

---

GIOVANNI LUCA PERDONÒ

---

## LE RESPONSABILITÀ PENALI COLLEGATE ALL'USO DI *INTERNET* FRA COMPARAZIONE E PROSPETTIVE DI RIFORMA

---

**SOMMARIO:** 1. Internet: rischi ed opportunità. — 2. La dimensione normativa internazionale: *a)* il quadro dell'Unione europea; *b)* lo scenario comunitario in senso stretto; *c)* gli ultimi sviluppi della normativa internazionale in materia di criminalità informatica: dalla Convenzione del Consiglio d'Europa sulla cybercriminalità alla decisione quadro 2005/222/GAI relativa agli attacchi contro i sistemi di informazione. — 3. Brevi note di comparazione con l'ordinamento americano: *a)* premesse generali; *b)* il modello americano di ascrizione della responsabilità degli *Internet Service Providers*. — 4. Brevi riflessioni sulla normativa nazionale di recepimento della direttiva 2000/31 CE. — 5. Spunti di riforma in relazione alle altre direttive. — 6. Conclusioni.

---

### 1. INTERNET: RISCHI ED OPPORTUNITÀ.

---

La crescente diffusione delle tecnologie dell'informazione, ed in particolare di *Internet*, ha reso il settore delle comunicazioni e dei collegamenti telematici sempre più importante, in termini non soltanto di estensione quantitativa delle relazioni sociali e commerciali che si svolgono con tali mezzi, ma anche qualitativa, per la rilevanza sociale che esse assumono nello sviluppo della società contemporanea; conseguentemente, dal punto di vista della politica criminale, lo sviluppo delle stesse determina l'emersione di nuovi beni meritevoli di tutela o di nuove forme di aggressione nei confronti di beni tradizionali.

In via preliminare, non è esagerato affermare che il *Web* ha stravolto la nostra vita: ogni informazione può arrivare attraverso *Internet* e, ormai, è possibile fare mille operazioni comuni usando la rete. L'effetto dirompente della diffusione delle nuove tecnologie è di tale portata che ha favorito la nascita di una vera e propria « mitologia » legata al mondo di *Internet*, in virtù della quale l'enfaticizzazione della sua centralità nella vita moderna ha generato l'illusione che il *Web* rappresenti una ricchezza in sé. Una dimostrazione di quanto detto è offerta da quel fenomeno che, solo qualche anno fa, ha dapprima visto crescere la bolla dei c.d. titoli *high tech* e, successivamente, crollare i loro valori di Borsa, in tal modo contribuendo a diffondere la consapevolezza che il *software* non è altro che un sistema di organizzazione dell'azienda, un moltiplicatore di efficienza, ma non costituisce una ricchezza in sé, proprio perché non può prescindere dall'andamento dell'economia reale.

Pertanto, premessa la natura esclusivamente strumentale di *Internet*, deve ritenersi quest'ultimo un moltiplicatore di opportunità, ma anche

di minacce. In altri termini, la rete è un moltiplicatore non solo di economia, ma anche di criminalità, al punto da poter diventare un veicolo per la pedofilia, oppure da fungere da supporto al terrorismo di matrice islamica; dunque, la tecnologia informatica, depurata dall'enfasi iniziale, si presenta in tutte le sue contraddizioni, che poi sono quelle della stessa modernità: non a caso si è giunti a parlare di *digital divide*, riferendosi alla rete come fattore fondamentale di divisione, appunto, fra gli esseri umani, fra coloro che trovano accesso al sistema, e sono i privilegiati, e coloro che ne sono perennemente esclusi<sup>1</sup>. Molteplici sono i campi in cui il fenomeno tecnologico, con la sua generalizzazione — o se si preferisce, la sua «democratizzazione» —, può rappresentare un formidabile fattore di sviluppo: si pensi a quella concezione dei rapporti tra Stato e cittadino identificata con la c.d. *democrazia elettronica*, volendosi con ciò alludere a nuove forme di partecipazione popolare, non solo nella fase della elezione dei rappresentanti, ma anche in quella in cui questi prendono le decisioni<sup>2</sup>, oppure a quell'aspetto, già attuale, che si manifesta attraverso l'intensificarsi della trasparenza amministrativa o l'informatizzazione delle relazioni tra P.A. e utenti<sup>3</sup>; senonché, a fronte delle potenzialità accennate, nuove e tradizionali minacce si affacciano.

Infatti, da una parte, significativo è il ruolo che le nuove tecnologie dell'informazione possono assumere nella piena maturazione del rapporto di cittadinanza<sup>4</sup>; dall'altra, è evidente la più ampia diffusione dei pericoli di lesione della *privacy*, per non dire del rischio di degenerazioni in senso autoritario degli attuali regimi democratici ovvero degli effetti destabilizzanti che possono derivare rispettivamente dall'acquisito controllo da parte dei poteri pubblici<sup>5</sup>, ovvero di privati<sup>6</sup>, delle informazioni riguar-

<sup>1</sup> V. G. AMATO, *Un altro mondo è possibile? Parole per capire e per cambiare*, Milano, 2006, 71; ZENO-ZENCOVICH, *Il «diritto ad essere informati» quale elemento del rapporto di cittadinanza*, in questa *Rivista*, 2006, 8.

<sup>2</sup> Cfr., per tale spunto, MORALES GARCIA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 125 s.

<sup>3</sup> È di recentissima emanazione il «Codice dell'amministrazione digitale», approvato con il d.lgs. 7 marzo 2005, n. 82 ed entrato in vigore il 1° gennaio 2006, che si propone, tra l'altro, di diffondere l'uso delle nuove tecnologie tra cittadini e P.A., come indicato dalla Relazione governativa al Codice, in *Guida dir.*, 2005, n. 8, 44 ss.

<sup>4</sup> ZENO-ZENCOVICH, *Il «diritto ad essere informati» quale elemento del rapporto di cittadinanza*, in questa *Rivista*, 2006, 7 ss., il quale, dopo aver sottolineato il ruolo essenziale che l'informazione svolge nel qualificare il rapporto di cittadinanza, evi-

denzia come tale processo si rifletta non solo sugli obblighi comunicativi (anche in termini di informazione giuridica) dello Stato e delle istituzioni sopranazionali, ma anche sul rapporto tra formazione ed informazione, nel senso che le pubbliche autorità hanno il compito, nella prospettiva indicata, di promuovere la c.d. «alfabetizzazione informatica».

<sup>5</sup> Si pensi alle critiche rivolte al sistema dei controlli e delle restrizioni delle garanzie costituzionali introdotti, negli USA, con l'esperienza del *Patriot Act*, su cui cfr. BILLÉ, «*Patriottismo*» costituzionale e libertà d'informazione: il caso statunitense, in questa *Rivista*, 2006, 124 ss.

<sup>6</sup> Si pensi al d.l. 22 settembre 2006, n. 259, convertito, con modificazioni, dalla l. 20 novembre 2006, n. 281, il quale prevede, in corrispondenza dell'art. 3, il delitto di illegale detenzione di documenti, supporti e atti concernenti i dati e contenuti di conversazioni e comunicazioni relativi al traffico telefonico e telematico illegalmente formati o acquisiti; come opportunamente rilevato, l'intervento normativo, nato sull'onda dell'emergenza del caso Telecom, si pone a tutela di un interesse diffu-

danti la riservatezza dei cittadini; sul versante, invece, del commercio elettronico e della documentazione amministrativa, le opportunità previamente indicate si accompagnano al rischio per la sicurezza degli operatori, sia in ordine alle interferenze illecite nelle transazioni, sia in ordine alla identificabilità degli interlocutori e alla documentazione delle operazioni, cui si collegano nuove forme di aggressione a beni tradizionali, quale, ad esempio, quello della fede pubblica.

Ciò premesso, il carattere transfrontaliero del fenomeno ed il rischio di sfruttamento illecito delle potenzialità messe a disposizione dalla rete impongono l'esigenza di predisporre norme il più possibile omogenee, che si traducano in una strategia coordinata ed estesa su scala sovranazionale<sup>7</sup>.

A dire il vero, il quadro delle iniziative internazionali finalizzate al contrasto dei fenomeni criminosi collegati ad *Internet* si presenta alquanto articolato, e ciò sia per l'ambito degli ordinamenti interessati, sia per quanto concerne gli strumenti impiegati ed i relativi effetti sui sistemi giuridici.

Così, a parte testi ormai di interesse poco più che storico, come la Raccomandazione N° R (89) 9, datata 13 settembre 1989, « *sur la criminalità en relation avec l'ordinateur* » e la Risoluzione finale, del settembre del 1994, adottata in coincidenza del XV Congresso dell'*Association internationale de droit pénal*<sup>8</sup>, muovendo dal livello europeo, vengono in considerazione le misure adottate nell'ambito del diritto comunitario in senso stretto (c.d. primo pilastro), del diritto dell'Unione in materia di cooperazione di polizia e giudiziaria (c.d. terzo pilastro) e, infine, del Consiglio d'Europa.

## 2. LA DIMENSIONE NORMATIVA INTERNAZIONALE: A) IL QUADRO DELL'UNIONE EUROPEA.

Quanto al livello europeo, l'avvento della cooperazione intergovernativa e del terzo pilastro del Trattato sull'Unione Europea ha determinato, nell'ambito della materia identificata con la Giustizia e gli affari interni, un intensificarsi degli interventi dell'UE: in particolare, il Consiglio dell'UE ha adottato, il 28 novembre 1996, una risoluzione per contrastare le informazioni di contenuto illegale e nocivo su *Internet*. Il Gruppo di lavoro per la tutela delle persone con riguardo alla tutela dei dati personali, con la Raccomandazione 3/1999 del 7 settembre 1999, ha affrontato il tema della conservazione, da parte dei fornitori dei servizi *Internet* e per fini giudiziari, dei dati relativi alle comunicazioni<sup>9</sup>.

so sovra-individuale e finanche politico-istituzionale, messo a repentaglio dalla circolazione ed accumulo di notizie illecite, capace di produrre gravi alterazioni e distorsioni delle condizioni di vita sociale, anche a prescindere dalla lesione alla riservatezza delle singole persone: PALAZZO, *Tolleranza zero per le intercettazioni illecite?*, in *Dir. pen. proc.*, 2006, 1326.

<sup>7</sup> Cfr. MILITELLO, *Iniziative sovranazionali di lotta alla criminalità organizza-*

*ta ed al riciclaggio nell'ambito delle nuove tecnologie*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, cit., 95 ss.

<sup>8</sup> Per una ricostruzione di tali testi, cfr. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, 7-11.

<sup>9</sup> Cfr. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004, 179 ss., ed *ivi* 190.

Inoltre, merita considerazione anche il « Piano d'azione contro la criminalità organizzata », dapprima adottato dal Consiglio « Giustizia ed Affari interni » del 28 aprile 1997, quindi approvato dal Consiglio dell'UE, tenutosi ad Amsterdam nel giugno del 1997; l'articolato documento mette in guardia dal rischio che la criminalità organizzata sfrutti a proprio vantaggio le nuove tecnologie. Nella riunione straordinaria del Consiglio del 1999 a Tampère (FL), appositamente dedicata all'obiettivo della creazione di uno spazio di « libertà, sicurezza e giustizia », si menziona anche la « criminalità ad alta tecnologia ». Sempre il Consiglio europeo, inoltre, durante il vertice di Feira (PT) nel giugno 2000, ha approvato un piano d'azione in materia informatica « eEurope », che prevede l'adozione di una strategia coordinata e coerente per fronteggiare la criminalità informatica<sup>10</sup>.

In una risoluzione del 1997<sup>11</sup>, il Parlamento Europeo sottolinea la necessità di fare chiarezza sulle « possibilità di riciclaggio dei proventi illeciti tramite Internet », sull'impiego di tecniche per filtrare i « contenuti penalmente rilevanti ed indesiderati su Internet », sulle « frodi nelle transazioni commerciali elettroniche e sul pericolo di un sistematico spionaggio economico ».

La caratteristica comune di tutti i documenti fin qui esaminati può sintetizzarsi nell'attribuzione di un valore poco più che politico agli stessi, i quali, in quanto privi di efficacia vincolante, non potevano sottrarsi alla critica secondo cui la materia avrebbe richiesto interventi normativi puntuali nella direzione di una disciplina omogenea e non limitata entro i confini nazionali.

Nella direzione testé accennata, pertanto, è da valutare con favore l'intervento del Consiglio dell'Unione europea, che, con la decisione quadro datata 24 aprile 2005, n. 2005/222/Gai in materia di attacchi contro i sistemi di informazione, ha provveduto a porre le basi per l'armonizzazione, in ambito europeo, della disciplina giuridica della materia in esame.

Ciò vale a maggior ragione se si ritiene che, di fronte all'alternativa tra « regionalismo » e « globalizzazione » nella scelta della dimensione di intervento più adeguata, il piano delle iniziative europee sia preferibile, dal punto di vista della praticabilità e degli strumenti messi a disposizione, tanto all'approccio meramente bilaterale (dei trattati internazionali), quanto a quello tendenzialmente globale (vedi la Convenzione ONU sul crimine organizzato transnazionale del dicembre 2000)<sup>12</sup>.

#### B) LO SCENARIO COMUNITARIO IN SENSO STRETTO.

L'analisi degli interventi normativi emersi in ambito europeo si muove all'interno di determinate coordinate; invero, il quadro a disposizione esprime una costante tensione dialettica tra libertà e sicurezza, o, in altri termini, tra libertà e controllo. A questo punto, sarà interessante ricono-

<sup>10</sup> Cfr. MILITELLO, *Iniziative sovranazionali di lotta alla criminalità organizzata ed al riciclaggio nell'ambito delle nuove tecnologie*, cit., 103 s.

<sup>11</sup> Risoluzione del Parlamento Europeo, doc. A4 0333/97, approvata il 27-28

ottobre 1997, in relazione al « Piano d'azione contro la criminalità organizzata ».

<sup>12</sup> Cfr. MILITELLO, *Iniziative sovranazionali di lotta alla criminalità organizzata ed al riciclaggio nell'ambito delle nuove tecnologie*, cit., 108 ss.

scere tali linee di fondo anche coordinando i diversi provvedimenti e mettendone in luce eventuali contraddizioni e sfasature. Inoltre, sarà necessario valutare l'opportunità di privilegiare, soprattutto in ambito europeo, alcune fonti ad altre, e ciò per la loro diversa intensità vincolante; infine, giudicare i singoli provvedimenti dal punto di vista della capacità di incidere in modo adeguato sulla materia affrontata.

Con riferimento alla dialettica su accennata, l'analisi degli interventi emersi a livello comunitario, come, in tema di responsabilità degli intermediari di servizi telematici, la direttiva 2000/31, sul commercio elettronico, recepita dalla legge comunitaria del 2001 (l. 39/2002) e dal d.lgs. 70/2003, e la direttiva 2002/58, relativa alla vita privata e alle comunicazioni elettroniche, pone in risalto, in prima battuta, la tensione verso le istanze garantiste.

Infatti, con la prima direttiva, il Parlamento europeo ed il Consiglio, nella Sezione IV sulla responsabilità dei prestatori (coloro che, secondo l'art. 2, lett. b) della direttiva, prestano un servizio della società dell'informazione), hanno stabilito alcuni principi fondamentali, fra cui la regola generale secondo cui il *provider* risponde se ha deliberatamente collaborato alla commissione di un reato e quella, ricavabile dall'art. 15, comma I, che impedisce agli Stati membri di imporre ai medesimi prestatori un dovere generale sia di controllo sulle informazioni che essi trasmettono (o anche solo memorizzano), sia di ricerca attiva della presenza di materiali illeciti<sup>13</sup>.

Così, premessa la distinzione fra il semplice trasporto delle informazioni, altrimenti detto *mere conduit*, cui la normativa equipara la fornitura di accesso alla rete, la memorizzazione temporanea, detta *caching* e la memorizzazione prolungata (*hosting*), con riferimento al trasporto e alla concessione di accesso alla rete, l'art. 12 prevede l'esclusione della responsabilità del *provider* che non ha dato origine alla trasmissione, non ha selezionato il destinatario della comunicazione e non ha modificato le informazioni trasmesse, ovverossia che non è intervenuto sul contenuto del materiale illecito; per l'attività di memorizzazione temporanea, oltre ai requisiti indicati per il *mere conduit*, l'art. 13, comma I, lett. e), prevede che il *provider* debba rimuovere le informazioni memorizzate o disabilitarne l'accesso qualora sia effettivamente venuto a conoscenza che l'autorità amministrativa o giudiziaria competente ne ha disposto la rimozione, oppure che l'accesso all'informazione è già stato disabilitato. Infine, per quanto riguarda l'attività di *hosting*, nella quale il *provider* consente la memorizzazione sul proprio *server* di informazioni fornite da un destinatario del suo servizio (per esempio, immissione in rete di un sito predisposto da un suo cliente), l'art. 15 della direttiva prevede che l'intermediario, ai fini dell'esclusione della responsabilità, non sia al corrente della illiceità

<sup>13</sup> Sul punto cfr. PETRINI, *La responsabilità penale per i reati via internet*, cit., 191, il quale sottolinea come la direttiva, in ossequio al principio di effettività, escluda qualsiasi obbligo impossibile e controproducente, oltre che inutile; tale regola è ovviamente ripresa dal legislatore nazionale che, con la l. 39/2001 e col d.lgs. 70/2003, esclude la configurabilità di una posizione

di garanzia in capo al *provider* e, di conseguenza, di qualsiasi ipotesi di responsabilità omissiva impropria a suo carico per il mancato impedimento di un reato attraverso le sue strutture di rete. Sui profili civilistici della responsabilità del *provider*, cfr. SICA, *Le responsabilità civili*, in *Commercio elettronico e servizi della società dell'informazione*, a cura di Tosi, Milano, 2003, 267 ss.

dei materiali e che si attivi per rimuoverli solo non appena ne sia a conoscenza. A titolo di specificazione del primo dei due requisiti, si dispone che, per quanto attiene alle azioni risarcitorie, all'effettiva conoscenza venga equiparata la percezione di fatti o circostanze che rendono manifesta l'illegalità dell'attività<sup>14</sup>; la soluzione, nell'ottica della sola responsabilità civile, non pone problemi di rilievo; diversamente dovrebbe ritenersi nel caso in cui il legislatore nazionale opti per la previsione di una fattispecie penale, a meno di non includervi una responsabilità di tipo colposo.

Sul versante delle responsabilità, agli Stati membri è riconosciuta la possibilità di introdurre l'obbligo per il *provider* di impedire o porre fine ad una violazione a richiesta dell'autorità amministrativa o giurisdizionale, nonché di comunicare alle autorità competenti, a seguito di loro richiesta, l'identificazione degli utenti che hanno concluso accordi di memorizzazione dei dati.

Sulla scia delle indicazioni contenute nella Raccomandazione 3/1999 in materia di conservazione dei dati del traffico per i *providers* di *Internet*, la direttiva 2000/31/CE, in definitiva, nell'escludere un obbligo di conservazione del traffico, sembra privilegiare l'esigenza di tutela della *privacy*, anche se, come si legge nei *consideranda*, la motivazione profonda di una scelta così attenta ai diritti fondamentali della persona si giustifica principalmente nell'ottica, tutta economicistica, della necessità di garantire lo sviluppo del commercio elettronico, che sarebbe seriamente minacciato se gli operatori dovessero adattare le proprie infrastrutture per la conservazione di copia di tutto il traffico di dati circolante attraverso i propri *servers*, ben oltre il tempo strettamente necessario per elaborare i dati della fatturazione<sup>15</sup>.

Alla medesima *ratio* si ispira la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa alla vita privata e alle comunicazioni elettroniche, nella parte in cui prevede espressamente una serie di accorgimenti per evitare che dalla divulgazione dei dati transitati e conservati nelle strutture di rete possa derivare un pregiudizio alla riservatezza degli utenti, tra i quali il divieto di memorizzare i dati relativi alle comunicazioni (art. 5) e l'obbligo di cancellare o di rendere anonimi i dati relativi al traffico di comunicazioni (art. 6).

L'art. 15, di contro, prevede alcune eccezioni alle dianzi citate disposizioni, dal momento che agli Stati membri è riservata la possibilità di adottare misure legislative per garantire la conservazione dei dati, quando ciò sia necessario, opportuno e proporzionato per la prevenzione, la ricerca, l'accertamento ed il perseguimento dei reati.

Di tale ultima opzione si è avvalso il legislatore nazionale, con la l. 31 luglio 2005, n. 155 di conversione del d.l. 27 luglio 2005, n. 144, recante « Misure urgenti per il contrasto del terrorismo internazionale ». Infatti, in deroga alla norma generale prevista dall'art. 123 d.lgs. 196/2003 (codice della *privacy*), che prevede, per i dati relativi a qualsiasi forma di traffico

<sup>14</sup> Si pensi al caso in cui, soprattutto nell'ambito dell'*e-commerce*, il *provider* non possa non rendersi conto che un sito è intitolato con un nome identico al marchio di un notissimo prodotto commerciale, in palese violazione della disciplina dei do-

maine names, dei marchi e della concorrenza.

<sup>15</sup> MORALES GARCIA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime*, cit., 134.

(telefonia e comunicazioni elettroniche), la cancellazione o l'anonimato quando il loro trattamento non è più necessario, cioè con il completamento della trasmissione della comunicazione, l'art 6 del provvedimento di contrasto alla criminalità terroristica, nel risolvere il conflitto tra le esigenze della *privacy* e quelle della sicurezza pubblica, introduce, a carico del fornitore, l'obbligo di conservazione del traffico telematico, ad esclusione dei soli contenuti delle comunicazioni, per finalità di accertamento e repressione dei reati, e ciò per un tempo di sei mesi, prorogabili di altri sei per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407 comma 2 lett. a c.p.p., nonché dei delitti in danno dei sistemi informatici o telematici<sup>16</sup>.

La tendenza all'accentuazione delle esigenze di sicurezza si perfeziona con la direttiva del 15 marzo 2006, 2006/24/CE<sup>17</sup>, riguardante la conservazione dei dati generati e trattati nell'ambito della fornitura dei servizi accessibili al pubblico di comunicazione elettronica e di reti pubbliche di comunicazione, che modifica la direttiva 2002/58 CE.

L'obiettivo del potenziamento dell'azione di contrasto del terrorismo si è imposto a partire dalla strage di Madrid del marzo 2004, tanto che nel Piano d'azione contro il terrorismo della Commissione si pianificava, tra l'altro, una proposta di decisione-quadro concernente proprio la conservazione dei dati delle telecomunicazioni. Durante la presidenza inglese dell'Unione europea e dopo l'attentato di Londra del luglio 2005 è stata presentata una proposta di direttiva della Commissione<sup>18</sup>, successivamente approvata con emendamenti dal Parlamento europeo in data 14 dicembre 2005 e definitivamente dal Consiglio GAI in data 21 febbraio 2006.

Muovendo dalla constatazione che l'esistenza di differenze sul piano delle disposizioni legislative, regolamentari e tecniche negli stati membri relativamente alla conservazione dei dati sul traffico costituisce un ostacolo per il mercato interno delle comunicazioni elettroniche, si è giunti, attraverso la direttiva in esame, alla previsione dell'obbligo di conservazione

<sup>16</sup> La disposizione in esame vieta, sia pure temporaneamente, la cancellazione dei dati relativi a qualsiasi forma di traffico telefonico o telematico, che devono essere conservati fino al 31 dicembre 2007 dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico soltanto per quanto riguarda le informazioni che consentono la « tracciabilità degli accessi » e, qualora disponibili, dei « servizi », escluso quindi il contenuto delle comunicazioni; per un'analisi critica della normativa in questione, soprattutto in merito alla flessione delle garanzie tipiche dello Stato di diritto, cfr. FILIPPI, *Le disposizioni processuali*, in *Dir. pen. proc.*, 2005, 1212 ss. e part. 1215, il quale, in relazione ai profili processuali della disciplina, critica il regime delle autorizzazioni all'acquisizione dei dati telefonici e telematici, nel primo periodo di conservazione (ventiquattro mesi per il traffico telefonico e sei mesi

per quello telematico), laddove l'art. 6 del decreto, obliterando ogni riferimento alla garanzia di giurisdizione di cui all'art. 15 Cost., attribuisce al p.m. la legittimazione a disporre l'acquisizione dei dati; cfr., inoltre, STRACUZZI, *Tabulati telefonici: senza norme attuative resta il rebus della conservazione dei dati*, in *Guida dir.*, 2005, n. 47, 88 ss., il quale evidenzia l'assenza di specifiche sanzioni civili, penali o amministrative in caso di violazione delle disposizioni sulla conservazione dei dati.

<sup>17</sup> Cfr. sul punto, DI PAOLO, *Le novità del Parlamento europeo e Consiglio - direttiva del 15 marzo 2006, 2006/24/CE, riguardante la conservazione dei dati generati e trattati nell'ambito della fornitura dei servizi accessibili al pubblico di comunicazione elettronica e di reti pubbliche di comunicazione che modifica la direttiva 2002/58 CE*, in *Cass. pen.*, 2006, 1944 ss.

<sup>18</sup> COM (2005) 438, che risale al 21 settembre 2005.

dei dati del traffico telefonico, ad opera dei fornitori del servizio, per un minimo di sei mesi ed un massimo di due anni dalla data della comunicazione (art. 6), mentre, per quanto riguarda gli *Internet Server Providers*, l'obbligo di rilevazione e conservazione dei dati «esterni»<sup>19</sup> delle comunicazioni elettroniche è stato riferito ad un arco temporale più breve, pari a sei mesi; contestualmente, sono fatte salve misure speciali, adottate dagli Stati membri, in deroga al periodo massimo indicato ed in presenza di «circostanze particolari che giustificano la proroga».

A temperamento di tali ultime restrizioni, la direttiva prevede l'istituzione di organi di vigilanza a livello nazionale, cui conferire il controllo dell'applicazione delle disposizioni nazionali adottate per la protezione e la sicurezza dei dati, nonché l'introduzione di adeguate sanzioni amministrative o penali per punire accessi o divulgazioni non autorizzate dei dati (art. 13, comma 2).

c) GLI ULTIMI SVILUPPI DELLA NORMATIVA INTERNAZIONALE IN MATERIA DI CRIMINALITÀ INFORMATICA: DALLA CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CYBERCRIMINALITÀ ALLA DECISIONE QUADRO 2005/222/GAI RELATIVA AGLI ATTACCHI CONTRO I SISTEMI DI INFORMAZIONE.

Al fine di riavvicinare le legislazioni nazionali, in modo che ogni ordinamento punisca secondo regole comuni determinati fatti ritenuti particolarmente gravi, la Convenzione di Budapest del 23 novembre 2001<sup>20</sup> prevede l'introduzione di una serie di ipotesi incriminatrici così articolate: reati contro l'integrità dei dati e dei sistemi informatici, frodi informatiche, pornografia minorile realizzata e diffusa *on line* e reati contro la proprietà intellettuale.

Per quanto attiene alle regole generali per i gestori dei servizi di rete, la Convenzione prevede, in primo luogo, l'obbligo di punire i fatti di complicità (art. 11, comma I) e, in secondo luogo, alcuni significativi obblighi di collaborazione in capo al *provider*. È previsto, infatti, che gli Stati membri adottino le misure necessarie per consentire che i fornitori di servizi raccolgano e registrino i dati sul traffico, oppure collaborino con le autorità competenti alla registrazione dei dati medesimi (art. 20); a tale obbligo si aggiunge quello per cui (art. 21) il *provider*, in relazione ai casi più gravi, deve raccogliere e registrare non solo i dati relativi al traffico, ma anche al contenuto delle comunicazioni specifiche.

L'art. 18 prevede l'obbligo del *provider* di fornire alle autorità competenti i dati in possesso sui propri abbonati ed in particolare quelli relativi alla loro identità ed al tipo di servizi di comunicazione utilizzati.

<sup>19</sup> Si tratta di dati che non attengono al contenuto delle comunicazioni telefoniche e telematiche, bensì di quelli relativi «al traffico, all'ubicazione, di quelli connessi per identificare l'abbonato o l'utente» che faccia uso di un servizio di comunicazione elettronica accessibile al pubblico

o di rete pubblica di comunicazione, per fini privati o commerciali, senza esservi necessariamente abbonato.

<sup>20</sup> Cfr. SARZANA DI S. IPPOLITO, *La convenzione europea sulla cybercriminalità*, in *Dir. pen. proc.*, 2002, 509 ss.



Il testo della Convenzione risulta abbastanza ampio, considerato che essa è composta di 48 articoli, suddivisi in quattro capitoli — definizioni, misure da adottare a livello nazionale in tema di diritto sostanziale e processuale, cooperazione internazionale, clausola finale —, fra cui numerose fattispecie di diritto penale sostanziale, che le parti devono adottare a livello nazionale (artt. 2-11), relative alla riservatezza, all'integrità e alla disponibilità dei dati informatici e dei sistemi di informazione (accesso illegale, interferenza rispetto ai dati e ai sistemi, ecc.), collegate alle attività informatiche (frode informatica), commesse per mezzo dello strumento informatico (pedopornografia via *Internet*), connesse ad attività di violazione del diritto d'autore.

La Convenzione in esame rappresenta un progresso rispetto alla precedenti iniziative internazionali, costituite da strumenti, come la Raccomandazione, di indubbio peso politico, ma di efficacia normativa limitata. Senonché, lo strumento della convenzione internazionale non implica l'immediata trasposizione delle sue disposizioni negli ordinamenti degli stati aderenti, ma solo l'adeguamento, con gli strumenti giuridici ritenuti più adeguati, ai principi generali descritti nel testo. Principi che, di per sé, spesso assumono portata eccessivamente compromissoria, forse in conseguenza della decisione di aprire la Proposta alla firma di Paesi terzi, cioè estranei al Consiglio d'Europa, come gli U.S.A., il Canada, l'Australia e il Giappone. Le differenti tradizioni giuridiche dei Paesi menzionati e di quelli appartenenti all'area UE, infatti, possono riscontrarsi nelle difficoltà con cui, nell'avvicendamento dei vari progetti, si è affermato il principio di proporzionalità per ciò che attiene agli strumenti di attuazione in ambito processuale contro la delinquenza informatica<sup>21</sup>.

Altra vicenda emblematica delle diversità di impostazioni giuridiche e culturali che separano le due sponde dell'oceano è quella relativa alla trasmissione alle Autorità USA dei dati personali dei passeggeri dei voli transatlantici al fine di combattere il terrorismo e conclusasi con la sentenza della Corte di giustizia delle Comunità europee del 30 maggio 2006 (C-317/04 e C-318/04), che ha annullato le decisioni della Commissione e del Consiglio attraverso le quali era stato dato il via libera alla schedatura dei passeggeri degli aerei diretti o transitanti negli Stati Uniti e che il Parlamento europeo, le autorità per la protezione dei dati e il garante europeo per la protezione dei dati avevano ritenuto lesive della *privacy*<sup>22</sup>.

Senonché, non c'è dubbio che il ravvicinamento del diritto sostanziale rappresenta, come più volte ricordato, un'esigenza imprescindibile, attra-

<sup>21</sup> Per ulteriori approfondimenti sul punto, cfr. MORALES GARCIA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime*, cit., 130.

<sup>22</sup> In realtà, la Corte ha deciso la questione limitandosi a constatare che sia la Commissione che il Consiglio avevano basato la loro decisione sulle disposizioni della direttiva n. 95/46/Ce, che però esclude dal suo ambito di applicazione i trattamenti di dati personali effettuati

per l'esercizio di attività che non rientrano nel diritto comunitario, come quelle previste dai Titoli V e VI del Trattato sull'Unione europea e comunque i trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia penale, ma la vicenda è comunque il risultato di una differente sensibilità che caratterizza la cultura giuridica europea rispetto a quella statunitense in materia di contemperamento fra le istanze di sicurezza e la tutela dei diritti individuali.

verso cui passa l'efficace attuazione almeno degli strumenti esistenti a livello europeo, come dimostra la vicenda dei riferimenti alla criminalità informatica della decisione quadro sul mandato d'arresto europeo, dell'allegato alla convenzione Europol e della decisione del Consiglio che ha istituito Eurojust<sup>23</sup>.

In tale direzione si muove la decisione quadro 2005/222/GAI relativa agli attacchi contro i sistemi di informazione.

In linea con la tradizione delle decisioni quadro, anche essa è preceduta da un ampio preambolo di ben diciotto *considerando*, che ricostruiscono la genesi, la *ratio*, i precedenti ed i principi fondamentali del nuovo strumento normativo. Nell'ottica del rafforzamento della cooperazione giudiziaria e di polizia mediante il ravvicinamento delle legislazioni degli Stati membri, emergono alcune definizioni chiave, quale quella di *sistema di informazione*, di *dati informatici*, di *persona giuridica* e quella riconducibile al concetto di *senza diritto*. Le prime due definizioni ricalcano esattamente quelle previste dalla Convenzione del Consiglio d'Europa sul *cybercrime* (art. 1), oltre a porsi in termini di continuità con la disciplina di primo pilastro ed i precedenti normativi in chiave internazionale; in particolare, la medesima definizione di *sistema di informazione* si ricollega a quella adottata dall'OCSE nel 1992 nelle sue linee guida per la sicurezza dei sistemi di informazione<sup>24</sup>.

Prevedendo la fissazione di « norme minime relative agli elementi costitutivi dei reati », il testo in esame pone a carico degli Stati membri l'obbligo di incriminare tre fondamentali tipologie di condotte: l'accesso illecito ai sistemi di informazione (art. 2), l'interferenza illecita sui sistemi (art. 3) e l'interferenza illecita sui dati (art. 4), incluse le forme dell'istigazione, del favoreggiamento, della complicità e del tentativo (art. 5).

È interessante segnalare che la decisione quadro non prevede un obbligo di penalizzazione quando le condotte siano di scarsa gravità, e ciò in linea con la deroga e le possibilità di riserve contenute nella Convenzione del Consiglio d'Europa; sempre in senso restrittivo, ma sotto il profilo soggettivo, si è ritenuto di restringerne l'ambito di operatività alle ipotesi di commissione intenzionale degli illeciti, non sussistendo l'obbligo di incriminare condotte colpose, ancorché connotate da grave negligenza.

Per quanto concerne le singole ipotesi criminose, cui gli stati membri sono chiamati ad uniformarsi entro il 16 marzo 2007, va rilevato che l'attuale quadro normativo nazionale, con la l. n. 547/1993, sembra già in grado di coprire molti degli obblighi previsti dalla decisione quadro<sup>25</sup>, soprattutto se si considera l'obbligo di interpretazione conforme delle norme interne rispetto alle decisioni quadro, da ultimo affermato dai giudici di Lussemburgo anche nell'ambito del « terzo pilastro »<sup>26</sup>; resta da verificare,

<sup>23</sup> V. CIMINI, *Il contrasto della criminalità informatica*, in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006, 342.

<sup>24</sup> Per una ricostruzione più ampia di tali aspetti, cfr. CIMINI, *Il contrasto della criminalità informatica*, cit., 343-346.

<sup>25</sup> Cfr. CIMINI, *Il contrasto della criminalità informatica*, cit., 352.

<sup>26</sup> Corte di giustizia del 16 giugno 2005, causa C-105/03, *Pupino*, sulla quale cfr. il commento di CHERUBINI, *L'obbligo di interpretazione conforme « sconfina » nel terzo pilastro: note a margine della sentenza Pupino*, in *Studi sull'integrazione europea*, 2006, 157 ss.

inoltre, la conformità delle norme di diritto interno al sistema sanzionatorio, piuttosto articolato e dettagliato, delineato dal provvedimento normativo europeo, incluse le ipotesi aggravate riferite a reati commessi, ad esempio, nell'ambito di un'organizzazione criminale.

Infine, di notevole interesse appare la previsione, in corrispondenza dell'art. 9 della decisione quadro, dell'introduzione di sanzioni effettive, proporzionate e dissuasive, comprensive di sanzioni penali o non, a carico delle persone giuridiche.

### 3. BREVI NOTE DI COMPARAZIONE CON L'ORDINAMENTO AMERICANO: A) PREMESSE GENERALI.

Prima di affrontare le linee essenziali della disciplina prevista, *in subiecta materia*, nel sistema nordamericano, occorre anticipare alcune osservazioni di metodo e di carattere sistematico.

In primo luogo, nonostante la crescita esponenziale delle legislazione federale nei tempi più recenti, il diritto federale statunitense conserva una natura prevalentemente interstiziale: ad esempio, il diritto federale può disciplinare un caso in maniera parziale, regolando la sola *cause of action* a cui può essere contrapposta una *defence* di diritto statale, o viceversa; ovvero, il diritto federale può allocare un diritto il cui rimedio è relegato al diritto statale, o, per converso, il diritto federale può limitarsi a creare, in un determinato caso, un rimedio effettivo per un diritto già ascrivito dallo Stato.

Tutto ciò comporta che il panorama istituzionale ereditato dall'evoluzione storica nordamericana delinei un sistema in cui esiste un completo e biunivoco parallelismo giudiziario fra corti statali e corti federali, queste ultime potendo essere adite o per via di *federal question* o per via di *diversity*<sup>27</sup>.

Da tali premesse discende uno dei temi più classici in materia di diritto americano: il problema del *common law* federale, rispetto al quale la risposta tradizionale, di segno negativo, è stata recentemente messa in discussione anche sulla base del fatto che l'asserzione per cui il *judge-made law* federale sarebbe circoscritto a campi che non hanno nulla a che vedere con il *common law* tradizionale è palesemente contraddetta da importante casistica che estende il *federal common law* ad intere aree del diritto dei contratti e dei *torts*<sup>28</sup>.

Senonché, ai fini delle questioni in tale sede affrontate, occorre subito chiarire che è pacificamente riconosciuta l'assenza di ogni potere, in capo alle corti federali, di creare fattispecie di reato in quei casi in cui la punibilità non sia prevista espressamente dal Congresso.

In secondo luogo, l'analisi di alcune pronunce giurisprudenziali in materia di responsabilità dei *providers* rivelerà tutte le difficoltà che il comparatista continentale generalmente incontra nel distinguere aspetti sostanziali e processuali, come dimostra l'esperienza costituzionale nord-americana, in cui la *due process clause* del V e XIV emendamento è stata

<sup>27</sup> Su tali problematiche, cfr. MATTEI, *Common Law, Il diritto anglo-americano*, in SACCO (diretto da), *Trattato di diritto comparato*, Torino, 2001, 175 ss.

<sup>28</sup> In questo senso, cfr. *op. ult. cit.*, 185 ss.

interpretata come garanzia sia processuale che sostanziale; nel demarcare nettamente la parte speciale da quella generale, in virtù del principio caro ai *common lawyers* secondo cui « *general propositions do not decide concrete cases* »; infine, nel comprendere le ragioni profonde della particolare attenzione riconosciuta nel moderno diritto penale anglo-americano all'elemento soggettivo (*mens rea*), la cui prova oltre ogni ragionevole dubbio attraverso la giuria rappresenta una suprema garanzia individuale che il penalista di *civil law*, invece, è abituato a ricercare sul piano dell'elemento oggettivo.

Inoltre, ulteriore elemento di complessità è rappresentato dal fatto che, pur assistendo ad un'espansione del diritto penale federale, la materia è di regola competenza dei singoli Stati; ad ogni modo, l'abolizione dei *common law crimes*, spesso positivamente sancita in *statutes* penali statali, gli standard uniformi di garanzie elaborati dalla Corte Suprema federale, nonché i contributi offerti dalla dottrina attraverso il *Model Penal Code*, rappresentano aspetti che consentono di affrontare anche in termini generali questioni relative ai profili di responsabilità penale degli ISP.

#### B) IL MODELLO AMERICANO DI ASCRIZIONE DELLA RESPONSABILITÀ DEGLI *INTERNET SERVICE PROVIDERS*.

Nell'ambito dell'alternativa fra la via dell'irresponsabilità del *provider* e quella dell'eccesso di responsabilizzazione del prestatore, la giurisprudenza ha mostrato di oscillare fra i diversi modelli ascrivibili della *vicarious liability* e della *strict liability*, per poi approdare allo schema basato sul *contributory infringement*, nel quale viene valutato l'effettivo contributo del terzo (il *provider*) nella causazione dell'evento dannoso.

Tale impostazione emerge dallo stesso DMCA (Digital Millennium Copyright Act) del 1998 e, soprattutto, al par. 512, intitolato *Limitations on liability relating to material on line*, che individua, ai fini dell'esonero da responsabilità, criteri grosso modo corrispondenti a quelli indicati dalla direttiva 2000/31 CE<sup>29</sup>, mentre, sul piano del bilanciamento fra il principio di non sorveglianza dei siti ed il criterio della conoscenza, la risposta statunitense appare decisamente preferibile nel momento in cui il suddetto provvedimento legislativo detta analiticamente, a fronte della vaghezza della normativa europea, i requisiti della *notification*, che sia idonea a far sorgere in capo al prestatore il dovere di intervenire, secondo lo schema della denuncia da parte del soggetto che si dichiara leso, cui segue la *notification* formale su cui si fonda l'*actual knowledge* del *provider* medesimo<sup>30</sup>.

<sup>29</sup> I casi di esonero da responsabilità del fornitore di un servizio telematico sono i seguenti: 1) trasmissione effettuata da un terzo; 2) trasmissione, connessione e stoccaggio delle informazioni come parte di un processo tecnico che non consente all'intermediario la selezione del contenuto; 3) non selezione, da parte dell'operatore, dei destinatari; 4) contenuto non costituente oggetto di registrazione e conservazione oltre il tempo necessario per la prestazione

tecnica di trasmissione; 5) informazione non sottoposta a modifiche da parte del *provider*.

<sup>30</sup> Cfr. SICA, *Le responsabilità civili*, cit., 275 ss.; sul punto, cfr. l'interessante caso *Parker v. Google, Inc., civil action* no. 04-CV-3918, deciso dalla *United States District Court for the Eastern District of Pennsylvania* (March 10, 2006), riportata in P. SAMMARCO, *Il motore di ricerca, nuovo bene della società dell'informazione:*

L'esperienza giuridica nordamericana, dunque, è stata caratterizzata da un atteggiamento, almeno inizialmente, estremamente liberale nella materia in esame, e ciò in nome dell'affermazione di una generalizzata ed illimitata libertà di comunicazione via *Internet*, di per sé ritenuto « mezzo profondamente democratico », non invasivo e affidato ai « passi concreti » dell'utente nella scelta dei contenuti e servizi da fruire, oltre che economico e « non scarso », come sono, al contrario, le bande di frequenza, per le trasmissioni radio e televisive; conclusione fatta propria dalla giurisprudenza costituzionale nelle pronunce sull'illegittimità del *Telecommunication Act* del 1996, per violazione del Primo Emendamento nella parte in cui comminava sanzioni penali ed amministrative a chi diffondesse o agevolasse la diffusione a minorenni, via *Internet*, di comunicazioni oscene o palesemente offensive della decenza (c.d. *Communications Decency Act*)<sup>31</sup>.

Nel caso in esame, sia la Corte federale del Distretto della Pennsylvania, che la Corte Suprema degli *States* hanno posto alla base delle proprie decisioni l'esigenza di un trattamento differenziato fra i diversi mezzi di comunicazione di massa, caratterizzati da « regole proprie » e diversamente connotati per ciò che concerne « i valori, gli abusi ed i pericoli »<sup>32</sup>.

La Corte Suprema USA, in particolare, facendo ricorso ai canoni argomentativi tipici della propria tradizione, individua due aspetti fondamentali del *Communications Decency Act* suscettibili di censura: in base al primo, incentrato sulla genericità del termine « indecente » e della locuzione riferita a materiali che « nel contesto descrivono o raffigurano, in forme palesemente offensive secondo i parametri vigenti all'interno di una comunità, attività o organi sessuali o escretori », ha dedotto l'insanabile contrasto del divieto — penalmente sanzionato — con il Primo Emendamento; sulla scorta del secondo aspetto, invece, ha confutato le obiezioni del Governo, evidenziando l'irrilevanza dell'astratta possibilità di ricorrere a canali alternativi di comunicazione, l'inadeguatezza del richiamo ai requisiti della « consapevolezza » e della « persona individuata », di per sé non adattabili alla maggior parte degli strumenti di *Internet* (*chat-rooms*, gruppi di informazione, posta elettronica diffusa, *Web*), che invece si caratterizzano nel senso di essere aperti a tutti, la non dimostrata esclusione dall'ambito di applicazione del CDA del materiale scien-

funzionamento, responsabilità e tutela della persona, in questa *Rivista*, 2006, 626-631; la Corte, chiamata a pronunciarsi su una presunta violazione del diritto d'autore, diffamazione e violazione della *privacy* ad opera del motore di ricerca *Google*, ha escluso ogni forma di responsabilità della medesima sulla base della ritenuta legittimità della automatica memorizzazione temporanea delle informazioni risiedenti su *Internet* compiuta dai motori di ricerca.

<sup>31</sup> Cfr. la pronuncia della Corte federale degli Stati Uniti, Distretto della Pennsylvania, 11 giugno 1996, *Aclu et al. v. Reno et al.*, che ha disposto la sospensione cautelare delle norme penali del CDA, trad. it. in questa *Rivista.*, 1996, 604 s., a cura e con nota di ZENO-ZENCOVICH, *Ma-*

*nifestazione del pensiero, libertà di comunicazione e la sentenza sul caso « Internet »*, 640 ss.; Corte Suprema degli Stati Uniti, 26 giugno 1997, *Aclu et al. v. Reno et al.*, trad. it. in questa *Rivista*, 1998, 64 ss., che, respingendo l'impugnazione del Governo avverso la predetta impugnazione cautelare, ha dichiarato l'illegittimità costituzionale delle disposizioni del *Telecommunications Act*, che comminava sanzioni per chi diffondi o agevoli la diffusione, a minorenni, via *Internet*, di comunicazioni oscene.

<sup>32</sup> Parzialmente critico, nei confronti delle decisioni in commento, PICOTTI, *Fondamento e limiti della responsabilità penale dei service-providers in internet*, cit., 382.

tifico, educativo o sociale, e, infine, l'indisponibilità tecnologica di effettive iniziative in buona fede, idonee a selezionare i destinatari di comunicazioni via *Internet*. Tali argomenti, quindi, hanno fatto propendere la Corte Suprema per il carattere palesemente irragionevole delle disposizioni esaminate; sulla base del testo in esame, infatti, non si sarebbe potuto escludere il divieto di discussioni, ad esempio, sulle pratiche di controllo delle nascite, sull'omosessualità o sulla violenza sessuale nelle carceri.

L'orientamento giurisprudenziale da ultimo esaminato, in realtà, si scontra con la recente evoluzione dell'ordinamento degli USA; la necessità di approntare una risposta efficace, di tipo preventivo e repressivo, al nuovo fenomeno del terrorismo internazionale, ha indotto il legislatore statunitense ad attenuare sensibilmente gli *standard* di garanzia tradizionalmente appartenenti al patrimonio giuridico di tale ordinamento democratico, al punto da giungere ad introdurre la possibilità di penetranti ingerenze, da parte dei pubblici poteri, nella sfera privata, in nome di istanze socialdifensive spesso più predicate che effettivamente perseguite.

Il richiamo delle linee di tendenza testé accennate rimanda immediatamente alle disposizioni contenute nel « *USA Patriot Act* » del 26 ottobre 2001 e del « *Homeland Security Act* » del 19 novembre 2002<sup>33</sup>, maggiormente noto come *Patriot Act II*.

Con riferimento alla disciplina delle intercettazioni di comunicazioni telefoniche, telematiche o tra presenti (c.d. intercettazioni ambientali), infatti, occorre muovere dal quadro di una già discutibile disciplina organica in materia di sorveglianza elettronica, che distingueva fra indagini a carattere interno (regolate dall'*Omnibus Crime Control and Safe Streets Act* del 1968<sup>34</sup>) e indagini rivolte all'acquisizione di informazione classificata come *foreign intelligence information*, necessaria per proteggere la nazione di fronte al terrorismo internazionale o ad attività di spionaggio (regolate dal *Foreign Intelligence Surveillance Act* del 1978); la sezione 215, sancendo che tale scopo non necessariamente deve costituire l'unico obiettivo dell'indagine, bensì uno « scopo significativo », ha accorciato sensibilmente le distanze fra il regime delle indagini a carattere interno e quelle a carattere spionistico, così includendo i cittadini statunitensi fra i destinatari delle indagini la cui autorizzazione è attribuita ad un giudice della *FISA Court*, che, a differenza del giudice ordinario, agisce sempre nella più totale segretezza<sup>35</sup>. L'estensione, infine, alle comunicazioni mediante mezzi elettronici (sezioni 214 e 216), del regime delle comunicazioni telefoniche ha comportato la legittimazione degli organi di polizia federale (FBI), sulla base della

<sup>33</sup> Di cui segnala, ai fini del tema in esame, la Sez. 225, dedicata al cyberterrorismo e denominata « *Cyber Security Enhancement Act of 2002* ».

<sup>34</sup> L'*Omnibus Crime Control and Safe Streets Act* consentiva che gli organi di polizia effettuassero tal intercettazioni solo nel corso di indagini riguardanti certi reati tassativamente previsti; il *Patriot Act* completa l'elenco aggiungendovi altre fattispecie, fra cui quella di frode commessa on il mezzo di elaboratori elettronici (*computer fraud* 18 USC 1030).

<sup>35</sup> La *FISA Court*, il cui organo d'appello è rappresentato da una *Court of review*, agisce in segreto, senza pubblicare le sue decisioni e permettendo solo al Governo di apparire innanzi ai giudici, con la conseguente impossibilità, da parte della persona sottoposta ad una sua ordinanza di contestarne la legittimità, come invece accade nelle indagini condotte in ordinari procedimenti penali: cfr. BILLÉ, « *Patriottismo* » costituzionale e libertà d'informazione: il caso statunitense, cit., 143 nt. 55.

mera allegazione, da parte del *Public Prosecutor*, della rilevanza della misura ai fini delle indagini ed a prescindere dalla sussistenza del *fumus* della commissione di alcun reato (*probable cause*), all'espletamento di un'attività di sorveglianza talmente penetrante da poter acquisire una quantità pressoché illimitata di dati a carattere personale, con grave sacrificio di quel diritto fondamentale, riconducibile al Primo, al Quarto ed al Quattordicesimo Emendamento, rappresentato dalla *privacy* dei cittadini<sup>36</sup>.

In particolare, la sezione 212 permette ai *provider* dei servizi *Internet* di fornire agli inquirenti ogni informazione anche estranea alle *content information* (come, ad esempio, le parole-chiave personali di accesso al servizio) ritenuta immediatamente pericolosa per la vita umana e ciò senza dover ottenere una previa autorizzazione da parte di un giudice, così come (sezione 217) la polizia federale risulta libera di intercettare ogni genere di informazione<sup>37</sup>, se un *provider* attesta che l'utente sia entrato in rete senza permesso.

Le reazioni al rigore repressivo di tale legislazione emergenziale, in cui la priorità assoluta della sicurezza è perseguita attraverso il sacrificio delle garanzie della giurisdizione e la preferenza accordata al rafforzamento indiscriminato dei poteri investigativi<sup>38</sup>, sono affidate prevalentemente ad alcune pronunce di incostituzionalità di diversi Tribunali Federali, in merito all'utilizzo, ad esempio, della *National Security Letter* (section 505 del *Patriot Act*)<sup>39</sup>, vale a dire del mandato amministrativo di comparizione avvolto nella segretezza e che riguarda questioni inerenti alla sicurezza nazionale, ovvero della Corte Suprema degli Stati Uniti<sup>40</sup>.

<sup>36</sup> Per un'analisi più dettagliata della disciplina, ed un'attenta critica degli effetti che ne conseguono sul piano della tutela delle garanzie, nonché sulla stessa funzione che il diritto penale dovrebbe svolgere in uno Stato di diritto, cfr. MANNA, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in *Riv. it. dir. proc. pen.*, 2004, 1022 ss., ed *ivi*, 1026-1029.

<sup>37</sup> Per quanto concerne, invece, il contenuto delle *e-mails*, la nuova legge non fa venire meno la necessità del provvedimento giudiziario, ma estende la possibilità degli inquirenti di rivolgersi a qualsiasi giudice, purché dotato di giurisdizione sul reato per cui si procede (Sez. 220): cfr. REBECCA, *Intelligence e controllo delle comunicazioni telematiche nella legislazione statunitense antiterrorismo*, in *Dir. pen. proc.*, 2003, 1292 ss.

<sup>38</sup> Per un'idea delle contrapposte reazioni suscitate negli USA dal *Patriot Act*, cfr. le vibranti proteste espresse nella società civile, fra cui quella della Electronic Frontier Foundation, *EFF analysis of the provisions of the USA Patriot Act*, in *www.eff.org*, ovvero le critiche di DERSHOWITZ, *Why Terror-*

*ism Works. Understanding the Threat, Responding to the Charge*, trad. it. CORRADI, *Terrorismo*, Roma, 2003, 152 ss.; dall'altro lato, il giudizio complessivamente positivo formulato da O.S. KERR, *Internet surveillance law after the USA Patriot Act: the big brother that isn't*, The George Washington University Law School, *Public Law Research Paper*, n. 42, 2002, 81.

<sup>39</sup> Cfr. la decisione della *United States District Court Southern District of New York*, *John Doe v. John Ashcroft*, 2004, cit. in BILLE, « *Patriottismo* » costituzionale e libertà d'informazione: il caso statunitense, cit., 146.

<sup>40</sup> Cfr., sia pure con riferimento alla violazione dei diritti fondamentali per i detenuti di Guantanamo, *Hamdi v. Rumsfeld*, Secretary of Defense, 542 U.S. (2004); *Rasul et al. v. Bush*, Presidente of the United States, et al., Case No. 03-334 (U.S., decided June 28, 2004); *Rumsfeld, Secretary of Defense v. Padilla et al.*, Case No. 03-1027 (U.S. decided June 28, 2004), tutti citati in CERQUA, *I profile processuali della legislazione antiterrorismo U.S.A.: brevi cenni*, in *Cass. pen.*, 2006, 1948 ss.

#### 4. BREVI RIFLESSIONI SULLA NORMATIVA NAZIONALE DI RECEPIMENTO DELLA DIRETTIVA 2000/31 CE.

Il rigore repressivo riscontrato nell'ordinamento nordamericano, per quanto concerne il controllo investigativo sulle informazioni utili a prevenire fenomeni terroristici, invece, non sembra ravvisabile nelle esperienze giuridiche europee; invece, sul piano dei criteri di imputazione della responsabilità del *provider* per i reati commessi attraverso la rete, a prescindere dalle differenze derivanti dalla tradizione normativa di questi ultimi Paesi, nella sostanza si assiste ad un orientamento volto ad evitare forme di responsabilità oggettiva in capo ai detti prestatori, sulla scia di quanto già emerso in ambito statunitense.

Dunque, sul piano della prevenzione, il vecchio Continente non ha rinunciato alle garanzie minime in tema di *Habeas data*<sup>41</sup>, né le modifiche alle fattispecie incriminatrici afferenti all'attività terroristica autorizzano a ritenere integrato un nuovo esempio di « diritto penale del nemico »<sup>42</sup>.

Più in particolare, per quanto concerne la normativa nazionale di recepimento della direttiva 2000/31, la legge delega 39/2002 si è limitata alla semplice riproduzione letterale del testo della direttiva. Essa, infatti, prevedeva, nelle ipotesi di lesione del diritto del privato, l'obbligo di predisporre sanzioni « effettive, proporzionate e dissuasive », senza specificarne la natura, limitandosi a riprodurre lo schema classico secondo cui la direttiva può imporre agli Stati membri solo l'adozione (genericamente) di sanzioni « effettive, proporzionate e dissuasive » lasciando libero lo Stato di scegliere tra sanzione penale e sanzioni diverse<sup>43</sup>.

Ciò premesso, non si può certo dire che l'intervento del legislatore nazionale risponda ai canoni della migliore tecnica legislativa, se si considera che il Parlamento, con la delega al Governo, ha disatteso le istanze garantistiche sottese alla riserva di legge, laddove ha totalmente devoluto al Governo la scelta di valore del tipo e della misura della sanzione<sup>44</sup>; successivamente, il legislatore delegato, nell'approvare il d.lgs. 70/2003, non ha ri-

<sup>41</sup> Cfr. RODOTÀ, *La vita e le regole*, Milano, 2006, 113, il quale sottolinea come, nella c.d. « società dell'informazione » la vita di ciascun individuo, almeno nei suoi tratti più significativi, si può ripercorrere attraverso lo schermo di un computer ed il rischio concreto è che ci si avvii verso la società del controllo totale, in cui si completa la trasformazione del cittadino in « uomo di vetro ».

<sup>42</sup> In questo senso, cfr. MANNA, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, cit., 1054.

<sup>43</sup> Sulla giurisprudenza della Corte di Giustizia CE, a partire dalla sentenza sul « mais greco » (CGCE, 21 ottobre 1989, causa 68/88, Commissione c. Grecia), cfr. BERNARDI, *I tre volti « del diritto penale comunitario »*, in AA.VV., *Possibilità e limiti di un diritto penale dell'unione europea*, a

cura di Ricotti, Milano, 1999, 79 ss.; con riferimento alla tematica dell'adeguatezza degli interventi attuativi predisposti dal legislatore nazionale in base alle direttive comunitarie, in materia di false comunicazioni sociali, cfr. SALCUNI, *Le false comunicazioni sociali: questioni di legittimità costituzionale e obblighi comunitari di tutela*, in RIDPP, 2003, 843 ss.

<sup>44</sup> Sul rapporto fra legge delega e decreto delegato, in relazione alle garanzie sottese al principio di riserva di legge, sia consentito il rinvio a PERDONÒ, *L'uso illecito e le violazioni in materia di alienazione: riproposizione di vecchi schemi a fronte della rinuncia alle chances offerte dalle nuove frontiere della politica criminale*, in MANNA (a cura di), *Il Codice dei beni culturali e del paesaggio, gli illeciti penali*, Milano, 2005, 83-86.



tenuto opportuno introdurre sanzioni penali a carico del *provider*, ma ha affidato prevalentemente alla reazione civile, ad eccezione di marginali ipotesi di natura amministrativa<sup>45</sup>, compiti che più efficacemente altre tipologie sanzionatorie avrebbero potuto assolvere.

In particolare, considerato che l'impianto normativo riflette la scelta di preferire l'imposizione, a carico dei fornitori del servizio, di obblighi di collaborazione diretta e indiretta, non integranti doveri di difficile esecuzione, piuttosto che un inesigibile obbligo di sorveglianza o di ricerca attiva di circostanze che indichino la presenza di attività illecite, ben avrebbe potuto il legislatore nazionale, in base ad una tecnica ispirata al modello ingiunzionale, sanzionare penalmente, o in via amministrativa, l'inottemperanza di specifici provvedimenti amministrativi o giurisdizionali che dispongano la rimozione di informazioni illecite o che ne disabilitino l'accesso<sup>46</sup>.

D'altronde, altre tecniche di tutela penale, come quella, ad esempio, sperimentata nell'ordinamento tedesco, non sembrano aver sortito risultati apprezzabili. In tale prospettiva, si consideri l'art. 1 della legge sui servizi di informazione e comunicazione emanata il 22 luglio 1997 dal legislatore tedesco (LuKDG), che ha istituito a sua volta una legge sui servizi telematici (TDG), il cui art. 5, nel dettare le regole in ordine alla responsabilità dei fornitori, prevede, al secondo comma, che essi sono responsabili dei materiali altrui da essi resi disponibili solo se hanno conoscenza dei loro contenuti e sia loro tecnicamente possibile ed esigibile impedirne la disponibilità<sup>47</sup>. Il legislatore tedesco, nel tentativo di contemporaneamente di non rinunciare a combattere la diffusione di illeciti attraverso la co-responsabilizzazione di un soggetto garante e quella di non gravare eccessivamente sulla possibilità di realizzare profitti, ha dato forma ad una fattispecie oggetto di rilievi critici sotto un duplice profilo: un primo,

<sup>45</sup> Il legislatore nazionale, infatti, si è affidato al sistema delineato dalla L. 689/1981, come si evince dall'art. 21 del d.lgs. 70/2003, che prevede la sanzione amministrativa pecuniaria, raddoppiata nei casi di particolare gravità o di recidiva, per le violazioni delle disposizioni del medesimo testo normativo in materia di obblighi informativi: sul punto, cfr. BUONOMO, *Le responsabilità penali*, in *Commercio elettronico e servizi della società dell'informazione*, a cura di TOSI, cit., 306.

<sup>46</sup> Cfr. PETRINI, *La responsabilità penale per i reati via internet*, cit., 207 ss., secondo cui, data la difficoltà di immaginare una posizione di garanzia, sembra opportuno introdurre nel nostro ordinamento una responsabilità penale del *provider* ristretta a pochi ed esigibili doveri di collaborazione con l'autorità giudiziaria o di polizia.

<sup>47</sup> Nell'ambito del medesimo art. 5, il primo comma stabilisce che i fornitori di servizi sono responsabili secondo le leggi comuni dei propri materiali da essi resi disponibili. Il terzo comma che gli stessi soggetti non sono responsabili dei materiali al-

trui ai quali hanno fornito solo l'accesso (e si precisa che una ritenzione automatica e di breve durata di materiali altrui, conseguente alla richiesta di utenti, va considerata come fornitura di accesso). Il quarto, infine, che qualora, nel rispetto della riservatezza delle comunicazioni a distanza di cui al § 85 della legge sulle telecomunicazioni, il fornitore di servizi acquisisca conoscenza di contenuti illeciti e una chiusura sia tecnicamente possibile ed esigibile, rimangono salvi, secondo le leggi generali, gli obblighi di impedimento della disponibilità di tali materiali; le disposizioni introdotte dal legislatore tedesco nel 1997, in conclusione, laddove sanciscono l'irrelevanza dei comportamenti di mera fornitura di accesso alla rete, l'implicita esclusione di un obbligo generalizzato di controllo da parte del *provider*, la previsione di doveri di impedimento dell'accesso e di eliminazione dei materiali illeciti solo a limitatissime condizioni, sembrano anticipare le linee portanti della direttiva 2000/31 CE, come puntualmente posto in risalto da PETRINI, *La responsabilità penale per i reati via internet*, cit., 205.

caratterizzato dall'improprio riferimento ad una categoria, quella dell'inesigibilità, difficilmente compatibile con le situazioni considerate dalla norma, dal momento che il richiamo espresso sembra riferirsi, più che al profilo soggettivo della fattispecie, a quei criteri di ragionevolezza, proporzione e non discriminazione menzionati dalla Dichiarazione finale della Conferenza ministeriale europea di Bonn dell'8 luglio 1997; un secondo, infine, focalizzato sull'inefficacia dell'intervento sanzionatorio in esame, non solo perché in gran parte dei casi verrebbe a svolgersi dopo che la diffusione dei materiali illeciti ha già avuto luogo (e dunque al massimo potrebbe essere funzionale ad impedirne ulteriori effetti), ma soprattutto per i problemi che causerebbe in caso di erronea valutazione del carattere illecito o meno del materiale transitante in rete. Infatti, appare dubbia l'opportunità di investire della posizione di garanzia un soggetto che, non avendo spesso attitudini professionali ed intellettuali tali da potergli far discernere con precisione la natura illecita di condotte realizzate attraverso la rete, potrebbe seriamente mettere in pericolo la libera circolazione delle idee e delle opinioni<sup>48</sup>.

Certamente, non si ignorano le tradizionali critiche rivolte a tecniche di tutela che passano attraverso la « procedimentalizzazione » della conformazione strutturale dell'illecito, a causa del suo preteso contrasto col principio di riserva di legge<sup>49</sup>; tuttavia, una scelta di tal segno sembra suggerita dalla stessa previsione dell'art. 16, comma 1, lett. b) del decreto legislativo in esame, che lega la conoscenza dell'illiceità di un'attività o di un'informazione alla comunicazione delle autorità competenti, così innovando rispetto all'art. 14, lett. b) della direttiva, che invece non prevede la necessità di « ufficializzare » la conoscenza da parte delle autorità competenti.

Il ricorso alla predetta tecnica di tutela, infatti, affiderebbe alla sanzione il compito di reagire all'omessa esecuzione di un provvedimento individuale e concreto, pertanto rilevante sul piano dell'accertamento concreto del fatto e non su quello della ricostruzione del precetto, la cui descrizione resterebbe assegnata alla legge nel momento in cui impone l'osservanza della classe di provvedimenti cui appartiene quello nello specifico notificato<sup>50</sup>.

<sup>48</sup> Per queste riflessioni, cfr. più diffusamente FORNASARI, *Il ruolo della esigibilità nella definizione della responsabilità penale del provider*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, cit., 423 ss., il quale aggiunge che sarebbe stata preferibile l'introduzione di una sanzione penale, o meglio amministrativa, a carico del provider per mancato rispetto di obblighi di denuncia e per inadempimento di obblighi dettati da un'autorità pubblica; parzialmente diverso è il giudizio espresso da PICOTTI, *Fondamento e limiti della responsabilità penale dei service-providers in internet*, in *Dir. pen. proc.*, 1999, 379, il quale, essendo favorevole, in generale, alla predisposizione di obblighi giuridici, di controllo preventivo e successivo, ed eventualmente anche di « impedimento », in capo ai fornitori e gestori responsabili dei vari

servizi, valuta positivamente le disposizioni legislative tedesche nella misura in cui co-responsabilizzano i providers attraverso il riconoscimento di posizioni di garanzia, penalmente rilevanti, in capo ai medesimi.

<sup>49</sup> In tal senso, cfr. NUVOLONE, *Norme penali in bianco e riserva di legge: a proposito della legittimità costituzionale dell'art. 650 c.p.*, in *Giur. cost.*, 1956, 1271; BRICOLA, *Il II e il III comma dell'art. 25*, in BRANCA (a cura di), *Commentario alla Costituzione. Rapporti civili. Art. 24-26*, Roma-Bologna, 1981, 243 ss.

<sup>50</sup> M. ROMANO, *Repressione della condotta antisindacale. Profili penali*, Milano, 1974, 160 ss.; PEDRAZZI, *Odierna esigenza economiche e nuove fattispecie penali*, in *RIDPP*, 1975, 1110; MARINUCCI-DOLCINI, *Corso di diritto penale*, p.g., 3<sup>a</sup>, Milano, 2001, 397.

Pertanto, sembra rigidamente ancorato ad una concezione eccessivamente formalistica del principio di riserva di legge l'impianto argomentativo rinvenibile nelle decisioni del *Conseil constitutionnel* del 23 luglio 1996 e del 27 luglio 2000, con cui la suprema magistratura francese ha dichiarato l'illegittimità costituzionale di fattispecie in cui il potere d'individuare un elemento costitutivo sia affidato all'Autorità amministrativa (il *Comité supérieur de la télématique*), attraverso la repressione penale del *provider* che non abbia rimosso i materiali illeciti nonostante la pubblicazione di un provvedimento del suddetto *CST* sul *Journal officiel de la République*, oppure alla richiesta di un privato che denunci la presenza di contenuto illecito o se ne dichiari pregiudicato, secondo uno schema analogo a quello previsto dal nostro art. 328, co. 2, c.p., che non sembra integrare, a dire il vero, un'ipotesi di norma penale in bianco<sup>51</sup>.

Meno felice appare, invece, la decisione di non dare indicazione alcuna, più che della nozione di « effettiva conoscenza » dell'illiceità, del livello di « prontezza » richiesto per la rimozione dei contenuti ritenuti illeciti<sup>52</sup>, dal momento che, in caso di ricorso a forme di tutela penale, ragionevolmente di tipo contravvenzionale, tale concetto aderirebbe più efficacemente al principio di determinatezza attraverso l'aggancio a parametri oggettivi<sup>53</sup>.

Inoltre, la proposta di introdurre una ipotesi contravvenzionale che reprima l'inosservanza di specifici obblighi di collaborazione segnalati dalle Autorità competenti risponde all'opportunità di evitare l'impropria dilatazione della responsabilità penale che deriva dall'ammettere l'applicazione, a carico del prestatore di servizi, della clausola generale dell'art. 40 cpv. c.p., per omesso impedimento del reato commesso da terzi servendosi dei servizi offerti dal *provider*; senza trascurare, tra l'altro, sul fronte dell'elemento soggettivo, le notevoli potenzialità repressive offerte dall'istituto del dolo eventuale<sup>54</sup>.

<sup>51</sup> Con la legge 96-659 del 18 giugno 1996, il Parlamento francese ha modificato in parte la legge 30 settembre 1986 in tema di libertà delle telecomunicazioni, introducendovi gli artt. 43-2 e 43-3; in base alla normativa in esame, il provvedimento del *CST* costituiva un presupposto per fondare la responsabilità penale del *provider* per i fatti di reato commessi attraverso le sue strutture di rete; dopo la pronuncia di illegittimità costituzionale dei predetti articoli, la l. 28 giugno 2000 ha introdotto una nuova disposizione (l'art. 43-9), che subordinava la punibilità del *provider* alla mancata attivazione di poteri di rimozione a seguito di richiesta di un privato. Attualmente, in base alla disciplina introdotta con la legge 1° agosto 2000, n. 2000-719, l'intervento penale è sostanzialmente limitato ad alcuni doveri di collaborazione, fra cui l'informazione, la tenuta di dati e la loro messa a disposizione dell'autorità giudiziaria: per un esame più approfondito delle questioni in esame, cfr. PETRINI, *La responsabilità*

*penale per i reati via internet*, cit., 20201-204; per un'analisi della disciplina francese in materia di criminalità informatica, cfr. NEDELEC, *La criminalità informatica nel diritto penale francese*, in *Dir. pen. proc.*, 2002, 241 ss.

<sup>52</sup> Cfr., in tal senso, COMANDÉ, *E-commerce: un passo verso regole certe*, in *Guida dir.*, 2003, n. 16, 10 ss., e segnatamente 11.

<sup>53</sup> Cfr., ad esempio, C. cost., n. 34/1995, che ha dichiarato incostituzionale una disposizione incriminatrice in materia di asilo, ingresso e soggiorno di cittadini extracomunitari (art. 7-bis l. 28 febbraio 1990, n. 39); sulla crisi della tradizionale dimensione della tassatività e sulla problematicità di ogni procedimento di sussunzione, cfr. DI GIOVINE, *L'interpretazione nel diritto penale tra creatività e vincolo alla legge*, Milano, 2006, *passim*.

<sup>54</sup> In senso contrario a strumentalizzazioni in senso repressivo, cfr. MANNA, *Profili problematici della nuova legge in tema di pedofilia*, in *Ind. pen.*, 1999, 50.

In realtà, a parte la questione — di carattere generale — relativa alla possibilità di far coincidere l'evento di cui alla norma dianzi richiamata con l'intero fatto di reato<sup>55</sup>, non sembra di poter riscontrare una posizione di garanzia atta a fondare ipotesi di responsabilità penale in capo al *provider*, soluzione verso cui si orienta anche recente giurisprudenza nel momento in cui ritiene non configurabile, per il prestatore, « un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né un obbligo generale di ricercare attivamente fatti o circostanze che indichi la presenza di attività illecite »<sup>56</sup>.

Una fattispecie incriminatrice conformata alla tecnica precedentemente descritta, invece, prevarrebbe, in quanto speciale, su un'eventuale ipotesi di omissione impropria<sup>57</sup>.

In conclusione, alla luce dei più recenti sviluppi della giurisprudenza della Corte di giustizia delle Comunità europee, poiché il settore dei reati commessi attraverso gli strumenti informatici richiede una politica legislativa uniforme nei diversi Paesi, indifferentemente dal loro grado di sviluppo tecnologico ed in vista di una stretta collaborazione tra gli ordinamenti sul fronte della repressione, sarebbe auspicabile un nuovo intervento del legislatore europeo, anche attraverso una direttiva che, in materia di commercio elettronico, imponga agli Stati membri l'adozione di sanzioni penali costruite secondo il modello ingiunzionale dianzi descritto. L'osservazione da ultimo effettuata non deve destare meraviglia, se si considera che anche la Commissione europea<sup>58</sup>, prendendo ufficialmente posizione in ordine alla portata ed alle conseguenze della sentenza della Corte di giustizia delle Comunità europee 13 settembre 2005 nella causa C-176/03<sup>59</sup>, riconosce alla Comunità europea una competenza « strumentale » in materia penale<sup>60</sup>.

Infatti, se è vero che, alla luce di questa sentenza, il principio del monopolio del legislatore nazionale potrà in futuro subire un'ulteriore ed assai incisiva limitazione<sup>61</sup>, la possibilità che rientrano nell'ambito del primo pi-

<sup>55</sup> In senso affermativo, cfr. GRASSO, *Il reato omissivo improprio*, Milano, 1983, 140 s.; *contra*, cfr. FIANDACA, *Il reato commissivo mediante omissione*, Milano, 1979, 181; RISICATO, *Combinazione e interferenza di forme di manifestazione del reato. Contributo ad una teoria delle clausole generali di incriminazione suppletiva*, Milano, 2001, 450; più articolata la posizione di LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999, 361-371; MARCONI, *Rappresentanza politica e responsabilità per omissione impropria*, Milano, 2005, 245 ss.

<sup>56</sup> Tribunale di Milano, 25 febbraio 2004, n. 1993, in *www.penale.it*, con nota di CAVANNA, *La responsabilità dei providers alla luce della sentenza del Tribunale di Milano — Sezione V Penale in composizione collegiale — n. 1993 del 25 febbraio 2004*.

<sup>57</sup> In tal modo colmando vuoti di tutela che la magistratura potrebbe ritenere

di riempire con interpretazioni di tipo estensivo-additivo, secondo quella tendenza opportunamente messa in luce, in termini generali, da FIANDACA, *Diritto penale giurisprudenziale e spunti di diritto comparato*, in ID. (a cura di), *Sistema penale in transizione e ruolo del diritto giurisprudenziale*, Padova, 1997, 1 ss.

<sup>58</sup> Comunicazione 23 novembre 2005, COM (2005) 583 final, indirizzata al Parlamento europeo ed al Consiglio.

<sup>59</sup> Sul tema, cfr. VIGANÒ, *Recenti sviluppi in tema di rapporti tra diritto comunitario e diritto penale*, in *Dir. pen. proc.*, 2005, 1433 ss.

<sup>60</sup> Sul tema, cfr. MIRABILE, *Verso un nuovo diritto penale europeo: la Comunicazione 23 novembre 2005, COM (2005) 583 final della Commissione al Parlamento europeo ed al Consiglio*, in *Cass. pen.*, 2006, 1934 ss.

<sup>61</sup> Il problema evoca quello della legalità penale e del deficit di democraticità

lastro tutte le disposizioni, comprese quelle di diritto penale, necessarie per la realizzazione effettiva degli obiettivi della Comunità, residuando, per il terzo pilastro, gli aspetti di diritto e procedura penale che abbisognano di un trattamento « orizzontale », potrebbe comunque essere bilanciata dalla circostanza per la quale il ricorso allo strumento penale deve essere necessario, così come incombe sul legislatore comunitario un obbligo motivazionale in relazione alla suddetta necessità; conclusione che altro non implica se non la restituzione, al principio di *extrema ratio*, di quella centralità da sempre sacrificata dal legislatore nazionale<sup>62</sup>.

## 5. SPUNTI DI RIFORMA IN RELAZIONE ALLE ALTRE DIRETTIVE.

Per quanto riguarda, invece, la recentissima direttiva del 15 marzo 2006, 2006/24/CE sulla conservazione dei dati generati e trattati nell'ambito della fornitura dei servizi accessibili al pubblico di comunicazione elettronica e di reti pubbliche di comunicazione, che modifica la direttiva 2002/58 CE e impone agli Stati membri di adottare adeguate sanzioni amministrative o penali per punire accessi o divulgazioni non autorizzati dei dati (art. 13, comma 2), occorre segnalare che gli obiettivi di tutela testé indicati sono già sostanzialmente garantiti dalle vigenti fattispecie incriminatrici di cui al primo e secondo comma dell'art. 617-*quater* c.p., cui occorre aggiungere l'ulteriore ipotesi delittuosa prevista dall'art. 3 della « controversa » l. 20 novembre 2006, n. 281, che ha convertito il decreto-legge n. 259/2006 recante disposizioni urgenti per il riordino della normativa in tema di intercettazioni illegali<sup>63</sup>. Tale fattispecie, che punisce, con la medesima sanzione base della suddetta disposizione codicistica, chi consapevolmente detenga atti, supporti o documenti concernenti dati e contenuti relativi al traffico telefonico e telematico illegalmente formati o acquisiti, nonché documenti formati attraverso la raccolta illegale di informazioni, di cui sia stata disposta la distruzione, predispone una tutela anticipata dell'interesse collettivo volto ad impedire la circolazione di dati illecitamente acquisiti — piuttosto che alla tutela della riservatezza dei soggetti interessati —<sup>64</sup>; in assenza di alcuni dei presupposti della fatti-

delle istituzioni comunitarie, per cui cfr. PICOTTI, *Diritto penale comunitario e Costituzione europea*, in AA.VV., *Il diritto penale nella prospettiva europea - quali politiche per l'Europa?*, a cura di CANESTRARI e FOFFANI, Milano, 2005, 325 ss.

<sup>62</sup> Sul tema, in generale, della sussidiarietà, cfr., tra l'altro, DONINI, *Il volto attuale dell'illecito penale*, Milano, 2004, 85 ss.

<sup>63</sup> Le critiche principali, infatti, sono state rivolte soprattutto con riferimento al profilo del principio del contraddittorio per la formazione della prova, di cui il provvedimento dispone un sacrificio irragionevole e la sua sostituzione col contraddittorio sul verbale relativo all'acquisizione e alle operazioni di distruzione degli atti

di cui all'art. 240 c.p.p., a fronte dell'interesse delle parti ad accertare le circostanze di fatto rilevanti ai fini dell'accertamento della responsabilità o dell'innocenza dell'imputato: sul punto, cfr. FILIPPI, *Distruzione dei documenti e illecita divulgazione di intercettazioni: lacune ed occasioni perse di una legge nata già « vecchia »*, in *Dir. pen. proc.*, 2007, 152 ss.

<sup>64</sup> Sui profili dell'offesa della fattispecie in esame, cfr. GAMBARDELLA, *Il delitto di detenzione di atti relativi a intercettazioni illegali*, in *Dir. pen. proc.*, 2007, 165, il quale individua la tecnica di tipizzazione impiegata dal legislatore in quella del *pericolo eventualmente indiretto*, ovvero del *delitto c.d. ostativo*, con le conseguenti critiche sul piano del rispetto del principio di

specie, per altro, è da ritenersi salva l'eventuale illiceità penale delle condotte strumentali alla acquisizione, così come la configurabilità di un concorso formale eterogeneo nel caso della realizzazione contestuale, attraverso un'unica condotta storica, del delitto in esame e della ricettazione<sup>65</sup>. Diversamente, un fatto storico che integrasse contemporaneamente il delitto di detenzione illegale di materiale *ex art.* 240 c.p.p. e quello *ex art.* 167 Cod. *privacy*, non darebbe luogo ad un concorso formale eterogeneo di reati, in virtù della clausola di riserva prevista da quest'ultima disposizione<sup>66</sup>.

Ciò premesso, anche il quadro relativo alla violazione delle disposizioni sulla conservazione si presenta disarticolato e confuso, soprattutto se si considera che i recenti interventi di riforma — fra cui quello risalente al d.l. 144/2005 e alla l. 155/2005 — non prevedono alcun tipo di sanzione nei casi di abuso in materia di conservazione dei dati.

Pertanto, alla luce dell'attuale assetto di disciplina della materia in esame, si profila una irragionevole disparità di trattamento fra l'ipotesi di cancellazione di dati di traffico telefonico o telematico durante il periodo di conservazione obbligatoria, in caso di richiesta, ad esempio, da parte del pubblico ministero nel corso della propria attività di indagine, che risulta priva di tutela penale anche alla luce delle sanzioni predisposte dal Codice *privacy*, e quella, viceversa, di mancata cancellazione del medesimo materiale al termine del periodo di conservazione obbligatoria, che, in virtù della circostanza per la quale il trattamento in violazione dell'art. 123 d.lgs. 196/2003 interessa il profilo della conservazione, rientra nell'ambito di applicazione dell'art. 167, primo comma, del Codice da ultimo menzionato<sup>67</sup>. Inoltre, poiché la norma incriminatrice in esame integra un reato di danno, che richiede la prova, tutt'altro che agevole, del nocumento e del fine di trarre profitto o di arrecare un danno, non è infondato il timore che, nelle ipotesi di mero pericolo, la giurisprudenza possa ricorrere, dilatandone oltre ogni ragionevole limite la portata, alla nuova fattispecie di detenzione illegale di materiale relativo alle comunicazioni telefoniche e telematiche di cui alla l. 281/2006, in tal modo dando adito all'emersione di diversi profili di irragionevolezza, essendo quest'ultimo delitto punito più gravemente di quello previsto in materia di trattamento illecito di dati personali, oltre che sovrapponendo due piani, quello delle intercettazioni illecite e quello dei dati lecitamente raccolti ma conservati oltre termine, che traggono origine da situazioni differenti e presuppongono distinte *rationes* di tutela: infatti, come opportunamente rilevato<sup>68</sup>, nono-

offensività; per un commento «a caldo» della fattispecie, cfr. MARZADURI, *Intercettazioni: le troppe lacune di un testo approvato «con riserva»*, in *Guida dir.*, 2006, n. 47, 11.

<sup>65</sup> Cfr. GAMBARDILLA, *Il delitto di detenzione di atti relativi a intercettazioni illegali*, cit., 167; BRICCHETTI, *Fino a quattro anni di carcere se c'è detenzione illegale dei supporti*, in *Guida dir.*, 2006, n. 47, 19; per la configurabilità, prima che il giudice abbia disposto la distruzione del materiale, della detenzione illecita ai sensi del-

l'art. 167, comma I, d.lgs. 196/2003, cfr. BUSIA, *Dimenticato l'uso improprio di materiale lecito*, *ibidem*, 26.

<sup>66</sup> GAMBARDILLA, *Il delitto di detenzione di atti relativi a intercettazioni illegali*, cit., 167 s.

<sup>67</sup> In questo senso, cfr. STRACUZZI, *Tabulati telefonici: senza norme attuative resta il rebus della conservazione dei dati*, cit., 93.

<sup>68</sup> Sul tema dell'inutilizzabilità rafforzata conseguente all'accertamento della natura «illegale» delle acquisizioni di dati

stante l'improprio utilizzo della locuzione « intercettazioni illegali », l'oggetto materiale della fattispecie delittuosa di recente conio deve restringersi al concetto di illiceità, che presuppone l'esistenza di materiale formato o raccolto attraverso la violazione di norme penali sostanziali che tutelano la riservatezza (art. 615-bis ss. c.p.) e dagli artt. 167 ss. del Codice della *privacy*.

In altri termini, la casistica legata all'inosservanza degli obblighi di conservazione e sicurezza dei dati relativi alle comunicazioni telematiche rivela un quadro confuso e contraddittorio<sup>69</sup>, per cui meriterebbe un intervento di razionalizzazione, da effettuarsi, in questo caso, ad opera del legislatore nazionale piuttosto che del suo omologo europeo.

## 6. CONCLUSIONI.

Il carattere transfrontaliero di molte modalità lesive di beni giuridici perpetrate attraverso la rete, le difficoltà legate alla individuazione del *locus commissi delicti*, la « spiritualizzazione » dello stesso fatto tipico delle fattispecie, nuove e vecchie, in vario modo collegate all'informatica ed alla telematica, rendono necessario un processo di armonizzazione dei reati su scala sovranazionale; in primo luogo, in ambito europeo, dove il lento ma progressivo ed inesorabile processo di integrazione ha reso possibile la predisposizione di strumenti di cooperazione in materia penale di significativa importanza, che acquista maggior senso proprio attraverso il decisivo ravvicinamento della disciplina di diritto sostanziale<sup>70</sup>; in secondo luogo, in ambito più esteso e tendenzialmente globale, anche se non si possono trascurare quelle perplessità derivanti dagli inconvenienti che un'intensa cooperazione fra Stati caratterizzati da differenti *standard* di tutela delle garanzie individuali può determinare proprio sul piano del rispetto del principio di proporzione e delle libertà fondamentali.

e notizie, cfr. C. CONTI, *Le intercettazioni « illegali »: lapsus linguae o nuova categoria sanzionatoria?*, in *Dir. pen. proc.*, 2007, 158 ss.

<sup>69</sup> Tale situazione si aggiunge ad un quadro, quello codicistico relativo alle intercettazioni di comunicazioni informatiche e telematiche (artt. 617-*quater* e *quinquies* c.p.) e alle altre violazioni della segretezza e riservatezza di dati e comunicazioni in tema di corrispondenza informatica o telematica (artt. 616, comma 4, nonché 621 e 623-bis c.p.), già caratterizzato dalla sovrapposizione quasi inestricabile di fattispecie incriminatrici e da notevoli disarmonie sanzionatorie, come ben dimostrato da PICOTTI, voce *Reati informatici*, in *Enc. giur.*, vol. agg. VIII, Roma, 2000, 23.

<sup>70</sup> Non si può, al riguardo, non men-

zionare, nell'ottica della creazione di uno spazio di giustizia « comune » all'interno dell'UE, l'importante decisione-quadro 13 luglio 2002/584/GAI del Consiglio dell'Unione europea sul mandato d'arresto europeo e le procedure di consegna tra Stati membri, cui l'ordinamento nazionale si è conformato con la l. 22 aprile 2005, n. 69, che prevede, all'interno delle fattispecie per le quali, in base all'art. 8, si fa luogo alla consegna obbligatoria in base al mandato d'arresto europeo, gran parte dei reati informatici e di quelli che possono realizzarsi attraverso condotte illecite via *Internet*: per un approfondimento sull'istituto del mandato d'arresto europeo, cfr. PANSINI-SCALFATI (a cura di), *Il mandato d'Arresto Europeo*, Napoli, 2005.