CORATELLA
STUDIO LEGALE

L'impatto della Convenzione internazionale di Budapest sul D. Lgs. n. 231/2001: i cyber crimes

Avv. Manuela Mazzucco
Equity Partner Coratella – Studio Legale

Nello scorso anno l'elencazione dei reati presupposto della responsabilità amministrativa degli enti è stata nuovamente ampliata con l'introduzione dei reati informatici e del trattamento illecito di dati (art. 24 *bis* del decreto), dell'omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. *25 septies* del decreto) e della ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. *25 opties* del decreto).

I reati originariamente previsti nel decreto sono oramai numericamente inferiori rispetto a quelli di nuova introduzione che, con cadenza pressoché annuale, sono stati via via aggiunti al testo normativo di riferimento.

Nella mio breve intervento mi soffermerò sui reati informatici e sull'impatto che la loro introduzione nell'elencazione dei reati presupposto della responsabilità amministrativa degli enti ha sull'impresa.

La Convenzione di Budapest del 23 novembre 2001 o Convenzione sui crimini informatici (entrata in vigore il 1° luglio 2004) è stata il frutto del lavoro, di circa quattro anni, di un comitato di esperti nominato dal Consiglio d'Europa: è una Convenzione internazionale (tra i sottoscrittori non appartenenti al Consiglio d'Europa vi sono anche Stati Uniti, Canada e Giappone), anche perché molti di questi crimini permettono un passaggio "indolore" attraverso i confini e coinvolgono molto spesso sistemi informatici collocati in diversi punti geografici del mondo. Per tale ragione, l'obiettivo enunciato chiaramente nel Preambolo della Convenzione, è quello di promuovere una politica comune, intesa a tutelare la società dai crimini informatici, sempre più insidiosi e sempre più caratterizzati dalla transnazionalità, attraverso l'armonizzazione delle procedure nazionali ed il potenziamento dell'assistenza giudiziaria in questi settori. La Convenzione, pertanto, coinvolge gli Stati contraenti a più livelli, impegnandoli a modificare il proprio ordinamento interno per

armonizzare sia le fattispecie penalistiche sia gli strumenti investigativi ed a creare più snelle forme di cooperazione ed assistenza giudiziaria internazionale.

Tra le modifiche più significative, oltre a quelle di diritto penale sia sostanziale che processuale in materia di "reati informatici" e di "mezzi di ricerca della prova", l'"imposizione" a tutti gli Stati contraenti, fra cui l'Italia, di prevedere la responsabilità delle persone giuridiche in relazione a tutte le fattispecie di reato oggetto della Convenzione: di conseguenza, nel nostro Paese, l'imposto ampliamento della categoria dei reati presupposto della responsabilità amministrativa degli enti ex D.Lgs. n. 231/2001.

Ebbene, preme allora precisare che la definizione "dottrinaria" più diffusa di crimine informatico include tutte quelle tipologie di crimini in cui un **sistema di elaborazione** o **una sua parte** ricopre uno dei seguenti ruoli:
a) oggetto (ciò include la distruzione o la manipolazione dell'elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto);
b) strumento (quando ciò che avviene in relazione all'elaborazione non è di per sé illegale, ma serve a commettere crimini di altro tipo, es. sabotaggio). In pratica un sistema di elaborazione, o ciò che viene prodotto dall'elaboratore, è usato come mezzo per compiere frodi, sabotaggi, falsificazioni.

A livello europeo, in maniera più ampia, si ricomprendono nella nozione di "reato informatico" tutti i reati previsti dalla Convenzione internazionale di Budapest (artt. 2-11), "*tutti gli altri reati commessi attraverso un sistema informatico*" e tutti quelli in cui siano individuabili le "*prove elettroniche di un reato*".

La Convenzione, inoltre, impone definizioni comuni o quantomeno un'armonizzazione delle definizioni legali anche con riferimento alle nozioni di "sistema informatico", "dati informatici", "service provider", "trasmissione di dati", etc.

Ogni Stato sottoscrittore, dando esecuzione alla Convenzione, fa sì che, pur nella particolarità dei singoli ordinamenti, in ogni Stato si abbiano più o meno gli stessi tipi di reati informatici previsti e puniti anche negli altri paesi (e di sanzioni): ciò permetterà una maggiore chiarezza e una facilità nella realizzazione di cooperazione più Stati.

Con la Decisione quadro 2005/222/GAI del Consiglio dell'Unione Europea – che si pone come una naturale prosecuzione dell'azione di contrasto attuata a livello comunitario ancora con l'adozione delle Convenzione di Budapest sul Cybercrime – le 25 Nazioni aderenti all'Unione europea si vincolano ad armonizzare la propria normativa in materia penale introducendo, entro il 16 marzo 2007, delle leggi *ad hoc* in tema di sicurezza delle reti

e dei sistemi di informazione al fine di predisporre con urgenza un'adeguata tutela dagli attacchi contro i sistemi di informazione.

La Decisione quadro prevede una responsabilità penale a carico delle imprese, riferita a "*qualsiasi entità che abbia tale qualifica* [n.d.a. di persona giuridica] *ai sensi della legislazione applicabile, eccetto gli Stati o altri organismi pubblici nell'esercizio dell'autorità statale e le organizzazioni internazionali.*".

Ebbene, in Italia, la Convenzione di Budapest viene ratificata con la Legge n. 48/2008, anche se – è bene dirlo – nel nostro Paese la repressione di tali reati è perseguita già dal 1993 (Legge 23 dicembre 1993, n. 547): da un lato, si ha dunque solo un restyling del complesso di fattispecie e altre prescrizioni introdotte nel codice penale quindici anni orsono, ma, dall'altro, si rinuncia ad attuare la proposta – avanzata, ad esempio, dal Progetto Nordio – di disciplinare i vari reati informatici all'interno di un'unica sezione codicistica, con una propria organicità e caratterizzazione specifica (verrà difatti confermata la scelta della tecnica novellistica e non adottata la creazione di un titolo autonomo nel codice penale).

La novità effettiva e rilevante, dunque, è che anche nel nostro Paese tali reati possono divenire il presupposto giuridico per l'incriminazione dell'ente. La normativa italiana vigente sino all'entrata in vigore della legge n. 48/2008, infatti, ancorava la responsabilità da reato degli enti solo taluni delitti c.d. informatici e, segnatamente:
- art. 24, frode informatica commessa a danno dello Stato o di altro ente pubblico;
- art. 25 *quater*, assistenza a gruppi terroristici mediante fornitura di strumenti di comunicazione;
- art. 25 *quinquies*, lett.c), divulgazione, cessione o detenzione di materiale pedopornografico.

La novella comunitaria, invece, "copre" tutti i casi di "attacchi informatici": l'art. 7 della Legge n. 48/2008 introduce l'art. 24 bis del D. Lgs. n. 231/2001 (Delitti informatici e trattamento illecito di dati), con risposta sanzionatoria graduata in funzione della gravità dei reati.

A tali sanzioni si aggiunge la circostanza che, a livello europeo, si è imposta una modernizzazione delle procedure investigative, soprattutto della Polizia Giudiziaria, ed un rafforzamento dei poteri di indagine e di cooperazione internazionale (cooperazione indispensabile data la difficile individuazione, per questi reati, non solo del tempus ma anche del locus commissi delicti).

La legge di ratifica, pertanto, recependo le indicazioni della Convenzione modifica alcuni degli articoli del codice di procedura penale relativi a Indagini preliminari - Attività della Polizia Giudiziaria - Mezzi di ricerca della prova, modernizzando la disciplina in materia di:
- ispezioni;
- perquisizioni (viene estesa alle perquisizioni in ambito informatico la possibilità per la polizia giudiziaria di procedere ugualmente all'acquisizione delle prove violando le misure di sicurezza qualora essa non sia in possesso delle password);
- sequestri (sequestri presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni delle lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza è consentito "*anche se inoltrati per via telematica*");
- intercettazioni di conversazioni o comunicazioni.

I doveri di esibizione riguardano ora anche "*i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*".

Il pesante intervento sulle tecniche di indagine utilizzate dalle forze di polizia è una delle novità più importanti della legge: le modifiche apportate al codice di procedura penale impongono alla polizia giudiziaria di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Queste modifiche pongono fine a un dibattito che da anni si trascinava nelle aule di giustizia e che vedeva contrapposto chi – tipicamente, le forze di polizia – riteneva di poter sequestrare e analizzare computer senza adottare particolari cautele tecniche a chi – gli avvocati – chiedeva il rispetto dei principi fissati dalla computer forensics (la disciplina che studia il modo di eseguire le "autopsie informatiche"): per la prima volta nel nostro ordinamento si esplicita la necessità che la acquisizione di dati digitali avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro non modificabilità.

Infine, risulta di estrema importanza la disposizione normativa la quale prevede che le indagini in materia di reati informatici e di pedo-pornografia debbano essere affidate agli uffici del pubblico ministero presso il tribunale del capoluogo del distretto di corte d'appello; una novità che rende auspicabile la creazione di appositi "pool" di magistrati inquirenti specializzati. In fase di indagine, infatti, spesso l'individuazione del responsabile del fatto illecito e l'acquisizione delle prove richiede *attività complesse* di frequente orientate verso Stati esteri, e tutte urgenti in relazione alla volatilità del cyberspazio, per le quali è necessaria una specializzazione ad hoc.
.
Opportunamente, pertanto, la Convenzione ha previsto un corposo rafforzamento delle procedure di cooperazione internazionale, e non solo. La cooperazione, infatti, dovrà

avvenire a vari livelli: per un verso, *tra gli Stati*, nelle tradizionali forme della cooperazione giudiziaria e di polizia; per altro verso, ed è un dato particolarmente significativo, è sollecitata la cooperazione *tra pubblico e privato*, *fra Stato e industria privata* (ad esempio, i detentori di dati informatici, ivi inclusi i service providers, che possono cooperare con le pubbliche autorità procedendo alla collazione o memorizzazione in real-time di «dati di traffico» o di «contenuti» associati a determinate comunicazioni generate con sistema computerizzato, congelando, in sostanza i c.d. data evidence al fine di preservarli efficacemente).

Cosa comporta l'estensione della responsabilità amministrativa delle persone giuridiche come prevista dal decreto legislativo 231/01 ai reati informatici? Quali rischi per l'impresa?
Ricordiamo che in base all'art. 5 del D. Lgs, 231/2001 l'ente (fornito di personalità giuridica o anche le società e associazioni anche prive di personalità giuridica) è responsabile per i reati commessi nel suo interesse o a suo vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa o anche da persone sottoposte alla loro direzione o vigilanza,qualora uno dei soggetti dinanzi citati, omettendo la sorveglianza od il controllo dovuti, abbia reso possibile la commissione, a beneficio dell'azienda, dei reati su menzionati da parte di persona soggetta alla sua autorità.

Inoltre, la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato o non è imputabile.

Perché l'introduzione dei reati informatici nel novero dei c.d. reati presupposto dovrebbe destare maggiore allarme per le imprese e convincerle a dotarsi di adeguate procedure di controllo e di un efficace modello organizzativo?

Lo si comprende agevolmente, se si considera che se si escludono le tipologie di reati adattabili solo alle imprese del tutto fuori legge (è il caso dei reati di terrorismo, di violenza sessuale e di mutilazione degli organi genitali femminili, ma anche di gran parte dei reati di falso nummario e delle ipotesi di riciclaggio), oggi qualunque ente è esposto al rischio di un incriminazione ai sensi della 231/2001, poiché ogni impresa è oramai organizzata a livello informatico e telematico.

Se i reati contro la P.A. sembrano definire, ovviamente, le c.d. aree a rischio delle sole aziende che intrattengono rapporti contrattuali con le Amministrazioni pubbliche; l'abuso di informazioni privilegiate concerne le società quotate; l'omicidio (ma non le lesioni connesse a violazioni della normativa antinfortunistica) coinvolgono soprattutto le imprese

produttive e non quelle operanti nell'ambito dei soli servizi, pressoché tutti gli enti di cui al D. Lgs. n. 231/2001 possono, invece, essere interessati dai reati informatici.

Tali reati, inoltre, rispetto agli altri reati del catalogo del decreto, possono essere commessi da chiunque e non esistono delle aree o funzioni maggiormente a rischio, il che comporta la necessità di una vigilanza quanto mai difficile dovendo, in teoria, essere estesa a tutti i dipendenti.

Tra l'altro, tali reati, nella maggior parte dei casi, sono strumentali al raggiungimento di uno scopo ulteriore, per cui risulta difficile individuarli fino a quando non si realizzi la finalità ultima.

In considerazione di tali peculiarità, parte della dottrina ha criticato l'inserimento di tali reati nell'ambito di applicazione del decreto, sostenendo che:
- essi non sono riconducibili alla tipica attività di impresa;
- spesso sono commessi non tanto a vantaggio dell'ente quanto piuttosto a suo danno;
- risulta alquanto complicato sottoporli ad un efficace controllo.

Tale responsabilità ha invero una sua ragion d'essere atteso che numerosi sono i casi in cui l'attacco ad un sistema informatico può essere realizzato per arrecare un vantaggio ad un ente (pensiamo alle ipotesi di spionaggio o sabotaggio industriale).

É anche vero, però, che con riferimento a taluni reati, quali quelli di pedo-pornografia, è obiettivamente difficile immaginare un qualsivoglia interesse o vantaggio dell'ente. Eppure, i procedimenti penali occasionati dalla detenzione, in server aziendali, di materiale di natura pedopornografica, ad esempio, hanno oggi giorno un'incidenza che può considerarsi degna di attenzione.

Quel che è più grave, è che, come già evidenziato, le aziende potranno venire chiamate a rispondere ai sensi dell'art. 8 della Decisione Quadro anche nel caso di autore del reato non identificato, come già avviene in forza dell'art. 8 D.L.vo n. 231/01.

E le sanzioni sono pesantissime.

Come possono difendersi le imprese: quali sono le metodologie che i responsabili aziendali devono mettere in atto per tutelarsi?

L'ente non risponde dei reati informatici compiuti attraverso l'utilizzo dei propri sistemi informatici se prova:

– di avere adottato e attuato efficacemente modelli di gestione idonei a prevenire il reato;
– di avere affidato ad un organismo dotato di autonomi poteri d'iniziativa e di controllo, la vigilanza e l'aggiornamento di tali modelli;
– che la commissione del reato è dipesa dall'elusione fraudolenta di tali modelli di organizzazione e gestione.

In ogni caso, ad evitare censure penali – anche solo per aver omesso il doveroso controllo su coloro che, in qualche misura subordinati, hanno consapevolmente posto in essere atti d'illegittimo accesso ai sistemi o d'indebita interferenza agli stessi od ai dati informatici ivi contenuti, poi riverberatisi a beneficio dell'ente stesso – occorre che ci si ponga in un'ottica di scrupoloso rispetto della sicurezza e della legalità.

In poche parole, che le aziende dovranno predisporre preventive ed idonee misure di sicurezza e di controllo per prevenire che al loro interno si commettano reati informatici. Un valido modello organizzativo e gestionale e l'adozione di sicure procedure in materia di sicurezza possono costituire un valido ausilio, forse l'unico baluardo invocabile in un processo di tale specie. Ciò che andrà incessantemente svolta, inoltre, è una lecita attività di direzione e di vigilanza, puntuale e penetrante sì da rendere l'azienda scevra dall'odiosa responsabilità di carattere omissivo voluta dal legislatore comunitario.