prevede: a) che la competenza del giudice possa essere determinata unicamente per legge; b) che la competenza debba essere determinata sulla base di un principio di ragionevolezza e; c) che le norme sulla competenza non possano essere applicate retroattivamente.
Con il principio del giudice naturale precostituito per legge si assicura, in sostanza, l'imparzialità di chi esercita la funzione giurisdizionale ossia di chi è chiamato a *juris-dicere*: non ci si riferisce anche al magistrato inquirente (si veda fra tutte C.Cost., sent. 148/63 ed anche sent. 481/95).
A tal proposito, inoltre, è utile osservare che la legge di ratifica della Convenzione di Budapest non ha introdotto alcuna novità all'art. 328 c.p.p. (giudice per le indagini preliminari), ed in genere non ha spostato la competenza del giudice per le indagini preliminari. Ciò significa che pur essendo la competenza per le indagini preliminari ed i procedimenti di primo grado in seno ai magistrati inquirenti presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente, in ogni caso il giudice per le indagini preliminari competente resta immutato.
Ci troviamo di fronte, indubbiamente, ad un'anomalia del sistema che merita un ripensamento o, quantomeno, di un'integrazione. E ciò in considerazione del fatto che il pubblico ministero sarà costretto a sgretolare la medesima indagine tra più uffici del GIP – si pensi ai reati commessi in più circondari appartenenti allo stesso distretto di corte d'appello – nel caso in cui egli debba richiedere eventuali provvedimenti, come ad esempio quello di emissione di misure cautelari reali (per citare le più frequenti nel caso di crimini informatici).

4.5 Art. 12. (Fondo per il contrasto della pedopornografia su internet per la protezione delle infrastrutture informatiche di interesse nazionale)

1. Per le esigenze connesse al funzionamento del Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di cui all'articolo 14- della legge 3 agosto 1998, n. 269, e dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione per le esigenze relative alla protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, di cui all'articolo 7-del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni,dalla legge 31 luglio 2005, n. 155, e` istituito, nello stato di previsione del Ministero dell'interno, un fondo con una dotazione di 2 milioni di euro annui a decorrere dall'anno 2008.

2. Agli oneri derivanti dal presente articolo, pari a 2 milioni di euro annui a decorrere dall'anno 2008, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 2008- 2010, nell'ambito del fondo speciale di parte corrente dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2008, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia.

3. Il Ministro dell'economia e delle finanze e` autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

5 CAPO IV: DISPOSIZIONI FINALI

5.1 Art. 13. (Norma di adeguamento)

1. L'autorita` centrale ai sensi degli articoli 24, paragrafo 7, e 27, paragrafo 2, della Convenzione e` il Ministro della giustizia.

2. Il Ministro dell'interno, di concerto con il Ministro della giustizia, individua il punto di contatto di cui all'articolo 35 della Convenzione.

5.2 Art. 14. (Entrata in vigore)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La scelta di un termine diverso da quello di quindici giorni – di cui all'ultimo comma dell'art. 73 Cost. – dovrebbe essere dominata dalla ragionevolezza. E ciò, in particolare, quando siano trascorsi sette anni per il recepimento di una Direttiva ispirata dall'emergenza terroristica ed alla paura "post-11 settembre 2001".

Sarebbe stato, pertanto, ragionevole non abbreviare il termine di vacatio legis. Un termine, si ricordi, che trova la sua ragione di fatto nel consentire una conoscenza della legge a tutti i cittadini e che rappresenta, inoltre, una mitigazione al principio secondo cui "*ignorantia legis non excusat*". Ciò è tanto più vero quando si tratti anche di norme penali incriminatrici.
Sarebbe stata opportuna, inoltre, l'introduzione di una norma transitoria per regolare le ipotesi in il processo penale sia già in itinere al momento dell'entrata in vigore della legge di ratifica.
Infine sarebbe stato auspicabile un sistema applicazione progressiva dell'articolo 7 della legge di ratifica. E ciò in quanto il brevissimo lasso di tempo intercorrente tra pubblicazione ed entrata in vigore della legge provocherà enormi disagi per tutti quegli enti soggetti al d.lgs. 231/2001 che non riusciranno – a meno di compiere evoluzioni e salti mortali – a predisporre i modelli organizzativi idonei.
Sarebbe stata pertanto opportuna l'introduzione di una norma transitoria finalizzata ad evitare un dispendio di energie e di risorse impegnate nelle indagini già in corso al momento dell'entrata in vigore della legge di ratifica della Convenzione di Budapest. Sarebbe stato sufficiente una norma in base alla quale le cause di inutilizzabilità della prova correlate alle modifiche al codice di procedura penale si dovessero applicare solo ai procedimenti instaurati successivamente alla data della sua entrata in vigore.