SCiNTLEX
Diritto e Società dell'Informazione

CRIMINALITà INFORMATICA “SENZA FRONTIERE”: BUDAPEST–ROMA IN SOLI 6 ANNI!

Criminalità informatica senza frontiere:
Budapest - Roma in soli 6 anni!

Finalmente è stata ratificata la Convenzione del Consiglio d'Europa sulla criminalità informatica

A cura di Dr. Luigi Foglia
Consulente Legale ICT - Studio Legale Lisi

Finalmente, dopo soli 6 anni, il senato ha approvato il disegno legge S2012 (approvato anche dalla camera lo scorso 20 febbraio) con il quale si ratifica la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001.

La Convenzione di Budapest è stato il risultato di quattro anni di lavoro degli esperti del Consiglio d'Europa coadiuvati da vari interventi internazionali: in una materia senza frontiere come quella della criminalità informatica non poteva mancare il contributo anche di altre nazioni non facenti parte dell'Unione Europea (tra le altre Canada, Stati uniti e Giappone).

L'obiettivo enunciato chiaramente nel Preambolo della Convenzione, è quello di promuovere una politica comune, intesa a tutelare la società dai crimini informatici, attraverso l'armonizzazione delle procedure nazionali ed il potenziamento dell'assistenza giudiziaria in questi settori.

La Convenzione del Consiglio d'Europa sulla criminalità informatica

(Fonte: Camera dei Deputati - PdL C2807)

La Convenzione di Budapest sulla criminalità informatica è articolata in quattro capitoli (definizioni, misure da adottare a livello nazionale in tema di diritto sostanziale e processuale, cooperazione internazionale, clausole finali).

In particolare, la Convenzione prevede un certo numero di misure normative di diritto penale sostanziale che le parti devono adottare a livello nazionale, indicate negli articoli da 2 a 11.

Si tratta dell'accesso illegale, intenzionale e senza diritto, a tutto o a parte di un sistema informatico (articolo 2); delle intercettazioni illegali e cioè delle intercettazioni di dati informatici, intenzionali e illecite, effettuate, attraverso mezzi tecnici, durante trasmissioni non pubbliche (articolo 3); dell'attentato all'integrità dei dati (danneggiamento, cancellazione, deterioramento, alterazione e soppressione dei dati informatici) fatto intenzionalmente e senza autorizzazione (articolo 4); dell'attentato all'integrità dei sistemi, concretantesi in un impedimento grave al funzionamento di un sistema informatico, effettuato intenzionalmente e senza diritto mediante il danneggiamento, la cancellazione il deterioramento, l'alterazione e la soppressione dei dati informatici (articolo 5); dell'abuso intenzionale e senza autorizzazione di dispositivi (e cioè la produzione, la vendita, l'ottenimento per l'uso, l'importazione, la diffusione e altra forma di messa a disposizione), compresi i programmi informatici, specialmente concepiti per permettere la commissione dei delitti sopraccitati, nonchè di parole chiave (password) o di codici di accesso o di sistemi analoghi che consentano di accedere a tutto o a parte di un sistema informatico (articolo 6).

La Convenzione prevede, inoltre, all'articolo 7 la repressione delle falsificazioni informatiche, e cioè l'introduzione, l'alterazione, la cancellazione, la soppressione intenzionale e senza diritto di dati informatici non autentici con l'intenzione che essi siano usati ai fini legali come se fossero autentici.
È prevista anche la repressione della frode informatica, e cioè il fatto di causare intenzionalmente e senza diritto un pregiudizio patrimoniale ad altri (articolo 8).

Altra importante infrazione prevista dalla Convenzione è quella relativa alla produzione, intenzionale e illecita, mediante un sistema informatico, di materiale pornografico minorile, nonchè l'offerta o la messa a disposizione, la diffusione o la trasmissione ovvero il procacciamento per sè o altri o il possesso di siffatto materiale (articolo 9).

La Convenzione prevede, poi, l'infrazione legata agli attentati alla proprietà intellettuale e ai delitti commessi deliberatamente a livello commerciale mediante sistemi informatici (articolo 10).

Per tutti i tipi di reati sopraccitati, tranne quelli previsti dall'articolo 2, dall'articolo 6, dall'articolo 9, paragrafo 1, lettere b, d) ed e), è prevista anche la repressione del tentativo; infine sono previste la punibilità del concorso nel reato e la responsabilità (penale, civile o amministrativa) delle persone giuridiche, quando detti reati siano commessi da una persona fisica esercitante poteri direttivi nel loro ambito (articoli 11 e 12). Nella Convenzione è stabilito, inoltre, che le sanzioni da adottare da parte degli Stati devono essere effettive, proporzionate, dissuasive e comprendenti anche pene detentive (articolo 13).

La seconda parte della Convenzione (articoli da 16 a 22) contiene le misure procedurali che riguardano il perseguimento dei reati dianzi citati, cioè la comunicazione rapida dei dati immagazzinati, compresi quelli relativi al traffico, e la loro pubblicazione, l'ordine di esibizione, la perquisizione e il sequestro dei dati informatici, la raccolta dei dati di traffico in tempo reale, l'intercettazione del contenuto dei dati e infine le misure giurisdizionali.

La terza e quarta parte della Convenzione prevedono, infine, le norme di coordinamento in tema di cooperazione internazionale e le clausole finali. Il capitolo relativo alla cooperazione internazionale enunzia le disposizioni relative all'estradizione (articolo 24), all'assistenza giudiziaria (articolo 25), all'informazione spontanea (articolo 26), alla procedura relativa alla domanda di assistenza in assenza di accordi internazionali applicabili (articolo 27); regola inoltre la riservatezza delle informazioni e le restrizioni nella loro utilizzazione (articolo 28), l'assistenza in materia di misure provvisorie (articolo 29), la divulgazione rapida dei dati conservati (articolo 30), l'assistenza concernente l'accesso ai dati immagazzinati (articolo 31), l'accesso transfrontaliero ai dati immagazzinati con il consenso o accessibili al pubblico (articolo 32), l'assistenza nella raccolta dei dati relativi al traffico in tempo reale (articolo 33), l'assistenza in materia di intercettazione dei dati relativi al contenuto (articolo 34), l'istituzione di punti di contatto attivi ininterrottamente, costituenti la rete 24/7 (articolo 35).

Misure di diritto sostanziale

Preliminarmente, deve essere sottolineato come l'Italia sia stato uno dei primi Paesi europei ad introdurre una legge organica, la legge 23 dicembre 1993, n. 547, in tema di delitti informatici.

Successivamente a questa sono entrate in vigore altre leggi, relative a specifici settori, volte a reprimere i comportamenti illeciti di pirateria informatica (legge 18 agosto 2000, n. 248, che ha modificato le disposizioni in materia della legge 22 aprile 1941, n. 633, introdotte dal decreto legislativo 29 dicembre 1992, n. 518), a garantire la protezione dei dati personali (legge 31 dicembre 1996, n. 675, e successive modificazioni), a contrastare la detenzione, lo scambio e il commercio di materiale pedopornografico in rete (legge 3 agosto 1998, n. 269) e ad estendere ai fenomeni di pedopornografia virtuale l'ambito di applicazione delle norme incriminatici introdotte dalla legge n. 269 del 1998 (legge 6 febbraio 2006, n. 38).

Alla luce di ciò, la portata dell'adeguamento normativo realizzato, per l'esecuzione della Convenzione, nel settore del diritto penale sostanziale è risultata modesta, essendo, in molti casi, già in vigore una disciplina esaustiva, addirittura più incisiva di quella richiesta dalle disposizioni della Convenzione medesima.

Si è proceduto comunque all'integrazione o alla modifica di alcune disposizioni del codice penale, per considerazioni legate, da un lato, all'esigenza di una migliore collocazione sistematica, dall'altro, all'insorgere di nuove problematiche, che avevano determinato l'inadeguatezza delle originarie forme di tutela.

In quest'ottica deve essere valutata la decisione di modificare il testo dell'articolo 635-bis del codice penale, introducendo, contestualmente, gli artt. 635- ter, 635-quater e 635-quinqiuies, e modificare l'art. 420. Ciò risponde sia ad un'esigenza di simmetria rispetto alla sistematica della Convenzione, che distingue nettamente il danneggiamento dell'integrità dei dati dal danneggiamento dell'integrità del sistema e disciplina le due ipotesi in distinti articoli (4 e 5), sia all'opportunità di introdurre una disciplina penale differenziata a seconda che l'oggetto della tutela (informazioni, dati e programmi informatici) abbia, o meno, rilevanza a fini pubblicistici.

Nella stessa prospettiva è stato deciso di conservare, per i reati di falso, l'impostazione accolta dal legislatore del 1993 che, attraverso l'equiparazione del documento informatico agli atti pubblici e alle scritture private, aveva permesso di estendere le tradizionali ipotesi di reato ai casi in cui ne fosse oggetto un documento informatico.

Peraltro, in considerazione della sopravvenuta inadeguatezza della definizione di documento informatico, inteso come supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli, è stata accolta, anche ai fini penali, la più ampia e corretta nozione di documento informatico, già contenuta nel regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, abrogando il secondo periodo dell'articolo 491-bis del codice penale.

Per gli stessi motivi è stato introdotto anche l'articolo 495-bis del codice penale, volto a sanzionare penalmente chi renda al certificatore di firme elettroniche false dichiarazioni o attestazioni, concernenti l'identità o lo stato o altre qualità della propria o dell'altrui persona.

Il disegno di legge introduce inoltre una nuova figura di truffa (640-quinquies) che ha come soggetto attivo il certificatore di firma elettronica il quale, violando gli obblighi previsti all'articolo 32 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, procuri a sè o ad altri un ingiusto profitto con altrui danno. La disposizione è apparsa necessaria in quanto, sebbene l'articolo 640-ter del codice penale incrimini già la frode informatica, per la ricorrenza di questo specifico reato appaiono necessarie condotte di alterazione del funzionamento di un sistema informatico ovvero di intervento senza diritto su dati, informazioni o programmi, che potrebbero non ricorrere nel caso dell'attività di certificazione. Peraltro, la nuova incriminazione appare incentrata non solo sulla semplice violazione degli obblighi del certificatore qualificato e accreditato [già sanzionata civilmente dalla lettera d) del comma 1 dell'articolo 30 del citato codice dell'amministrazione digitale], ma anche sulla effettiva ricorrenza di un ingiusto profitto con altrui danno.

Altro elemento significativo è rappresentato dall'ampliamento, ai fini penali, della nozione di pornografia infantile e dalla ricomprensione, nell'ambito della stessa, del materiale pornografico che ritragga o rappresenti persone con sembianze di minori, come soggetti efebici o comunque di aspetto adolescenziale, nonchè realistiche immagini virtuali di minori. Secondo la Convenzione, infatti, devono essere penalmente sanzionati anche il possesso, la produzione, la distribuzione e la divulgazione di tali immagini, potendo queste, che pure non rappresentano soggetti reali o comunque minori di età, essere utilizzate per incitare a compiere o a partecipare ad attività vietate dalla legge.

Tale disposizione ha già trovato attuazione, peraltro, a seguito dell'introduzione nel nostro ordinamento dell'articolo 600-quater del codice penale, introdotto dall'articolo 4 della legge 6 febbraio 2006, n. 38.

Le modifiche interessanti l'articolo 615-quinquies del codice penale sono state motivate, invece, dall'esigenza di adeguare perfettamente alle disposizioni della Convenzione il dettato di tale norma. In particolare la norma risulta estesa sotto il profilo oggettivo mentre non è stata realizzata la riformulazione dell'elemento soggettivo mancando la richiesta del dolo specifico (la convenzione richiedeva il dolo specifico del profitto per se o altri).

Infine, l'introduzione dell'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231, risponde all'esigenza di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi. Ne deriva che, in forza di questa previsione, la sanzionabilità dei crimini informatici risulta sganciata dall'individuazione degli effettivi autori-persone fisiche: unica soluzione possibile, visto e considerato che l'astrattezza del cyber spazio e la particolare natura del mezzo impiegato non consentono di individuare con certezza i veri colpevoli.

Misure di diritto processuale

In relazione ai reati previsti dagli articoli da 2 a 11 e ad ogni altro reato commesso per mezzo di sistemi informatici, nonchè ai fini della raccolta di prove elettroniche in ordine a qualunque tipo di reato, la Convenzione richiede, sul piano procedurale, che ciascuna Parte aderente disponga all'interno del proprio ordinamento:

- di misure coattive per la conservazione rapida - per un periodo di tempo non superiore a novanta giorni, ma prorogabile, e in regime di segretezza - di specifici dati elettronici, compresi i dati relativi al traffico, immagazzinati per mezzo di un sistema informatico (articolo 16);

- di misure strumentali all'utile attuazione delle misure di cui al punto precedente (articolo 17);

- di misure coattive che consentano di acquisire la cognizione sia di specifici dati informatici, che siano in possesso o sotto il controllo di qualunque persona, immagazzinati in un sistema informatico o su un supporto informatico, sia di dati relativi agli abbonati, che siano in possesso o sotto il controllo di un fornitore di servizi, intendendosi per dati relativi agli abbonati ogni tipo di informazione, anche non in forma di dati informatici, riferita agli abbonati e diversa dai dati relativi al traffico o al contenuto, che permetta di accertare una serie di ulteriori dati (articolo 18);

- della possibilità di effettuare perquisizioni o comunque accessi nei confronti di sistemi e supporti informatici e di dati informatici, nonchè di estendere rapidamente la perquisizione o l'accesso ad altri sistemi informatici, qualora questi ultimi siano situati nel territorio nazionale e i dati in essi immagazzinati siano legalmente accessibili dai primi (articolo 19, paragrafi 1 e 2);

- della possibilità di sequestrare o comunque acquisire dati, supporti e sistemi informatici oggetto di perquisizione o accesso, con l'adozione delle connesse misure finalizzate ad assicurare la conservazione, la non alterazione e l'inaccessibilità dei dati informatici (articolo 19, paragrafo 3);

- di misure coattive per ottenere, dalle persone che ne dispongano, le informazioni necessarie ai fini delle perquisizioni e degli accessi di cui sopra (articolo 19, paragrafo 4);

- di misure che consentano la raccolta o la registrazione in tempo reale, in regime di segretezza, di dati relativi al traffico concernenti specifiche comunicazioni, effettuate attraverso un sistema informatico (articolo 20); l'applicazione di tali misure può anche essere limitata, attraverso una riserva, a taluni tipi di reati, indicati nella riserva medesima, purchè questi reati non risultino meno numerosi di quelli ai quali, ai sensi del diritto interno, sono applicabili le misure di cui al punto seguente (articolo 14);

- di misure che consentano, in relazione a gravi reati determinati da ciascuno Stato, la raccolta o la registrazione, in tempo reale e in regime di segretezza, di dati relativi al contenuto di specifiche comunicazioni effettuate attraverso un sistema informatico (articolo 21).

Si è operato, di conseguenza, su due piani convergenti:

1) integrazione di talune disposizioni del codice di procedura penale - che già disciplinano misure di indagine corrispondenti a quelle previste dalla Convenzione - attraverso riferimenti espliciti e specifici alle realtà informatiche e telematiche, al fine di adeguare la formulazione testuale delle norme processuali alle esigenze applicative in ambito

informatico;

2) inserimento ex novo di disposizioni procedurali che disciplinano misure richieste dalla Convenzione attualmente non presenti nell'ordinamento interno, con relativi istituti di garanzia; è il caso dell'articolo 9 del disegno di legge, che introduce i commi 4-ter, 4-quater e 4-quinquies dell'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, con cui si introduce, tra l'altro, nell'ordinamento italiano la conservazione in via di urgenza dei dati relativi al traffico telematico.

29/02/2008 **Dr. Luigi Foglia - Consulente Legale ICT**