DIRITTO PENALE CONTEMPORANEO

LA NUOVA TUTELA PENALE EUROPEA DEI SISTEMI DI INFORMAZIONE

Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio

di Silvio Civello Conigliaro

SOMMARIO: 1. Introduzione. – 2. L'accesso abusivo ai sistemi di informazione. – 3. L'interferenza illecita. – 4. Intercettazione illecita, fabbricazione di *malware* e diffusione di *password*. – 5. Cause di non punibilità e circostanze aggravanti. – 6. Altre disposizioni.

1. Introduzione.

Il 3 settembre scorso è entrata in vigore la direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI. Tale strumento è stato adottato per perseguire il ravvicinamento del diritto penale degli Stati membri[1], oltre all'obiettivo, già fatto proprio dalla decisione quadro, di favorire la cooperazione tra le autorità giudiziarie e di polizia nel contrasto alla criminalità informatica. Quella informatica è, infatti, una delle «sfere di criminalità particolarmente grave» rispetto alle quali l'Unione, a norma dell'articolo 83 §1 del TFUE, ha facoltà di intervenire anche se l'intervento non sia indispensabile per l'efficace attuazione di una politica comune e a prescindere dal grado di armonizzazione delle legislazioni nazionali nel settore interessato.

Il provvedimento si fonda sulla considerazione che il buon funzionamento e la sicurezza dei sistemi di informazione siano fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa[2]; e tuttavia si può supporre che non sia stata la sola rilevanza degli interessi tutelati ad aver determinato questa priorità di intervento. Un certo ruolo nell'adozione della terza direttiva[3] di armonizzazione delle legislazioni penali sostanziali sotto il nuovo Trattato ha senz'altro giocato, infatti, la

[1] Cfr. il considerando 1 e l'articolo 1 della direttiva, che espressamente parlano di armonizzazione dei reati e delle sanzioni.

[2] Cfr. considerando 2.

[3] Lo strumento qui esaminato segue alla direttiva 2011/36 concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, alla direttiva 2011/92 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori.

Editore Luca Santa Maria | Direttore Responsabile Francesco Viganò (cc) BY-NC-ND 2010-2013 Diritto Penale Contemporaneo

preesistenza di una Convenzione del Consiglio d'Europa in materia[4]. Così, come già accaduto nel caso dello sfruttamento sessuale dei minori[5], anche questa volta il recepimento della normativa dell'Unione non costerà troppo fatica agli Stati membri.

Anche l'Italia, dotatasi già nel 1993 di una legge organica per la protezione dei sistemi informatici[6], ha recepito la Convenzione di Budapest con L. 18 marzo 2008, n. 48, apportando modifiche ai titoli XII e XIII del libro II del codice penale, nonché al decreto legislativo 8 giugno 2001, n. 231, e ciò ridimensiona decisamente il valore aggiunto della direttiva.

Quello che da circa vent'anni ci si è abituati a chiamare "diritto penale dell'informatica"[7] non subirà, sostanzialmente, grandi cambiamenti, se non una ridefinizione, in certi casi, del quadro sanzionatorio. Minime sono anche le differenze riscontrabili tra la direttiva e la sostituita decisione quadro. Tra queste paiono degne di nota, in particolare, l'obbligo per gli Stati di incriminare la condotta di intercettazione illecita di comunicazioni informatiche o telematiche[8], e la previsione della reclusione non inferiore nel massimo a due anni per le condotte di «fabbricazione, vendita, approvvigionamento per l'uso, importazione e distribuzione o messa a disposizione in altro modo» di *software* destinati o modificati principalmente al fine di commettere uno dei reati previsti dalla direttiva nonché di «*password* e codici d'accesso che permettono di accedere in tutto o in parte a un sistema di informazione» per la commissione degli stessi reati[9]. Sull'impatto che queste previsioni comportano sulla normativa interna si tornerà d'appresso (*infra* § 4).

---

[4] Il riferimento è alla Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001.

[5] Rispetto alla quale esisteva già la Convenzione del Consiglio d'Europa per la protezione dei bambini contro lo sfruttamento e gli abusi sessuali, fatta a Lanzarote il 25 gennaio 2007.

[6] Legge 23 dicembre 1993, n. 547.

[7] In realtà, la pur comoda espressione qui utilizzata, proveniente dal linguaggio adoperato dalle fonti sovranazionali, può risultare fuorviante. Sotto tale etichetta si raggrupperebbero, infatti, sia condotte lesive di interessi penalmente rilevanti realizzate tramite supporto informatico, sia condotte lesive di sistemi informatici, nonché fattispecie più tradizionali che possono oggi essere realizzate, eventualmente, anche mediante l'uso di sistemi informatici, i c.d. reati informatici in senso lato (così anche FLOR R., *Lotta alla criminalità informatica e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di* internet, in *questa Rivista*, 20 settembre 2012; contempla tale "tripartizione" anche BRENNER S., *Defining cyber crime: A review of federal and state law*, in R.D. CLIFFORD (Ed.), *Cybercrime*, Carolina Academic Press, 2001, 15-104, 17; sul punto vedi *amplius* L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 4, 2011, 827 e ss. Se anche la attuale collocazione dei vari "crimini informatici" (nelle diverse accezioni) in diverse parti del codice si giustificherebbe per la pluralità dei beni giuridici tutelati, non manca chi sostiene l'opportunità di un *corpus* di norme a tutela dell'unico bene della sicurezza informatica (cfr. CERQUA [a cura di], *I reati informatici*, Cedam, 2010, p. 10 ss.).

[8] Così stabilisce l'articolo 6 della direttiva.

[9] V., sul punto, l'articolo 7 della direttiva, rubricato «*Strumenti utilizzati per commettere i reati*».

2. L'accesso abusivo ai sistemi di informazione.

La prima condotta contemplata dalla direttiva è quella di accesso abusivo ad un sistema di informazione che, in base all'articolo 3, andrebbe punito solo quando effettuato in violazione di una misura di sicurezza, condizione prima non richiesta dalla decisione quadro né dalla Convenzione di Budapest. Tuttavia, questa scelta di limitare la punibilità alle condotte più ostinate e aggressive non impedisce agli Stati di adottare un più alto *standard* di protezione dei sistemi informatici, considerando abusivo anche l'accesso che non violi alcuna misura di sicurezza.

L'attuale formulazione dell'articolo 615 *ter* c.p. richiede la violazione di una misura di sicurezza, e stabilisce come pena per l'intruso informatico la reclusione fino a tre anni, un anno di più, quindi, rispetto a quanto richiesto dall'articolo 9 della direttiva. Sul punto, la giurisprudenza ha precisato che è sufficiente ad integrare la fattispecie la violazione di qualsiasi misura di protezione, anche bassa, come ad esempio una *password*; il reato si perfeziona, cioè, quando siano violate le condizioni impartite dal gestore del sistema, a prescindere dagli scopi e dalle finalità perseguite dall'autore della condotta[10].

Una volta superato l'ostacolo che presiede all'accesso del sistema, non rileverebbe neanche l'incapacità di disporre dei dati e dei programmi contenuti nel *computer* violato[11]. Può concludersi, quindi, che l'abusività della condotta andrà verificata al momento dell'accesso, indipendentemente dall'eventuale uso successivo dei dati acquisiti[12]; per questa ragione l'accesso per finalità illecite di chi, però, abbia titolo, non configurerebbe il reato di cui all'articolo 615 *ter*, e l'autore risponderebbe solo degli eventuali altri reati che grazie all'accesso gli sia stato possibile commettere[13].

Tuttavia, posto che l'articolo 615 *ter* punisce non solo l'accesso al sistema, ma anche il mantenimento in esso contro la volontà espressa o tacita di chi abbia diritto di escluderlo, si è considerato reato anche il comportamento del soggetto autorizzato all'accesso che si trattenga nel sistema per finalità estranee[14].

3. L'interferenza illecita.

Nessuna novità si registra in ordine alla definizione di interferenza illecita, che gli articoli 4 (relativamente ai sistemi informatici) e 5 (relativamente ai dati informatici)

---

[10] Cass. sez. un., 27 ottobre 2011, n. 4694, Casani, in *Foro It.*, 2012, II, 374, n. di DI PAOLA; per ulteriori approfondimenti sulla pronuncia si vedano anche le note di commento di BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. Pen. cont. – Riv. Trim.*, 1/12, p. 123 e FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Dir. Pen. cont. – Riv. Trim.*, 2/12, p. 126.

[11] Trib. Bologna, 22 dicembre 2005, in *Giur. merito*, 2006, 1224, n. di RABAZZI.

[12] Cass., sez. V, 25 giugno 2009, n. 40078, Genchi, in *Giur. it.*, 2010, 1155.

[13] Cfr. Cass., sez. V, 29 maggio 2008, n. 26707, Scimia, in *Foro it.*, II, 2009, 487; nello stesso senso Cass., Sez. VI, 8 ottobre 2008, n. 39290, Peparaio, in *Cass. pen.*, 2009, 2828.

[14] Cass. Pen., sez. V, 10 dicembre 2009, in ced. Cass., *Rv.* 245842 (m).

della direttiva riprendono fedelmente dalla decisione quadro, anche nel limitarsi a chiederne la punibilità per i soli casi gravi. Entrambe le condotte risultano già contemplate dal nostro codice penale, rispettivamente all'articolo 635 *quater*, che fissa la pena nella reclusione da uno a cinque anni, e dall'articolo 635 *bis*, che commina la più lieve sanzione della reclusione da sei mesi a tre anni, con pieno soddisfacimento, in entrambi i casi, delle richieste europee.

La distinzione tra l'interferenza (o il danneggiamento, secondo la nomenclatura adottata dal nostro legislatore) relativa ai sistemi e quella relativa ai dati, nella normativa europea come in quella interna, è legata alle conseguenze che la condotta assuma, ovvero a seconda che l'interferenza sui dati ostacoli o meno il funzionamento del sistema[15]. Il reato di danneggiamento di dati informatici di cui all'articolo 635 *bis*, peraltro, si configura anche qualora i dati cancellati siano recuperabili grazie all'intervento di un tecnico specializzato[16], in linea con la distinzione concettuale, operata dall'articolo 5 della direttiva, tra cancellazione e soppressione degli stessi.

L'articolo 4 della direttiva precisa che va punito l'atto intenzionale che ostacoli gravemente il funzionamento di un sistema o ne causi l'interruzione. Mentre l'articolo 420 co. 3° c.p., abrogato nel 2008, puniva espressamente «l'interruzione, anche parziale» del funzionamento dell'impianto, il vigente articolo 635 *quinquies*, allora contestualmente inserito per dare esecuzione alla Convenzione di Budapest, sottopone a pena solo chi «distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento», e ciò fa sorgere legittimi dubbi ermeneutici sulla possibilità di far rientrare il concetto di "interruzione" in quello di "grave ostacolamento" o di "parziale inservibilità": ove ciò non fosse possibile, il legislatore dovrebbe intervenire per reintrodurre la punibilità della condotta di interruzione.

4. Intercettazione illecita, fabbricazione di *malware* e diffusione *password*.

Come già accennato, l'introduzione delle fattispecie di cui agli articoli 6 e 7 della direttiva rappresentano le principali novità che il nuovo strumento comporta rispetto alla decisione quadro, anche se non si può certo considerarle rivoluzionarie, quanto meno rispetto al panorama italiano. Infatti, per quanto riguarda la condotta di intercettazione illecita, l'articolo 617 *quater*, 1°co. del codice penale prevede già la reclusione da sei mesi a quattro anni. L'articolo 615 *quinquies* c.p., invece, prevede la reclusione fino a due anni e la multa per la detenzione o diffusione di *malware* allo scopo di danneggiare sistemi informatici, dati o informazioni, nonché di «altre apparecchiature o dispositivi» da utilizzare per il medesimo fine[17].

---

[15] V. sul punto *I nuovi reati informatici,* a cura di DEMARCHI, Giappichelli, 2009, p.34.

[16] In questo senso, Cass., sez. V, 18 novembre 2011, n. 8555, S., in *Foro it.*, Rep., 2012, voce *Danneggiamento*, n.2.

[17] Va precisato che mentre inizialmente era punita la sola diffusione, già con la legge di ratifica della Convenzione di Budapest è divenuta punibile anche la mera detenzione.

Per quanto riguarda, poi, la detenzione e diffusione abusiva di *password* o altri codici di accesso, l'articolo 615 *quater* c.p. stabilisce la reclusione fino a un massimo di un anno e la multa, a fronte del massimo edittale di due anni di reclusione previsto dalla direttiva. Nonostante la tendenziale maggiore afflittività del cumulo di pena detentiva e pena pecuniaria previsto dall'attuale fattispecie codicistica, il legislatore italiano è comunque chiamato ad intervenire sul punto innalzando il massimo edittale di pena detentiva per rispondere alle aspettative della direttiva; e non si tratta dell'unico intervento richiesto sul punto. Per la configurazione del reato di cui all'articolo 615 *quater*, infatti, è attualmente altresì richiesto il dolo specifico di trarre profitto o arrecare danno[18], ma la permanenza di tale elemento ostacolerebbe il pieno soddisfacimento degli obblighi derivanti dalla direttiva sul punto, restringendo l'ambito di punibilità più di quanto permesso dagli obblighi di tutela penale derivanti dall'art. 83 TFUE. Né si potrebbe altrimenti ritenere la previsione del dolo specifico come manifestazione di quel filtro, espressamente ammesso dall'articolo 7 della direttiva, che consente la punibilità dei soli casi gravi, espressione che sembra fare eco, piuttosto, alla scelta operata in molti ordinamenti europei di non considerare punibili (o addirittura "tipici") i casi in cui la condotta non raggiunga una certa soglia di offensività del bene protetto[19].

Nessun intervento di recepimento è invece necessario relativamente alla creazione e diffusione di strumenti idonei all'attacco informatico, condotte rispetto alle quali, invece, il dolo specifico del danneggiamento di un sistema è previsto sia dal codice che dalla direttiva. Questa, sul punto, fa un generico riferimento agli "strumenti" utilizzabili per commettere i reati da essa previsti, ma solo per tenere conto delle varie modalità con cui possono essere effettuati gli attacchi a causa della continua evoluzione degli *hardware* e dei *software*. Pertanto, si richiede la verifica dell'intenzione di impiegarli al fine di commettere uno dei reati elencati proprio per evitare di criminalizzare la mera detenzione di strumenti solo potenzialmente idonei all'attacco informatico, laddove siano prodotti e commercializzati per scopi legittimi, come la verifica dell'affidabilità dei prodotti di tecnologia dell'informazione o la sicurezza dei sistemi di informazione.

5. Cause di non punibilità e circostanze aggravanti.

Il legislatore europeo ha previsto alcuni casi in cui gli Stati sono dispensati dall'incriminare le condotte da essa previste. Si tratta, anzitutto, dei cosiddetti casi di "minore gravità"; di questi viene fornita qualche esemplificazione, sostanzialmente riconducibile a figure tradizionali di condotta non punibile perché inoffensiva o di *periculum in abstracto*.

[18]Cfr. Trib. Milano, 28 settembre 2007, in *Foro ambrosiano*, 2007, 325.
[19] V. considerando 11.

Il considerando 17 precisa, inoltre, che non è sufficiente che "siano soddisfatti i criteri oggettivi dei reati previsti nella presente direttiva", ed elenca come cause di non colpevolezza il caso in cui l'autore non sappia che l'accesso non è autorizzato o quello di incarichi di collaudo o di protezione di sistemi di informazione (c.d. "*white hat" hacking*). Si prevede poi che "per gli obblighi e gli accordi contrattuali intesi a limitare l'accesso ai sistemi di informazione tramite norme d'uso o condizioni del servizio, nonché per controversie lavorative riguardo all'accesso e all'uso di sistemi di informazione del datore di lavoro per scopi privati, non dovrebbe essere prevista responsabilità penale, quando l'accesso in tali circostanze sia ritenuto non autorizzato e, pertanto, costituisca l'unico presupposto per l'esercizio dell'azione penale." Più genericamente, la decisione quadro disponeva di escludere la penalizzazione delle condotte effettuate da aventi diritto e persone autorizzate.

Per quanto riguarda le circostanze aggravanti, mentre la decisione quadro prevedeva una pena detentiva compresa nel massimo tra due e cinque anni qualora l'accesso abusivo o l'interferenza illecita fossero commesse nel quadro di un'organizzazione criminale o avessero causato gravi danni o colpito interessi essenziali, l'art. 9 § 3 della direttiva stabilisce la pena detentiva di almeno tre anni nel massimo, per la sola interferenza illecita, quando ci si sia avvalsi degli strumenti elencati all'articolo 7, colpendo un numero significativo di sistemi di informazione.

L'art. 9 § 4, invece, impone agli Stati di stabilire una pena detentiva non inferiore nel massimo a cinque anni in tre diverse circostanze relative alla condotta di interferenza illecita, ciascuna delle quali dovrebbe implicare.

La prima di queste è la realizzazione della condotta nell'ambito di un'organizzazione criminale, e ciò richiede un intervento del nostro Parlamento in quanto un tale aumento di pena non è attualmente contemplato nel nostro ordinamento se non limitatamente alle organizzazioni di stampo mafioso, a norma dell'art. 7 l. 13 maggio 1991 n. 152[20]. Ma, a ben vedere, anche se l'organizzazione nell'ambito della quale sia commesso il reato soddisfacesse i requisiti dell'articolo 416 *bis*, l'unica condotta punita in maniera adeguata agli *standard* europei sarebbe il danneggiamento dei sistemi informatici, in base al combinato disposto dell'articolo 635 *quater* c.p. (o 635 *quinquies* c.p. qualora il sistema sia di pubblica utilità) con il citato articolo 7, che permetterebbe di comminare fino a sette anni e mezzo di reclusione[21].

Relativamente al danneggiamento dei dati, invece, la normativa italiana vigente, soddisfa gli obblighi europei solo nel caso di dati relativi a sistemi di pubblica utilità; in tutti gli altri casi il giudice non potrà, anche avvalendosi dell'aumento della pena fino alla metà previsto dal decreto legge, infliggere una pena detentiva superiore a quattro anni e mezzo. Sul punto sarà dunque necessario novellare il codice.

La seconda aggravante, contemplata dall'articolo 9 §4 lett. *b* per le condotte di interferenza illecita, riguarda il caso in cui esse causino "gravi danni". Nonostante la

[20] Convertito in legge 12 luglio 1991, n. 203.

[21] Per un caso di reato informatico nel quadro di un'organizzazione criminale, v. Cass. Sez. V, 16 aprile 2004, Aiello, in *Foro. it.*, 2004, II, 667.

genericità della formulazione, anche in questo caso, deve ritenersi necessario un interevento sull'art. 635 *bis*, non potendosi considerare che l'aggravante comune di cui all'articolo 61 n. 7 codice penale, limitata però al danno patrimoniale o all'interesse di lucro, soddisfi le richieste di tutela penale formulate dall'Europa. E ciò potrebbe richiedere un conseguente intervento sull'art. 635 *quater*, che già prevede un massimo edittale di cinque anni di reclusione, in un ottica di graduazione delle pene e coerenza del sistema sanzionatorio.

Ulteriori problemi solleva la lettera *c)* dell'articolo 9 §4, che prevede un aumento di pena per le condotte che abbiano interessato infrastrutture critiche.

Sebbene si tratti di formulazione piuttosto generica, e non suffragata neanche di alcuna elencazione esemplificativa, in tale categoria possono certamente farsi rientrare i sistemi di pubblici e di pubblica utilità, che ci rimandano agli articoli 635 *ter* e 635 *quinquies* del codice. Quest'ultimo considera le interferenze illecite che interessano impianti di pubblica utilità come fattispecie autonome, che si distinguono da quelle di danneggiamento di dati e sistemi "comuni" anche nella struttura dell'illecito, presentandosi non come reati di evento, ma come un delitto di attentato. Nel caso di impianti pubblici, quindi, verrà punita anche la condotta che non causi un danno effettivo, sebbene con una pena troppo mite rispetto a quanto richiesto dalla nuova direttiva. Ma, a ben vedere, il mero aumento di pena per il caso di mancata verificazione dell'evento da quattro a cinque anni rispetterebbe il dettato della direttiva solo parzialmente, in quanto non darebbe adeguatamente conto della *ratio* della stessa, ovvero la maggiore gravità di un danno provocato a sistemi di pubblico interesse. In un'ottica di coerenza del sistema sanzionatorio, quindi, sarà necessario, alternativamente, un aumento a cinque anni per la indicata condotta di attentato (ed uno maggiore per il caso di verificazione dell'evento dannoso), oppure una riduzione delle pene attualmente previste dagli articoli 635 *bis* e 635 *quater* per le interferenze relative ai sistemi "comuni".

Sorprendentemente, invece, la direttiva non fa alcun riferimento al terrorismo, a differenza della decisione quadro che addirittura qualificava il reato informatico come tipico reato-mezzo delle organizzazioni terroristiche. Essa stabilisce, però, che nel punire la commissione di reati informatici dovrebbe considerarsi circostanza aggravante l'abuso di dati di terzi (c.d. furto di identità) quando ciò non rappresenti già una condotta autonomamente punibile nella normativa nazionale, ma senza per ciò stabilire alcuna pena[22]. La resistenza manifestata da alcuni Stati nel corso dei negoziati in Consiglio, ha impedito infatti di raggiungere una posizione comune sulla criminalizzazione del c.d. furto di identità come condotta autonoma. L'intenzione della Commissione di procedere in tal senso emerge però con chiarezza dal considerando 14.

Il considerando 18 afferma poi la necessità di tenere conto del fatto che la perpetrazione dell'attacco informatico sia stata agevolata dalla facilità di accesso al sistema a causa della propria attività lavorativa; tuttavia non si ritiene per ciò necessario un aumento di pena, quanto che tale circostanza sia tenuta in

[22] Cfr. art. 9 §5 della direttiva.

considerazione nel procedimento. Il codice penale, invece, prevede pene più severe per tutti i reati informatici quando siano commessi con abuso della qualifica di operatore del sistema. L'accesso con abuso di qualità, o quello commesso dal pubblico ufficiale, è stato considerato, in alcune pronunce della S.C., come fattispecie autonoma rispetto al reato base di cui al primo comma dell'articolo 615 *ter*[23]. Le sezioni unite hanno però recentemente statuito in senso contrario, considerandolo circostanza aggravante[24], applicabile anche al dipendente dell'unità in cui sia installato il sistema che disponga di conoscenze superiori, indispensabili per accedere al sistema stesso[25]. Rilevante in tal senso non sarà «l'astratta qualificazione professionale dell'agente, quanto piuttosto il collegamento funzionale con il sistema»[26].

6. Altre disposizioni.

L'articolo 8 della direttiva prevede, come di consueto, la punibilità dell'istigazione, del favoreggiamento e del concorso per tutte le condotte contemplate, richiedendo l'adozione di non meglio specificate sanzioni efficaci, proporzionate e dissuasive. La punibilità del tentativo, invece, è richiesta solo per l'interferenza illecita, e ciò impone nuovi provvedimenti al legislatore italiano, che, come si diceva, ha fin qui scelto di tutelare in modo differenziato i dati e i sistemi a seconda che siano o meno di pubblica utilità. Nel primo caso, poiché il danneggiamento è costruito come una fattispecie di attentato, il tentativo, pacificamente, non può considerarsi ammissibile. E, tuttavia, tale soluzione non viola gli obblighi scaturenti dalla direttiva in quanto la fattispecie di pericolo costruita dal nostro legislatore attribuisce comunque rilevanza penale agli "atti idonei diretti in modo non equivoco" all'interferenza illecita relativa agli impianti di pubblica utilità e fornisce una risposta sanzionatoria adeguata alle richieste europee sul punto. Nessun problema, invece, si pone (né si poneva) per la punibilità del tentativo negli altri casi di interferenza illecita.

Identiche a quelle della vecchia decisione quadro sono poi le previsioni relative alla responsabilità delle persone giuridiche, che rispondono dei reati informatici commessi a loro vantaggio. L'art. 24 *bis* introdotto nel 2008 al decreto legislativo 8 giugno 2001, n. 231, recependo una norma che prevede la punibilità delle condotte commesse "per conto" dell'impresa, include tanto quelle commesse nell'interesse dell'ente quanto quelle commesse nell'interesse (anche esclusivo) di altri, che però abbiano procurato vantaggio all'ente medesimo. Non sarà dunque necessario, sul punto, alcun adeguamento. La normativa italiana prevede anche, in armonia con la direttiva, sanzioni pecuniarie calcolate per numero di quote e importo delle medesime, oltre a diverse sanzioni interdittive, alcune previste solo per la diffusione di

[23] Così Cass. Pen., sez. V, 18 gennaio 2011, n. 24583, Soc. Tosinvest, in *Foro it.*, parte II, p. 375, con n. DI PAOLA, e Cass., sez. V, 30 settembre 2008, n. 1727, Romano, in *Riv. pen.*, 2009, 467.
[24] Cass., Sez. un., 27 ottobre 2011, n. 4694.
[25] Così GIP T. Brindisi, 25 febbraio 1999,in *Corti Bari, Lecce, Potenza*, 2001, II, 4.
[26] Così AMATO G., Danneggiamento perseguibile a querela, in *Guida al diritto*, 2008, 16, p. 60.

programmi o codici di accesso, ed altre per tutti gli altri reati. Tra queste non compare solo la chiusura temporanea o permanente degli stabilimenti usati per commettere l'illecito, unica nuova sanzione contemplata dalla direttiva e, tuttavia, solo proposta, in quanto l'obbligo degli Stati in fatto di responsabilità degli enti è solo di prevedere sanzioni efficaci, proporzionate e dissuasive (quindi anche non penali) e la suddetta sanzione interdittiva, insieme a tutte le altre, compare solo in un elenco esemplificativo di sanzioni accessorie facoltativamente applicabili insieme alla sanzione pecuniaria, l'unica espressamente richiesta dalla direttiva.