

«I REATI INFORMATICI: ASPETTI SOSTANZIALI E PROCESSUALI;

LE MISURE CAUTELARI PREVISTE DAL D. LGS. 231/2001»

Relazione tenuta in data 20.06.2008 dall'avv. Beniamino Migliucci

presso l'Università degli Studi di Ferrara al Seminario:

«D. Lgs. 231/2001 – La responsabilità “penale” delle persone giuridiche.

Modelli organizzativi: Aspetti problematici»

* * *

1. Premessa: la legge 18 marzo 2008, n. 48 e la riforma del diritto penale «dell'informatica».

La legge 18 marzo 2008, n. 48 di ratifica della Convenzione di Budapest sul “*cyber-crime*” del 23 novembre 2001¹ ha introdotto significative e sostanziali modifiche all'intero assetto dei reati c.d. «informatici» ed ha inciso altresì su profili processuali in tema di ispezioni, perquisizioni, sequestro di corrispondenza, regime della c.d. “*data retention*” (ovvero, conservazione dei dati) e, non ultimo, ha previsto l'estensione della responsabilità «amministrativa da reato» delle persone giuridiche ex D. Lgs. 231/2001 anche per la maggior parte dei reati informatici (in precedenza erano previsti quali reati “presupposto” soltanto la frode informatica aggravata ed il commercio di materiale pedopornografico)².

Si può quindi affermare che la legge 48/2008 rappresenta una riforma - sebbene imperfetta e non certo priva di lacune e contraddizioni - di carattere organico, tendente ad un riassetto dell'intera materia, sostanziale e processuale, dei reati

¹ La Convenzione di Budapest del 2001, risultato di un lavoro durato quattro anni di un comitato di esperti in seno al Consiglio d'Europa, è stata tuttora ratificata da 21 paesi, fra i quali non compaiono tuttavia alcuni di quelli a più alto sviluppo industriale e tecnologico, come la Germania, il Regno Unito, la Spagna, la Svezia e la Svizzera.

² La previsione dei reati informatici nel catalogo dei delitti richiamati dal D. Lgs. 231/2001 al fine di fondare una responsabilità «amministrativa da reato» degli enti (v. “nuovo” art. 24-*bis* D. Lgs. 231/2001) discende direttamente dall'art. 12 della Convenzione di Budapest.

informatici. Al riguardo, come si avrà modo di osservare nel prosieguo di questa relazione, la legge in parola - adottata formalmente quale «*Ratifica ed esecuzione*» della Convenzione di Budapest del 2001 ed approvata in tempi rapidissimi a Camere ormai sciolte della XV Legislatura – sembra piuttosto l'«occasione» colta dal Legislatore italiano per procedere ad una riscrittura di tutta la materia, anche al di là delle previsioni pattizie internazionali.

Nella presente relazione, in considerazione proprio dell'ampiezza della riforma del 2008 e delle notevoli ricadute della stessa sulla disciplina della responsabilità «amministrativa da reato» degli enti, si cercherà di dar conto soltanto di alcuni aspetti a nostro avviso più interessanti o problematici, non essendo possibile – visti anche i limiti di spazio e di tempo – affrontare ogni singola novità.

Facciamo ora un piccolo passo indietro.

In tema di reati e criminalità «informatica», com'è noto, il primo storico (ed anche, se vogliamo, organico) intervento del Legislatore italiano risale alla legge 23 dicembre 1993, n. 547 (recante «*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale*»)³, con la quale, da un lato, (i) erano state inserite nuove fattispecie di reato all'interno del codice penale (si pensi alla frode informatica di cui all'art. 640-ter o al danneggiamento di sistemi informatici o telematici di cui all'art. 635-bis) e, dall'altro, (ii) erano state introdotte nuove previsioni di adeguamento del (seppur appena approvato) codice di rito (si pensi, ad es., all'art. 266-bis in tema di intercettazioni informatiche o telematiche).

Da un punto di vista sostanziale, si può dire che il Legislatore del 1993 avesse tenuto ben presente che non si trattava tanto di introdurre fattispecie che tutelassero “nuovi beni giuridici”, quanto piuttosto di apprestare tutele più incisive contro “nuove forme di aggressione”, condotte con modalità prima sconosciute, a beni giuridici in larga parte già penalmente rilevanti e tutelati con norme codicistiche (si pensi, su tutti, all'esempio della frode informatica ex art. 640-ter c.p., rispetto alla quale il bene

³ La L. 547/1993 recepiva peraltro le indicazioni provenienti dal Consiglio d'Europa già a partire dagli anni ottanta.

giuridico tutelato resta fundamentalmente sempre il «patrimonio»⁴, cambiando invece notevolmente le forme di aggressione dello stesso rispetto alla truffa “tradizionale”).

Al riguardo, si può senz'altro affermare che, allora (1993) come ora (2008), il settore dei reati c.d. «informatici» ha sempre posto (e continua a porre) notevoli questioni in tema di tassatività, determinatezza e divieto di analogia, atteso che molto spesso vi sono condotte che colpiscono beni giuridici “tradizionali” o comunque già esistenti (la fede pubblica, il patrimonio, etc.) attraverso forme di aggressione del tutto nuove (per le modalità di realizzazione, per la peculiarità dell'oggetto materiale, etc.), determinate dalla continua evoluzione tecnologica e difficilmente inquadrabili sotto le figure di reato già presenti.

Questione parzialmente diversa, e ciò nondimeno di grandissima rilevanza dopo le modifiche al codice di rito introdotte dalla L. 48/2008, si pone in relazione, ad es., alle nuove disposizioni in tema di sequestro di corrispondenza (a seguito della riscrittura dell'art. 254 c.p.p.) dove i messaggi di posta elettronica (*e-mail*) sono equiparati alla posta tradizionale (lettere, etc.). In questo caso, infatti, vi è il possibile (ed assai concreto) rischio che l'Autorità giudiziaria, nel momento stesso della “apprensione” della comunicazione telematica, possa – per la natura stessa del messaggio *e-mail* (in quanto, molto banalmente, non è inserito in busta chiusa, né chiuso in un piego, etc., ma consistente in dati direttamente visibili *online*) – aprire lo stesso e conoscerne quindi il contenuto (nonostante la norma sul sequestro faccia divieto di apertura e presa di conoscenza del contenuto), senza le garanzie previste per le intercettazioni telematiche di cui all'art. 266-*bis* c.p.p. (rimasto peraltro inalterato dalla sua introduzione nel 1993⁵).

⁴ Va comunque precisato che secondo la giurisprudenza si tratta di un reato plurioffensivo: l'art. 640-*ter* c.p. tutelerebbe quindi anche la «riservatezza» e la «regolarità dei sistemi informatici» (in questo senso, fra le altre, Cass. pen., sez. V, 24 novembre 2004, *Nota*).

⁵ Al riguardo va ricordato l'ormai abbandonato disegno di legge c.d. “Mastella” sulle intercettazioni (licenziato dalla Camera il 17 aprile 2007) che proponeva l'introduzione di un nuovo art. 266-*ter* c.p.p. (secondo cui «*le norme del presente capo si applicano, in quanto compatibili, alle intercettazioni di corrispondenza postale che non interrompono il corso della spedizione*»).

Da una parte, vi è infatti il rischio concreto che residuino più o meno ampie aree di impunità, dettate, non solo e non tanto da una precisa e “cosciente” scelta del Legislatore (in ossequio ai principi di frammentarietà e sussidiarietà del diritto penale), quanto piuttosto dalla costante inadeguatezza ed arretratezza dello strumento legislativo di fronte all'avanzare della tecnologia informatica e telematica.

D'altro canto, non si può trascurare il fatto che si possono verificare casi di applicazione estensiva al limite dell'analogia di fattispecie di reato «informatico» a condotte difficilmente ivi sussumibili, determinata da una tecnica legislativa spesso imprecisa ed approssimativa ed anche, non ultimo, da una non sempre idonea preparazione tecnica in materia da parte degli organi inquirenti e giudicanti⁶.

A quest'ultimo proposito, la L. 48/2008 ha modificato l'art. 51 del codice di rito, secondo il quale ora le investigazioni per i reati informatici e di pedopornografia sono devolute all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto in cui il giudice competente ha la propria sede. Si tratta, evidentemente, di un tentativo di soddisfare l'esigenza di concentrazione e coordinamento, con l'intenzione, quindi, di garantire una maggior specializzazione attraverso un più alto tasso di «tecnicità» (è noto infatti che per le indagini relative ai reati *de quibus* non esiste una struttura assimilabile alla Direzione nazionale antimafia)⁷.

Un'altra questione di fondo in relazione ai reati «informatici» - soprattutto nell'ottica della commissione degli stessi nell'«interesse» o «a vantaggio» di un ente⁸ dopo la riforma *ex lege* 48/2008 del D. Lgs. 231/2001 – è rappresentata da possibili forme di responsabilità oggettiva occulta degli enti (ancorché nella forma atipica “para-penale”

⁶ Sebbene ormai presso quasi tutte le Procure della Repubblica siano stati istituiti gruppi di lavoro (o comunque incaricati singoli Pubblici ministeri) per la trattazione dei reati «informatici».

⁷ Nella relazione alla Camera al disegno di legge n. 2807 del 19.06.2007 si afferma chiaramente che «con l'art. 10 si è disposto l'inserimento del co. 3-quinquies nell'art. 51 del codice di procedura penale per concentrare la competenza per i reati informatici presso gli uffici di procura distrettuali. Ciò è stato previsto al fine di facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia».

⁸ Art. 8, co. 1 D. Lgs. 231/2001: «L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio».

di cui al D. Lgs. 231/2001) di fronte a condotte criminali sempre più insidiose commesse da soggetti sottoposti (v. art. 5, co. 1 lett. b D. Lgs. 231/2001) con un vantaggio o interesse anche remoto ed indiretto per l'ente medesimo.

In altri termini, là dove – ad es. - il dipendente della persona giuridica commetta un reato «informatico» compreso nel nuovo catalogo dell'art. 24-*bis* D. Lgs. 231/2001, e là dove alla commissione del reato consegua pure un qualche vantaggio per l'ente (conseguenza magari non voluta dall'autore), può verificarsi il rischio concreto di una responsabilità in capo all'ente stesso.

Il rischio appare ancor più evidente, come sempre, nel campo di applicazione delle *misure cautelari* che, in virtù del richiamo dell'art. 45 D. Lgs. 231/2001 alle sanzioni interdittive di cui all'art. 9, co. 2, rappresentano una forma di punizione “anticipatoria” assai penetrante (e potenzialmente compromettente) per il prosieguo dell'attività economica della persona giuridica.

Certo, si obietterà, la società andrà esente da responsabilità là dove dimostri di aver adottato ed implementato degli adeguati «modelli organizzativi», come prescritto dall'art. 6 D. Lgs. 231/2001.

Tuttavia, nel settore del diritto dell'informatica – a fronte di possibili elusioni da parte di dipendenti “tecnologicamente” esperti - appare in questo momento assai problematico definire o comunque indicare possibili direttive o linee guida sicure (o relativamente sicure...) al fine di esentare l'ente da responsabilità amministrativa da reato (soprattutto, come detto, in via cautelare, dove l'accertamento è per definizione sommario ed anticipatorio).

2. La nozione di reato «informatico» (e «telematico») in relazione al nuovo diritto penale sostanziale e processuale dopo la legge 18 marzo 2008, n. 48.

A questo punto occorre brevemente soffermarsi sulla non sempre agevole nozione di reato «informatico», anche a seguito della recentissima riforma della L. 48/2008.

La Convenzione di Budapest ha adottato una definizione assai ampia di reato «informatico», intendendo con tale espressione, da un lato, tutte le condotte delittuose in qualunque modo *commesse attraverso un sistema informatico* e, dall'altra, le fattispecie di cui si debbano o possano *raccogliere prove in forma elettronica*.

In estrema sintesi, in accordo sul punto con la dottrina maggioritaria (PICA, PECORELLA, SARZANA DI SANT'IPPOLITO), si può allora affermare che il connotato distintivo dei reati «informatici e telematici» (si riconosce generalmente che la mera nozione di reato «informatico» appare di per sé riduttiva, sebbene sia generalmente accolta ed utilizzata per brevità e comodità espositiva) consiste nella loro correlazione con l'*informatica* e i suoi prodotti (in quanto *attività di elaborazione e trattamento automatizzato dei dati*) ovvero con la telematica (in quanto *modalità di trasmissione e comunicazione a distanza di dati informatici*)⁹.

Per quanto riguarda più propriamente il settore d'indagine del presente lavoro, ci si limiterà ad accogliere una definizione se vogliamo “formale” o “letterale” di reato «informatico», in quanto espressamente recepito e richiamato dal codice penale e soprattutto dal “nuovo” art. 24-*bis* D. Lgs. 231/2001 (secondo la tecnica del rinvio “formale” alle fattispecie di reato codicistiche).

3. Il disegno di legge n. 2807 e l'approvazione della legge 18 marzo 2008, n. 48.

La L. 48/2008 è stata approvata quando la scorsa Legislatura era ormai già terminata, con un consenso pressoché unanime dell'(allora) maggioranza ed opposizione. Il dato non può che destare un certo stupore, anche nell'attuale mutato clima (non si sa

⁹ Per approfondimenti, si veda A. CISTERNA, *Previsto uno statuto processuale ad hoc (Commento alla L. 48/2008)*, in *Guida al Dir.*, 2008, f. 16, pp. 64 – 65 e gli Autori ivi citati.

quanto duraturo) di “larghe intese” ed ampie convergenze fra i due principali schieramenti politici¹⁰.

La legge nasce da un disegno di iniziativa governativa di alcuni mesi precedente (Disegno di legge 19 giugno 2007, n. 2807¹¹) ed ha subito un iter parlamentare quanto meno “singolare”: dopo la presentazione, infatti, il d.d.l. è stato trattato in due sedute preliminari delle Commissioni Giustizia ed Affari esteri della Camera (del 25 settembre 2007 e del 3 ottobre 2007), in cui peraltro ben poco è stato fatto, rimanendo quindi a “decantare” in attesa per quasi cinque mesi, fino al 19 febbraio 2008. In quella data, con un’accelerazione davvero inusuale, è stato concluso l’esame del testo in sede referente e quindi trasmesso il testo all’aula, con un solo emendamento. Il giorno successivo (20 febbraio 2008) la Camera ha approvato a larghissima maggioranza, provvedendo quindi a trasmettere il testo al Senato. Il Senato, a sua volta, ha esaurito in brevissimo tempo (sia in Commissione, sia in aula) l’esame del testo ed il voto finale è intervenuto in tempi quasi da “record” il 27 febbraio 2008.

Al riguardo, va sottolineata la protesta dell’on. Costa, il quale – replicando alla seduta del 19 febbraio 2008 al Presidente della II Commissione (Giustizia) della Camera on. Pisicchio – ha stigmatizzato l’accelerazione dell’iter parlamentare, affermando che si è soltanto «tentato di porre in essere un’istruttoria completa», atteso che «purtroppo non è stato possibile svolgere le audizioni» che erano state in precedenza programmate.

La fretta, si sa, come insegnavano i nostri padri, è cattiva consigliera e, quanto meno ad una prima lettura, la L. 48/2008 non sembra fare eccezione all’antica regola. Lasciamo, più che ai posteri, agli operatori del diritto (dottrina e giurisprudenza in

¹⁰ È peraltro notizia di questi giorni in cui si chiude il presente lavoro (17 giugno 2008) lo “strappo” verificatosi fra maggioranza ed opposizione in tema di “Decreto sicurezza”, soprattutto con riguardo alla norma processuale asseritamente “salva-Premier”.

¹¹ Recante «Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno».

testa) l'ardua sentenza: dai primi commenti apparsi, comunque, l'accoglienza alla L. 48/2008 è stata quanto meno "tiepida", se non apertamente critica.

Peraltro, pare interessante osservare come nella Relazione al disegno di legge n. 2807 si affermi – in punto di diritto penale sostanziale - che *«l'Italia [è] stato uno dei primi paesi europei ad introdurre una legge organica, la legge 23 dicembre 1993, n. 547, in tema di delitti informatici»* e che comunque il nostro paese ha introdotto diverse discipline *ad hoc* (L. 675/1996 sulla tutela della *privacy*; L. 269/1998 sulla pedopornografia in rete; etc.) : insomma, *«alla luce di ciò»*, secondo la Relazione, *«...la portata dell'adeguamento normativo da realizzare, per l'esecuzione della Convenzione [di Budapest], nel settore del diritto penale sostanziale è risultata modesta, essendo, in molti casi, già in vigore una disciplina esaustiva»*.

Ma, al di là degli intenti espressi nella Relazione al d.d.l., è facile capire che la L. 48/2008 rappresenta una vera e propria "rivoluzione copernicana" nel settore del diritto penale (e processuale) dell'informatica, le cui ricadute peraltro si possono ora soltanto intravedere, anche e soprattutto in relazione all'estensione della responsabilità «amministrativa da reato» degli enti per la commissione di delitti informatici.

4. I reati «informatici» dopo la L. 48/2008: alcune osservazioni.

Nonostante, come appena ricordato, nella Relazione al disegno di legge si accennasse a semplici «modifiche» o «adeguamenti» della disciplina (sostanziale) vigente in materia di reati informatici, la riforma del 2008 ha inciso realmente sul «volto» del diritto penale (sostanziale) dell'informatica, apportando significative (e non sempre positive) innovazioni.

Resta comunque immutata la scelta "di campo" del Legislatore di mantenere i reati informatici all'interno del codice penale. Ebbene, se la scelta di per sé appare condivisibile per ragioni politico-criminali, si deve riconoscere che essa spesso si trasforma in una "forzatura" foriera di collocazioni sistematiche quanto meno

“eccentriche”: si pensi, ad es., all’art. 640-*quinqüies* c.p. che integra una tipica fattispecie di inosservanza di norme amministrative assimilabile, al limite, ad una sorta di abuso d’ufficio o al limite corruzione *sui generis*, collocato fra i «*delitti contro il patrimonio mediante frode*» (!)

Un’altra “opzione” in materia di criminalità informatica confermata dal Legislatore della riforma del 2008 è la previsione di fattispecie esclusivamente delittuose: i reati c.d. «informatici» sono infatti tutti *delitti* (con ogni conseguenza in tema di elemento soggettivo, configurabilità del tentativo, prescrizione, effetti sulla recidiva, etc).

Ma torniamo ora alla L. 48/2008 ed alle rilevanti novità in tema di diritto penale sostanziale (che si riflettono poi, come vedremo, sulla disciplina della responsabilità degli enti, in virtù del nuovo art. 24-*bis*).

E così, schematizzando alquanto:

- sono state apportate rilevanti modifiche in materia di falsità informatica (art. 491-*bis* c.p.), soprattutto in relazione alla nozione (tipicamente “normativa”) di «*documento informatico*» (che passa da elemento “normativo” *ad hoc* di carattere esclusivamente penale – cfr. “vecchio” art. 491-*bis*, co. 2 c.p. - ad elemento normativo *extrapenale*, in quanto definito dall’art. 1 lett. P del c.d. “Codice dell’Amministrazione digitale”, D. Lgs. 7 marzo 2005, n. 82). Più in particolare, è stato abrogato il secondo comma dell’art. 491-*bis* c.p. che prevedeva una definizione normativa (di rilevanza solo penalistica) di «*documento informatico*», giustamente riconosciuta come ormai inadeguata¹². Secondo la vecchia disciplina infatti, risalente ancora alla L. 547/1993, tale nozione era collegata, da un lato, al concetto di «*supporto informatico*» ed attribuiva quindi rilevanza, più che al *dato* informatico, all’elemento «materiale» sul quale era contenuto (il «*supporto*»), e, dall’altro, legava il concetto di documento a quello di «*programma*», con opzione ancora una volta incongruente, atteso che il programma è uno strumento operativo e non un documento¹³. Con l’eliminazione di

¹² La Relazione al d.d.l. 2807 (si veda anche *retro*) parla di «*sopravvenuta inadeguatezza*» della definizione contenuta nel “vecchio” comma secondo dell’art. 491-*bis* c.p.

¹³ Sul punto si veda anche P. SCOGNAMIGLIO, *Criminalità informatica*, Simone, 2008, pp. 14 – 15.

tale definizione, e conseguentemente la “ri-espansione” della nozione contenuta nel D. Lgs. 82/2005 (Codice dell’Amministrazione digitale), il «documento informatico» oggetto di possibile falsificazione è la *«rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»*;

- è stata per la prima volta introdotta una disciplina penale a tutela delle certificazioni relative alle «firme elettroniche» (art. 495-bis; art. 640-quinquies c.p., quest’ultimo con una collocazione sistematica quanto meno “eccentrica” rispetto al bene giuridico protetto). Per quanto riguarda il nuovo delitto di false dichiarazioni al certificatore di firma elettronica (art. 495-bis c.p.), la previsione estende la tutela della veridicità delle dichiarazioni/attestazioni anche al nuovo “istituto” della firma elettronica (di sempre più largo uso anche fra colleghi nello svolgimento della professione); al riguardo, è interessante notare la creazione di una nuova qualifica soggettiva (il «certificatore di firma elettronica»), dotata di poteri certificativi tipici della pubblica amministrazione (cfr. art. 357, co. 2 c.p.) e che, nell’esercizio della propria attività (connotata da una chiara finalità di interesse pubblico), potrà eventualmente commettere il nuovo reato (“proprio”) previsto dall’art. 640-quinquies c.p. (*«Frode informatica del soggetto che presta servizi di certificazione di firma elettronica»*): a quest’ultimo riguardo, va subito osservato che la norma *de qua*, nonostante sia inserita all’interno del capo dei *«Delitti contro il patrimonio mediante frode»*, non presenta alcun connotato di fraudolenza, sanzionando piuttosto l’inosservanza (addirittura *sub specie* di mera violazione) degli obblighi certificativi (di firma elettronica) stabiliti in sede extrapenale (in particolare, dall’art. 32, co. 2 del Codice dell’Amministrazione digitale); la norma non richiede alcun evento di lesione patrimoniale, ma semplicemente si limita a “colorare” la condotta di un dolo specifico assai ampio (*«procurare a sé o ad altri un ingiusto profitto»* alternativamente e non cumulativamente all’*«arrecare ad altri danno»*);

- è stato riformulato il delitto di cui all’art. 615-quinquies c.p., che punisce la diffusione di dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico *«allo scopo di danneggiare illecitamente un sistema informatico o telematico»* (norma che mirava, nella formulazione di cui alla L. 547/1993 come

nell'attuale nuovo testo *post lege* 48/2008, a reprimere la diffusione di *virus* informatici, ovvero di quei programmi a tutti più o meno noti che “infettano” un sistema informatico o telematico cagionando gravi danni al funzionamento dello stesso e, talvolta, addirittura compromettendolo definitivamente); la nuova formulazione appare più completa dal punto di vista della descrizione della condotta («*si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione*») e soprattutto introduce l'elemento soggettivo del dolo specifico, che rischia però di sbilanciare eccessivamente l'attenzione dal piano materiale a quello, appunto, soggettivo (secondo quanto apparso nei primi commenti);

- è stata riscritta *ex novo* la disciplina in materia di danneggiamento informatico (dall'art. 635-*bis* all'art. 635-*quinqüies* c.p.) con un notevole “appesantimento” della disciplina attraverso l'introduzione di ben tre nuove fattispecie di reato (e la contestuale abrogazione del secondo e terzo comma dell'art. 420 in tema di attentato ad impianti di pubblica utilità); interessante sottolineare il nuovo regime di procedibilità a querela della persona offesa dell'ipotesi-base di danneggiamento di dati informatici (art. 635-*bis* c.p.), che in precedenza (L. 547/1993) era procedibile d'ufficio, la condotta, poi, è stata tipizzata con maggiore aderenza rispetto all'oggetto materiale (nella formulazione precedente del 1993 era fin troppo chiaro il legame con il danneggiamento “comune”); a livello sistematico (o meglio, “micro-sistematico”) le nuove fattispecie dall'art. 635-*bis* fino all'art. 635-*quinqüies* c.p., se, da un lato, dimostrano una censurabile “elefantiasi” normativa da parte del Legislatore, dall'altro lato giustamente suddividono l'oggetto materiale della condotta in «*informazioni, dati e programmi informatici*» separandolo dai differenti «*sistemi informatici e telematici*».

5. *Le modifiche al codice di procedura penale apportate dalla legge 18 marzo 2008, n. 48.*

Si è già accennato alle incisive modifiche al codice di rito, peraltro applicabili non solo ai reati «informatici» intesi in senso stretto, ma anche ai reati solo

“eventualmente” informatici (ovvero i reati per la cui commissione ci si sia in qualunque modo avvalsi di uno strumento informatico e/o telematico).

È stato infatti rivisto il regime delle ispezioni (art. 244 c.p.p.), delle perquisizioni (artt. 247, 248 c.p.p.), del sequestro di corrispondenza (artt. 254 e nuovo 254-*bis* c.p.p.), nel caso in cui tali atti vengano disposti dall’Autorità giudiziaria, così come sono state modificate le disposizioni di cui agli artt. 352 – 354 c.p.p. relativamente all’attività di Polizia giudiziaria. È stato poi modificato il regime della conservazione dei dati (c.d. “*data retention*”) di cui all’art. 132 Codice della Privacy (D. Lgs. 196/2003), i cui tre nuovi commi introdotti dalla L. 48/2008 prevedono, in sostanza, l’obbligo per i fornitori di servizi telefonici di conservare (oltre ai termini ordinari) per un periodo di novanta giorni, prorogabile fino a sei mesi, su richiesta peraltro dei soggetti più disparati (Questore, Ministro dell’interno, uffici specialistici della Guardia di finanza, etc.), i dati di traffico, per finalità essenzialmente di carattere *preventivo*.

In primo luogo, emerge subito che il Legislatore, a fronte di una riforma incisiva *anche* sul codice di rito (rimasto inalterato addirittura dalla L. 547/1993), abbia perso l’occasione per procedere ad una riforma organica o comunque per tentare di risolvere talune scottanti questioni applicative manifestatesi nella giurisprudenza più recenti (si pensi al tema delle intercettazioni di comunicazioni vocali effettuate con sistemi c.d. «*voice-over-IP*», come, ad es., «*Skype*»), l’apprensione in tempo reale della posta elettronica, etc.

Ma, al di là delle critiche all’impianto della riforma nella parte processuale, cerchiamo ora di evidenziare alcuni spunti particolarmente significativi.

In primo luogo, le disposizioni processuali riformate in tema di ricerca della prova prescrivono che, qualora l’oggetto di indagine sia un sistema informatico, debbano essere adottate «*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione*».

Insomma, viene giustamente riconosciuta la peculiarità del dato digitale, assai “volatile” ed alterabile per sua stessa natura. Tuttavia, non viene indicata alcuna modalità operativa in concreto, salvo la previsione del nuovo art. 354 c.p.p. che richiede, «*ove possibile*», che si proceda «*all'immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*».

Ragioni di carattere tecnico-informatico, impossibili da approfondire in questa sede, portano a dubitare che la Polizia giudiziaria (che agisce prima dell'intervento del Pubblico ministero) non stia in realtà effettuando un accertamento tecnico di natura «irripetibile» o surrogati di fatto equivalenti (che andrebbero, al contrario, ovviamente svolti in contraddittorio ex art. 360 c.p.p.).

Insomma, non convince molto il fatto che le operazioni informatico-digitali di cui al “nuovo” art. 354 c.p.p. integrino della mere osservazioni, individuazioni e/o acquisizioni di dati.

Parrebbe quindi fondata, in chiave processuale, l'eccezione difensiva secondo cui in simili casi vi sarebbe un'impossibilità, per Giudice, Avvocato ed anche Pubblico ministero, di esaminare il concreto funzionamento dei *software* utilizzati per il rilevamento, l'osservazione e la duplicazione dei dati digitali, e quindi di poter controllare la correttezza del procedimento seguito dalla Polizia giudiziaria in sede di operazioni ex “nuovo” art. 354 c.p.p.

L'art. 24-bis D. Lgs. 231/2001: i nuovi “reati informatici presupposto” commessi nell'interesse o a vantaggio dell'ente...

In relazione alla responsabilità «amministrativa da reato» degli enti, la legge 18 marzo 2008, n. 48 ha previsto, con l'introduzione del “nuovo” art. 24-bis al D. Lgs. 231/2001, l'estensione della disciplina sanzionatoria a *tutti i reati informatici* (e, quindi, non solo a quelli previsti dalla novella del 2008). Rimane singolarmente escluso il delitto di frode informatica di cui all'art. 640-ter c.p. (là dove non

aggravato dalla commissione «*in danno dello Stato o di altro ente pubblico*») e soprattutto il “nuovo” art. 495-*bis* c.p., riguardante la falsa attestazione al certificatore di firma elettronica: ma se nel caso della frode informatica si può in un certo senso intravedere una *ratio* nell’esclusione della fattispecie dal novero dei reati “presupposto” (stante, forse, una concezione eminentemente “privatistica” del delitto in esame), nel caso invece della falsa attestazione di cui al “nuovo” art. 495-*bis* non appare invero comprensibile la scelta, atteso che questo reato ben potrebbe essere commesso nell’«interesse» o «vantaggio» di persone giuridiche (tanto da parte di soggetti in posizione apicale, come da parte di soggetti in posizione subordinata).

Prima dell’approvazione della L. 48/2008, in tema di criminalità «informatica», era prevista una responsabilità amministrativa dell’ente solo in caso di commissione del reato di frode informatica aggravata dalla commissione in danno dello Stato o altro ente pubblico di cui all’art. 640-*ter* c.p., come previsto dall’art. 24 D. Lgs. 231/2001 (rimasto inalterato) o di reati in materia di pedopornografia (art. 25-*quinqüies* D. Lgs. 231/2001).

Con la L. 48/2008 e l’introduzione dell’art. 24-*bis* il quadro è radicalmente mutato¹⁴: ora le persone giuridiche (a condizione che vi sia un «interesse» o «vantaggio» e che l’autore sia un soggetto «qualificato», ancorché non identificato o inimputabile: si veda il “microsistema” di cui agli artt. 5 – 8 D. Lgs. 231/2001) risponderanno con le

¹⁴ Art. 24-*bis* D. Lgs. 231/2001: «1. In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinqüies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinqüies* 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-*quinqüies* 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-*quinqüies* 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)».

sanzioni, pecuniarie e soprattutto *interdittive* (di cui all'art. 9, co. 2 lett. a,b,c,d,e¹⁵), anche per la commissione dei reati di falsità in documenti informatici (art. 491-*bis* c.p.), accesso abusivo e diffusione di programmi diretti a danneggiare un sistema informatico (da art. 615-*ter* ad art. 615-*quinquies* c.p.), intercettazione o interruzione illecita di comunicazioni informatiche o telematiche e relativa installazione di apparecchiature atti a commettere tali condotte (art. 617-*quater* ed art. 617-*quinquies* c.p.), tutte le nuove e pletoriche ipotesi di danneggiamento informatico a dati e programmi (da art. 635-*bis* ad art. 635-*quinquies* c.p.) ed infine frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.).

La inclusione dei reati informatici all'interno del catalogo dei "reati presupposto" di cui al D. Lgs. 231/2001 dà attuazione agli artt. 12 e 13, par. 2 della Convenzione di Budapest, nonché dall'art. 9 della Decisione quadro 2005/222/GAI. Si tratta, evidentemente, di un passaggio-chiave della riforma del 2008, anche perché i c.d. «*computer crimes*» rappresentano oggi una realtà in costante espansione, soprattutto nell'ottica della commissione da parte di enti o società.

Non è questa la sede per affrontare i criteri di imputazione del reato-base o presupposto di cui al D. Lgs. 231/2001 in capo alla persona giuridica, né certo per poter illustrare la delicata materia dei «*modelli di organizzazione dell'ente*» (art. 6 D. Lgs. 231/2001) necessari perché lo stesso possa andare esente da responsabilità «da reato».

¹⁵ Le ricordiamo per completezza:

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi.

Tuttavia, qui basti osservare come l'estensione della responsabilità ai reati informatici necessariamente inciderà (o, meglio, *dovrà* incidere) sulla predisposizione ed attuazione di nuovi ed ancor più complessi (e dispendiosi) «modelli organizzativi», parametrati sulla realtà molto più sfuggente ed aleatoria della criminalità tecnologica, legata per definizione ad un'evoluzione rapida e spesso – per la persona giuridica - imprevedibile (si pensi, ad es., alla delicata questione dei *virus* ed alla continua elaborazione di simili programmi informatici, frutto molto spesso di geniali *hacker* mossi da svariate ragioni, ideologiche, economiche, etc.).

A quest'ultimo riguardo si potrebbe pensare al caso del soggetto dipendente della società “ALFA” che, mosso da (più o meno folli...) ragioni di carattere ideologico, diffonde un *virus* nel sistema della società “BETA” (condotta pacificamente sussumibile sotto l'art. 615-*quinquies* c.p. ed espressamente richiamato dall'art. 24-*bis* D. Lgs. 231/2001). Poniamo poi che la società “ALFA” tragga pure un vantaggio dalla diffusione di un *virus* nel sistema informatico della società “BETA”, che – *per accidens* – è concorrente sul mercato di “ALFA”. Ebbene, se quest'ultima non dimostrerà di aver predisposto un corretto modello organizzativo potrà essere ritenuta responsabile *ex lege* 231/2001 del reato commesso dal suo sottoposto da cui è derivato (seppure non volontariamente o accidentalmente) un «vantaggio» per la stessa.

... e le misure cautelari ai danni dell'ente (art. 9 e artt. 45 - 54 D. Lgs. 231/2001). Cosa cambia dopo la riforma della L. 48/2008?

In senso stretto, con la L. 48/2008 nulla è cambiato in tema di misure cautelari applicabili alle persone giuridiche ai sensi degli artt. 45 – 54 D. Lgs. 231/2001, rimasti immutati.

Tuttavia, come appena evidenziato, il nuovo art. 24-*bis* ha previsto la responsabilità dell'ente anche in caso di commissione di reati «informatici», e quindi appare ora

quanto mai necessario interrogarsi sulla portata di una simile estensione in relazione all'applicazione delle misure cautelari.

Assai in breve, va ricordato che le misure cautelari, in virtù del rinvio all'art. 9 contenuto nell'art. 45 D. Lgs. 231/2001, non sono altro che le stesse sanzioni interdittive che possono essere applicate con la sentenza di condanna, ed in particolare (v. art. 9, co. 2 lett. a,b,c,d,e D. Lgs. 231/2001):

- a) l'interdizione dall'esercizio dell'attività;
- b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) il divieto di pubblicizzare beni o servizi.

Accanto quindi alla tipica funzione “cautelare” (sebbene necessariamente parametrata sulla natura di persona *giuridica* e non di persona *fisica*), ed alle relative esigenze, vi è anche – con maggior evidenza rispetto alle misure cautelari di cui all'art. 272 ss. c.p.p. – una funzione *anticipatoria* della futura condanna.

In generale, è agevole osservare come il D. Lgs. n. 231/2001 ha previsto una disciplina delle misure cautelari che, ancorché specifica, risulta comunque chiaramente modellata sull'omologo sistema del codice di rito (dal quale, peraltro, in base alla norma generale di chiusura di cui all'art. 34, risulta integrato, e non solo per le misure cautelari, nei limiti della «compatibilità»).

In particolare, l'art. 45, co. 1 (che prevede l'applicazione delle misure cautelari «quando sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi

illeciti della stessa indole di quello per cui si procede») condiziona l'applicazione della misura, al pari delle misure cautelari personali regolate dal codice di rito, all'esistenza del *fumus delicti*, inteso come qualificata probabilità della sussistenza dei presupposti della responsabilità amministrativa da reato dell'ente (da valutarsi con una prognosi articolata, riguardante sia gli estremi di uno dei reati, espressamente ritenuto idoneo dal decreto a fondare detta responsabilità, sia la sussistenza dell'interesse o del vantaggio dell'ente, sia anche la riferibilità del fatto ad uno dei livelli qualificati di organizzazione dell'ente di cui all'art. 5 dello stesso decreto; in questo senso, si veda Cass. pen., sez. II, 26 febbraio 2007, n. 10500), nonché del *periculum in mora*, quest'ultimo circoscritto alla sola esigenza "specialpreventiva", sulla falsariga dell'art. 274 c.p.p. lett. (c), essendo giustamente parso incongruo, con riferimento alla responsabilità degli enti, il richiamo al pericolo di inquinamento probatorio e di fuga di cui all'art. 274 c.p.p., lett. (a) e (b)¹⁶.

Inoltre, come anticipato, la medesima disposizione di cui all'art. 45 cit., individuando il "tipo" di misura cautelare nelle «sanzioni interdittive previste dall'art. 9, comma 2»,

¹⁶ Fra la relativamente copiosa giurisprudenza in tema di presupposti di applicazione delle misure cautelari agli enti ex lege 231/2001 si segnala la sentenza della sezione VI della S.C. del 23 giugno 2006, n. 32627, secondo la quale: «*In tema di misure cautelari interdittive applicabili all'ente per l'illecito dipendente da reato la valutazione circa la sussistenza dei gravi indizi deve essere riferita alla fattispecie complessa che integra l'illecito stesso. Pertanto l'ambito di valutazione del giudice deve comprendere non soltanto il fatto reato, cioè il primo presupposto dell'illecito amministrativo, ma estendersi ad accertare la sussistenza dell'interesse o del vantaggio derivante all'ente, il ruolo ricoperto dai soggetti indicati dall'art. 5, comma 1, lett. a) e b), D. Lgs. n. 231, nonché è necessario verificare se tali soggetti abbiano agito nell'interesse esclusivo proprio o di terzi. Nel giudizio cautelare rientrano anche le condizioni indicate nell'art. 13 D. Lgs. n. 231, che subordina l'applicabilità delle sanzioni interdittive alla circostanza che l'ente abbia tratto dal reato un profitto di rilevante entità ovvero, in alternativa, che l'ente abbia reiterato nel tempo gli illeciti. Infine, anche nella fase cautelare il giudice deve fondare la sua valutazione in rapporto ad uno dei due modelli di imputazione individuati negli artt. 6 e 7 D. Lgs. cit., l'uno riferito ai soggetti in posizione apicale, l'altro ai dipendenti, modelli che presuppongono un differente onere probatorio a carico dell'accusa. Pertanto, in ragione della peculiarità del giudizio di gravità indiziaria a carico dell'ente, non è legittimo il ricorso alla tecnica di motivazione del provvedimento per relationem, con semplice rinvio all'ordinanza cautelare personale, rinvio che può assolvere all'onere della motivazione solo per quanto concerne uno dei presupposti, quello cioè della sussistenza dei gravi indizi circa la commissione dei reati».*

rivela con immediatezza lo stretto collegamento esistente tra le cautele applicabili in via provvisoria e le sanzioni (o meglio talune delle sanzioni) da irrogarsi all'esito del giudizio. In altri termini le sanzioni interdittive, la cui applicazione può essere anticipata in via cautelare, sono le stesse irrogabili all'esito del giudizio di merito e, correlativamente a quanto accade per l'irrogazione della sanzione interdittiva con la sentenza di condanna, presuppongono la ricorrenza dei presupposti di cui all'art. 3 D. Lgs. 231/2001, e cioè: la gravità indiziaria della responsabilità dell'ente per uno dei reati «per i quali (dette sanzioni) sono espressamente previste», nonché almeno una delle condizioni previste dalla stessa norma (e, cioè, la reiterazione degli illeciti ovvero un profitto di rilevante entità, con l'aggiunta, se si tratta di reato commesso da sottoposti all'altrui direzione, dell'esistenza di gravi carenze organizzative).

Un altro collegamento fra misure cautelari e sanzioni (definitive) interdittive a carico della persona giuridica consiste nella durata delle stesse, atteso che – in virtù del rinvio contenuto dall'art. 51, co. 1 D. Lgs. 231/2001 – questa «*non può superare la metà del termine massimo indicato dall'art. 13, co. 2*», per cui la durata sarà compresa fra un mese e quindici giorni ed un anno.

A questo punto si può osservare una differenza fondamentale, almeno in linea di principio, fra le misure cautelari “personali” (di cui agli artt. 272 ss. c.p.p.) e le misure cautelari applicabili all'ente di cui al D. Lgs. 231/2001: nelle prime infatti, almeno in teoria, vi è un maggior accento sulla funzione, appunto, *cautelare*, pur residuando certamente importanti riflessi sulla futura (eventuale) espiazione della pena; nelle seconde, invece, vi è un accento più spiccatamente *sanzionatorio* (in virtù del richiamo all'art. 9, co. 2) ed *anticipatorio*, mentre le esigenze cautelari (che devono sussistere) paiono in un certo senso poste in secondo piano.

A quest'ultimo riguardo, è interessante riprendere una questione recentemente affrontata in una sentenza della Cassazione (sempre in via cautelare), nella quale la S.C. ha correttamente collegato la commissione del reato-presupposto e le relative sanzioni interdittive previste dal D. Lgs. 231/2001 all'applicazione della misura cautelare (interdittiva) della stessa specie: insomma, in altri termini, se si procede

contro una persona giuridica per un reato per il quale *non* è prevista una sanzione interdittiva (o non è prevista la sanzione interdittiva *di quella specie*), non si potrà nemmeno applicare *quella* misura *in via cautelare*.

Secondo la S.C., infatti, «... poiché gli artt. 24 ss. D. Lgs. 231/2001. non prevedono l'applicazione di sanzioni interdittive per tutti gli illeciti dell'ente ovvero prevedono l'applicazione solo di alcune delle misure interdittive previste dall'art. 9, comma 2 a seconda del tipo di reato cui si ricollega la responsabilità "amministrativa" dell'ente, è da escludere l'adozione, in via cautelare e anticipata, di sanzioni interdittive che non potranno essere applicate in via definitiva all'esito del giudizio di merito: ciò in coerenza con la funzione strumentale propria della misura cautelare e in applicazione del principio di adeguatezza, proporzionalità e gradualità sanciti dall'art. 46 del D. Lgs. In particolare è stato correttamente avvertito nei primi approdi giurisprudenziali in materia che la congiunzione "e", che nell'art. 46 cit., comma 2, collega i due parametri ("entità del fatto e della sanzione") rilevanti nell'apprezzamento della proporzionalità della cautela impone al Giudice, che applica la misura, di svolgere un giudizio prognostico circa la sanzione che ritiene potrà essere applicata all'ente all'esito del giudizio. Ciò significa che, per rispettare il principio di proporzionalità, il riferimento alla sanzione "finale" è imprescindibile, confermandosi, anche per tal verso, che non può essere applicata, in via provvisoria, una sanzione interdittiva la cui applicazione non è prevista, in sede di condanna, in relazione al tipo di illecito contestato» (Cass. pen., sez. II, 26 febbraio 2007, n. 10500).

Al riguardo, non va poi dimenticato il disposto dello stesso art. 46, co. 3 D. Lgs. 231/2001, secondo il quale «l'interdizione dall'esercizio dell'attività può essere disposta in via cautelare soltanto quando ogni altra misura risulti inadeguata». La norma, chiaramente, richiama l'art. 275 c.p.p. (ed in particolare il primo periodo del comma terzo: «La custodia cautelare in carcere può essere disposta soltanto quando ogni altra misura risulti inadeguata») ed è interessante notare come la più grave delle sanzioni interdittive per le persone giuridiche («interdizione dall'esercizio dell'attività», art. 9, co. 2 lett. a D. Lgs. 231/2001), e quindi – in virtù del richiamo

contenuto nell'art. 45 D. Lgs. 231/2001 – la più grave delle misure cautelari, sia strettamente (e testualmente...) posta in correlazione con la più grave delle misure cautelari personali, ovvero la privazione della libertà attraverso la custodia in carcere.

La S.C. ha osservato in proposito che «... *la norma (la quale ha il suo omologo nell'art. 275 c.p.p., comma 3) fissa un principio di gradualità, da attuarsi nell'ambito, e non già al di fuori, dei presupposti di applicazione delle misure cautelari. A ben guardare proprio perché l'interdizione dall'attività deve costituire l'extrema ratio, la sua adozione deve presupporre una prognosi positiva circa la possibilità di applicare con la sentenza di condanna la sanzione interdittiva più grave*» (Cass. pen., sez. II, 26 febbraio 2007, n. 10500).

Un'ultima osservazione in tema di misure cautelari riguarda l'art. 17 D. Lgs. 231/2001. Secondo questa norma, infatti, le sanzioni interdittive non si applicano «...*quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni*»:

- integrale risarcimento del danno ed eliminazione delle conseguenze dannose o pericolose del reato (o comunque efficace tentativo in tal senso);
- eliminazione da parte dell'ente delle carenze organizzative che hanno determinato il reato, mediante adozione di nuovi «modelli organizzativi» idonei a prevenire reati della specie di quello verificatosi;
- messa a disposizione del profitto da parte dell'ente ai fini della confisca.

Insomma, l'art. 17 cit. prevede una importante causa “atipica” di non punibilità sopravvenuta (*rectius*, di non applicabilità delle sanzioni interdittive all'ente), quale tipica espressione di meccanismo “premiale” per la persona giuridica che si sia “ravveduta”. Tuttavia, per espressa disposizione legislativa, la norma si applica solo in fase sanzionatoria (con la sentenza di condanna). In altri termini, nulla esclude che, in via *cautelare*, all'ente “indagato” possa essere applicata la stessa misura interdittiva che, al momento della condanna, non sarà più applicabile (poiché l'ente ha *medio tempore* soddisfatto le condizioni previste dall'art. 17 cit.).

L'incongruenza appare non di poco momento, vista la natura chiaramente *sanzionatoria* ed *anticipatoria* delle misure cautelari *ex lege* 231/2001: viene quindi da pensare che, in caso di applicazione in via cautelare della misura interdittiva, la persona giuridica sia quasi "scoraggiata" dal provvedere a risarcire, riparare o comunque ri-organizzarsi, secondo le previsioni dell'art. 17 cit., visto che – in ogni caso – l'ente avrà già *di fatto* subito la misura interdittiva.

In conclusione, va osservato che - per quanto riguarda il «*sequestro*» (sia esso «*preventivo*» o «*conservativo*»: v. artt. 53, 54 D. Lgs. 231/2001) - non paiono esservi particolari problemi applicativi, atteso il richiamo pedissequo alle disposizioni del codice di rito (art. 53) e la natura *reale* della misura in parola (ancorché, non lo si nega, molto spesso assai invasiva ed economicamente "afflittiva").

Osservazioni conclusive.

La legge 18 marzo 2008, n. 48 rappresenta sicuramente una riforma organica (ancorché spesso incoerente ed imperfetta) in materia di criminalità informatica. Le nuove norme sostanziali apportano modifiche incisive, così come quelle processuali, i cui potenziali effetti applicativi sono ancora difficili da prevedere.

Finalmente anche l'Italia dà piena (sebbene, non fedelissima...) attuazione alla Convenzione di Budapest del 2001 sul c.d. «*cybercrime*».

Al riguardo, uno dei passaggi più interessanti della riforma consiste nell'estensione (prevista dalla Convenzione stessa) della responsabilità «amministrativa da reato» degli enti anche alla commissione dei reati «informatici» (con un paio d'eccezioni, invero non molto comprensibili). Viene quindi certamente colmata una lacuna del nostro ordinamento che, pur prevedendo un'analitica disciplina sulla responsabilità "amministrativo-penale" delle persone giuridiche, escludeva ancora la previsione dei c.d. «*computer crimes*».



Ma, al di là degli aspetti positivi della riforma, va sottolineata l'estrema rapidità e, se vogliamo, spregiudicatezza con cui la stessa è stata approvata (con un *iter* parlamentare sostanzialmente durato otto giorni, a Camere peraltro ormai sciolte).

In proposito, leggendo le nuove disposizioni del codice penale resta il dubbio che si sia trattato, come al solito, di una riforma soltanto “simbolica”, con l'introduzione di ulteriori nuovi reati mal formulati ed ancor peggio collocati, di difficile verifica pratica o, al contrario, di rischiosa e dirompente applicazione.

L'estensione poi della responsabilità «amministrativa da reato» degli enti in relazione anche ai reati informatici comporterà inevitabilmente per gli stessi maggiori (ed ancora incerti) oneri in materia di «modelli organizzativi», e ciò sia nella prospettiva delle sanzioni in sede di condanna, sia – con maggior urgenza ed evidenza – nell'ottica di evitare l'applicazione *prodromica* ed *anticipatoria* delle misure cautelari, il cui sistema applicativo non è comunque stato toccato dalla riforma del 2008.

Avv. Beniamino Migliucci