DIRITTO PENALE CONTEMPORANEO

LOTTA ALLA "CRIMINALITÀ INFORMATICA" E TUTELA DI "TRADIZIONALI" E "NUOVI" DIRITTI FONDAMENTALI NELL'ERA DI INTERNET*

di Roberto Flor

1. Introduzione.

Il nuovo millennio è stato caratterizzato dall'esplosione di Internet e dei nuovi prodotti tecnologici, che ha comportato dei cambiamenti epocali in ogni settore della vita umana.

Essi offrono molteplici opportunità di sviluppo, sul piano sociale, culturale ed economico, ma rappresentano altresì un terreno fertile per nuovi modi e tipi di comportamenti di rilievo penale, e dunque una nuova frontiera di lotta alla criminalità, che può offrire innovativi strumenti e mezzi per la ricerca delle prove e, in generale, per il contrasto a gravi fenomeni criminosi.

Il *cyberspace*, infatti, costituisce uno spazio virtuale in continua evoluzione che consente non solo la delocalizzazione delle risorse e la loro raggiungibilità, da parte dell'utente, da ogni luogo e distanza, anche grazie alle nuova dimensione del *cloud*[1] e della "struttura" del *web*, ma altresì la detemporalizzazione delle attività, che possono

*Testo italiano, rivisto ed integrato, del contributo destinato agli atti del convegno internazionale "Lo sviluppo delle scienze penalistiche alle soglie del nuovo millennio", Tirana, Albania, 20-21 aprile 2012.

[1] La nozione di *cloud computing* allude ad un insieme di tecnologie che permettono di memorizzare, archiviare e/o elaborare dati grazie all'utilizzo di risorse hardware/software delocalizzate in rete. Sia consentito il rinvio, anche per la definizione di *cloud computing*, a R. Flor, *Le prospettive de jure condendo del c.d. data retention nel cloud scenario, tra limiti ontologici, limiti costituzionali e tutela dei diritti fondamentali*, relazione presentata al convegno "Limiti convenzionali e costituzionali del 'Diritto Penale Europeo' dopo il Trattato di Lisbona – Il dibattito in Germania ed in Italia", Verona, 16-17 settembre 2011.

essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, senza che vi sia la necessità della presenza fisica della persona umana davanti allo schermo di un computer.

In questa costante evoluzione le manifestazioni criminose che si realizzano "in rete" hanno assunto nuove e differenti configurazioni, che trovano crescente rilievo offensivo ed allarmante impatto sociale e che necessitano di una risposta normativa.

Con l'entrata in vigore del Trattato di Lisbona la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale.

A livello europeo vi sono già concrete iniziative *in subiecta materia*, in particolare:

1. la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI del Consiglio, del 13 dicembre 2011[2];
2. la proposta di direttiva del Parlamento europeo e del Consiglio COM (2010)517 - C7-0293/2010 - 2010/0273(COD), relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI[3];
3. già prima dell'entrata in vigore del Trattato di Lisbona, le proposte di direttiva e di decisione quadro relative alle misure penali finalizzate ad assicurare il rispetto dei diritti di proprietà intellettuale[4];
4. nel settore della tutela dei diritti d'autore, oltre alle numerose iniziative non direttamente attinenti alla materia penalistica, ma che hanno portato la maggior parte degli Stati ad adottare anche strumenti penalistici di tutela (a partire dal Libro verde "Il diritto di autore e le sfide tecnologiche - Problemi di diritto di autore che richiedono un'azione immediata" del 1988) ed alle direttive a tutela del software, delle banche dati, nonché di attuazione agli obblighi internazionali derivanti dai trattati OMPI[5], si pensi al recente Libro Verde sulla *distribuzione online di opere audiovisive nell'Unione*

---

[2] Direttiva 2011/93/UE (e "Rettifica della direttiva 2011/92/UE del Parlamento europeo e del Consiglio"), del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (Gazzetta ufficiale dell'Unione europea L 335 del 17 dicembre 2011). Cfr. A Verri, *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE,* in *Dir. pen. cont.*, 28 marzo 2012.

[3] Proposta di direttiva del Parlamento europeo e del Consiglio COM (2010)517 - C7-0293/2010 - 2010/0273(COD), relativa agli attacchi contro i sistemi di informazione, che abroga la decisione quadro 2005/222/GAI.

[4] COM(2005) 276-1 definitivo, 2005/0127(COD), 2005/0128(CNS); SEC(2005)848 e, infine, COM(2006) 168 definitivo] di modifica della proposta di direttiva del Parlamento e del Consiglio relativa al rafforzamento del quadro penale per la repressione delle violazioni della proprietà intellettuale (2005/0127 COD), in attuazione della comunicazione della Commissione del 23 novembre 2005 [COM(2005) 583 definitivo] in merito alle conseguenze della sentenza del 13 settembre 2005 della Corte di Giustizia (C-176/03 Commissione contro Consiglio), relativa alla ripartizione di competenze fra primo e terzo pilastro. Sia consentito il rinvio a R. Flor, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Padova, 2010, 48 e ss.

[5] Su tali iniziative e sulle fonti e i modelli di tutela dei diritti d'autore basti il rinvio, in questa sede, a R. Flor, *Tutela penale e autotutela tecnologica*, cit., 12 e ss.; 253 e ss.; 315 e ss.; 364 e ss.

europea - Verso un mercato unico del digitale: opportunità e sfide[6], che evidenzia come il moltiplicarsi delle opportunità offerte dagli sviluppi tecnologici, in continuo movimento, incida sulla circolazione delle opere dell'ingegno (in particolare audiovisive). Gli spazi *on-line* sempre più si aprono alla condivisione delle risorse e tale scenario si arricchisce del "rapido sviluppo dei siti dei *social networks* e dei *social media*", basati sulla "creazione e sul caricamento di contenuti *online* da parte degli utenti"[7], che necessitano di risposte giuridiche adeguate;

5. la comunicazione della Commissione al Consiglio e al Parlamento europeo del 28 marzo 2012, su "Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica"[8], in cui si legge che la lotta alla criminalità informatica, il cui strumento giuridico principale è la Convenzione del Consiglio d'Europa sulla criminalità informatica, continua ad essere una priorità principale. È pertanto parte integrante del ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale e rientra tra gli sforzi intesi a sviluppare una strategia generale dell'UE per rafforzare la sicurezza informatica.

Tutte queste recenti iniziative sono connotate da due elementi comuni: 1) le potenzialità criminogene di Internet e, in generale, delle nuove tecnologie della comunicazione e dell'informazione; 2) la necessità di un intervento europeo e di una politica criminale europea nel contrasto alla criminalità informatica e, in generale, ai reati commessi in Internet o attraverso la rete.

2. Il "nuovo millennio" ed il passaggio dal *computer crime* al *cybercrime*.

La "criminalità informatica" non consiste in una categoria definita giuridicamente, anche se compare in fonti europee e sovranazionali[9]. Allo stesso modo

---

[6] COM(2011) 427 definitivo, del 13 luglio 2011, che si basa sulla strategia Europa 2020 (COM(2010) 245 del 19 maggio 2010), volta a promuovere una crescita intelligente, sostenibile e inclusiva a livello europeo, sull'agenda digitale europea e sulla comunicazione della Commissione "Un mercato unico per i diritti di proprietà intellettuale" (COM(2011) 287 definitivo, 24 maggio 2011).

[7] COM(2011) 427 definitivo. L'esponenziale crescita e diffusione dei *social networks* (SNs) in Internet, infatti, non solo determinano un sensibile cambiamento nelle modalità di intraprendere e di interpretare i rapporti sociali, economici, culturali e politici, ma offrono altresì nuove opportunità per violare la proprietà intellettuale.

[8] COM(2012) 140 final.

[9] Si veda già M. Briat, U. Sieber (eds.) *Computer Related Criminality: Analysis of Legal Policy in the OECD-Area*, Parigi 1986. Cfr. le Raccomandazioni n. R (89) 9 - sui profili di diritto penale sostanziale concernenti la lotta alla criminalità informatica - e n. R (95) 13, relativa ai problemi di procedura penale legati alla tecnologia dell'informazione; Convenzione *Cybercrime* adottata a Budapest il 23 novembre 2001; la direttiva 95/46/CE sulla tutela dei dati personali, nonché le direttive successive adottate in questo settore; le direttive in materia di protezione dei diritti d'autore e, in particolare, la direttiva 2001/29/CE; la direttiva 2000/31/CE sul commercio elettronico, le decisioni quadro contro gli attacchi informatici (2005/222/GAI), contro lo sfruttamento sessuale di minori e la pedopornografia (2004/68/GAI), contro il terrorismo (2002/475/GAI, parzialmente riformata dalla decisione 2008/919/GAI); sul piano processuale vedi quelle

non si rinviene una definizione internazionalmente riconosciuta di "*computer crime*" o "*computer related crime*" o "*cybercrime*"[10].

Sul piano empirico, essa abbraccia una molteplicità di comportamenti lesivi di interessi penalmente rilevanti, riconducibili ai "*reati informatici*", introdotti in molti ordinamenti nazionali.

Sul piano fenomenico si è assistito, dopo l'"esplosione" di Internet, al passaggio dalla dimensione "privata" o "individuale" del computer e delle delimitate reti di computer alla dimensione "pubblica" o "collettiva" dei sistemi, basati sull'interconnettività globale.

Nell'attuale società dell'informazione il fenomeno "*criminalità informatica*" risulta essere dunque flessibile ed aperto a fatti criminosi che possono essere commessi attraverso la rete o nel *cyberspace*.

Sul piano del diritto penale sostanziale, la "*criminalità informatica*" può includere sia fattispecie legali costruite, sul piano della formulazione, con *elementi di tipizzazione* connessi a procedimenti di *automatizzazione* di dati o informazioni, ovvero legate a modalità, oggetti o attività di carattere tecnologico (*reati informatici* in senso stretto) [11], sia tutte quelle fattispecie incriminatrici "comuni" che, pur *non* presentando espressamente elementi tipici caratterizzati dalla tecnologia, possono essere applicate a fatti commessi tramite la tecnologia, la rete o nel *cyberspace*[12] (reati informatici in senso lato).

In questo contesto assume rilevanza anche la distinzione fra reati cibernetici in senso stretto e reati cibernetici in senso lato.

---

sul mandato d'arresto europeo (2002/584/GAI) e sull'applicazione del principio del reciproco riconoscimento delle decisioni di confisca (2006/783/GAI), che includono la "*criminalità informatica*" nelle liste di reati per cui si prescinde, in conformità con il principio del mutuo riconoscimento, dal requisito della doppia incriminazione per l'esecuzione diretta dei provvedimenti emessi dall'autorità giudiziaria dello Stato richiedente. Vedi per tutti 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. Nella letteratura tedesca, anche sul richiamo alle fonti sovranazionali e sulle nuove competenze penali dell'Unione Europea, basti il rinvio a U. Sieber, *Computerkriminalität*, in U. Sieber, F. H. Brüner, H. Satzger, B. Von Heintschel-Heinegg (Hrsg), *Europäisches Strafrecht*. Baden-Baden, 2011, 393 e ss.

[10] Vedi M. F. Weismann, *International Cybercrime: Recent Developments in the Law*, in R. D. Clifford (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011, 257, 258.

[11] Si pensi, nell'ordinamento italiano, all'accesso abusivo a sistemi informatici (art. 615 ter c.p.) o alla frode informatica (art. 640 ter c.p.). Questa categoria di reati informatici si connota per un nuovo *oggetto passivo* su cui la condotta va a cadere (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure dal fatto che il computer ed i prodotti informatici in genere costituiscono lo *strumento* tipico di realizzazione del 'fatto' criminoso. Così L. Picotti, *La nozione di "criminalità informatica"*, cit.

[12] Si consideri, nel sistema italiano, la truffa comune (art. 640 c.p.), che può essere commessa attraverso l'invio di email ingannevoli che inducono in errore il destinatario determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti *online*. Oppure si pensi alla diffamazione *online*, o alle forme di manifestazione o diffusione del pensiero o di contenuti illeciti, quale la rivelazione od agevolazione "*in qualsiasi modo*" della conoscenza, da parte di terzi non legittimati, di una notizia che debba rimanere segreta. Su tali categorie si veda L. Picotti, *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique*, in *Rev. Int. Droit pénal*, 2006, n. 3/4, 525 s.

Nei primi l'elemento tecnologico e specializzante è caratterizzato proprio dalla *connessione* in rete o dalla fruibilità del *cyberspace*.[13]

I secondi, invece, presentano modalità o possibilità di realizzazione concreta "in rete" e sono formulati in termini più generali ed elastici, tanto da essere realizzabili o concepibili a prescindere dall'informatica e dalla rete[14].

Questa impostazione teorica trova un riscontro nelle disposizioni di carattere processuale previste dalla Convenzione sulla criminalità informatica del Consiglio d'Europa, che si applicano non solo ai reati da essa previsti (artt. 2-11), ma anche a tutti gli illeciti commessi attraverso i sistemi informatici ed a quelli per il cui accertamento è necessaria la raccolta della prova elettronica (ex art. 14 della Convenzione).

Una parte della dottrina americana ritiene che la categoria "*cybercrime*" comprenda almeno tre sub-categorie: reati in cui il computer o il sistema informatico costituiscono l'obiettivo delle attività criminali; reati in cui il computer e, in generale, le nuove tecnologie ed Internet, rappresentano gli strumenti per commettere o preparare un reato; reati in cui il sistema informatico e la rete costituiscono solo un "aspetto incidentale" nella commissione dell'illecito[15].

3. Investigazioni "a carattere tecnologico", tutela dei diritti fondamentali e limiti all'intervento penale nella giurisprudenza costituzionale di alcuni Stati stranieri.

3.1. Cenni alla nuova direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

L'innovazione-rivoluzione tecnologica offre anche nuovi strumenti e mezzi per la ricerca delle prove, e consente di perseguire altresì fini "preventivi". La concreta esigenza di misure efficaci di contrasto a gravi forme di criminalità vale anche rispetto a reati "tradizionali", che trovano nelle nuove tecnologie un essenziale ausilio per la loro realizzazione. Si pensi solo alle attività preparatorie di attentati terroristici, che possono trovare in Internet un formidabile mezzo di comunicazione e di pianificazione

---

[13] Si pensi, ad esempio, agli artt. 171, lett. a) bis e 171 ter, co. 2, lett. a) bis della l. n. 633/41 (che sanzionano la diffusione abusiva tramite l'immissione in un sistema di reti telematiche di un'opera dell'ingegno protetta). Su tali reati si consenta di rinviare a R. Flor, *Tutela penale e autotutela tecnologica*, cit., 329 e ss.

[14] Cfr. ancora L. Picotti, *La nozione di "criminalità informatica"*, cit.

[15] Vedi S. Brenner, *Defining Cybercrime: A Review of Federal and State Law*, in R. D. Clifford (ed.), *Cybercrime*, cit., 15-104, 17, cui l'Autrice si chiede se la categoria "*cybercrime*" abbracci nuove forme di criminalità e di crimini, ovvero se non si tratti piuttosto di "vecchio vino in nuove bottiglie" ("*old wine in new bottles*"). In verità questa espressione non è così distante da quella utilizzata da Barlow - "*Selling wine without bottles*" - con la quale quest'ultimo Autore intendeva rappresentare il nuovo scenario dominato dalla tecnologia, che ha determinato la trasformazione dell'architettura tipica su cui poggiava la tutela del diritto d'autore, e la crisi del sistema di tutela della proprietà intellettuale, dovuta alla proliferazione sia di fenomeni criminosi nuovi, che di "vecchi" fenomeni realizzati con nuovi strumenti [Internet]. Vedi J.P. Barlow, *Selling Wine without Bottles: The Economy of Mind on the Global Net*, in P. Ludlow (ed.), *High Noon on the Electronic Frontier, Conceptual Issues in Cyberspace*, III ed., MIT, 1999, 9 e ss., citato da R. Flor, *Tutela penale e autotutela tecnologica*, cit., 250.

degli attacchi, oppure alla lotta contro la diffusione di materiale pedopornografico *online*.

In questo ultimo settore il legislatore europeo, con la nuova direttiva in materia penale relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile ha previsto, all' art. 15, co. 3, che gli Stati adottino tutte le misure necessarie per assicurare che le investigazioni, in questo settore, avvengano con mezzi adeguati ed effettivi, "al pari della lotta alla criminalità organizzata o ad altri gravi reati". Il successivo co. 4 dispone, inoltre, che gli Stati assicurino l'individuazione degli autori dei reati e delle vittime anche tramite l'analisi di immagini o prodotti audio video trasmessi o resi disponibili attraverso le tecnologie dell'informazione e della comunicazione.

L'art. 25 della stessa direttiva prevede che gli Stati adottino le misure necessarie per assicurare la tempestiva rimozione delle pagine *web* contenenti immagini pedopornografiche, che abbiano *host* nel proprio territorio, ma con la possibilità di richiedere la stessa misura anche al di fuori dei limiti territoriali.

Gli Stati, inoltre, possono adottare misure di blocco di accesso degli utenti alle pagine web contenenti materiali pedopornografici.

La direttiva dispone che tale strumento deve essere predisposto attraverso una procedura trasparente e prevedere delle *safeguards* per garantire che la restrizione sia limitata, necessaria e proporzionata, nonché il diritto dell'utente ad essere informato del motivo della restrizione. Tale procedura dovrebbe altresì garantire il ricorso giudiziario avverso al provvedimento che dispone il blocco dell'accesso.

In sintesi, si tratta di strumenti specifici predisposti per la lotta al fenomeno della pedopornografia *online,* adattabili alle esigenze repressive e preventive di attività criminose che trovano nel *cyberspace* l'ambiente esclusivo ed ideale di manifestazione.

La regolamentazione di tali mezzi e la loro utilizzazione in concreto non può però prescindere dal bilanciamento con altri interessi contrapposti, a partire dai diritti fondamentali dell'individuo.

Tale bilanciamento presuppone l'individuazione di elevati standard comuni o condivisibili dagli Stati, almeno a livello europeo, che possono essere ricavati da importanti decisioni di Corti Costituzionali europee, nonché da una recente sentenza della Corte di Giustizia e che devono confrontarsi con le esigenze di accertamento e di ricerca della prova ed il rispetto di "nuove" manifestazioni dei diritti inviolabili dei cittadini, quali il diritto all'integrità, sicurezza e riservatezza dei sistemi informatici ed il diritto all'autodeterminazione informativa, da elevare ad espressioni di "tradizionali" diritti fondamentali, in particolare da ricondurre alle manifestazioni dei diritti della personalità[16].

---

[16] Sul dibattito contemporaneo si consenta di rinviare a R. Flor., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung in Riv. trim. dir. pen. ec.*, 3 , 2009 , 695 e ss., nonchè a ID., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention,* in *Ciberspazio e diritto*, 11, 2 , 2010 , 359 e ss. (con ampi riferimenti bibliografici). Con riguardo alla lotta al *cyber*-terrorismo vedi già U. Sieber., P. Brunst, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of*

3.2. Le sentenze delle Corti Costituzionali tedesca, rumena e ceca (cenni).

In questo complesso contesto le sentenze del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *Online Durchsuchung*[17] e del 2 marzo 2010 sul c.d. *Data retention*[18] costituiscono senza dubbio due decisioni epocali.

Con la prima pronuncia la Corte Costituzionale tedesca ha dichiarato incostituzionale il § 5 co. 2, n. 11, della Legge sulla protezione della Costituzione del *Nord Reno Westfalia* (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen* - VSG - come modificato il 20 dicembre 2006), in materia di raccolta e trattamento dei dati degli utenti, in specie in/da sistemi informatici ed attraverso la rete.

Con la seconda decisione, invece, il *Bundesverfassungsgericht* ha dichiarato incostituzionali i §§ 113a e 113b del *Telekommunikationsgesetz* (TKG, come modificato dall'art. 2, n. 6 della legge di riforma del settore delle telecomunicazioni e delle altre misure d'indagine sotto copertura, in attuazione della direttiva 2006/24/CE, che ha modificato la direttiva 2002/58/CE) ed il § 100g StPO, co. 1, prima parte, in quanto in contrasto con l'art. 10 co. 1 del *Grundgesetz* (GG) [19].

International Conventions, in Council of Europe (ed.), *Cyberterrorism – the use of the Internet for terrorist purposes,* Strasbourg, Council of Europe Publishing, 2007, 9 e ss.; P. Brunst., *Terrorism and the Internet, in* M. Wade, A. Maljevic (eds.), *A War on Terror? The European Stance on a new threat, changing laws and human rights implications,* New York, 2009, 51 e ss.; ID., *Legal Aspects of Cyber Terrorism, in* Centre of Excellence – Defence Against Terrorism (ed.), *Legal Aspects of Combating Terrorism,* Amsterdam, NATO Science for Peace and Security Series, 2008, 63 e ss.; ID., *Use of the Internet by Terrorists – A Threat Analysis, in* Centre of Excellence – Defence Against Terrorism (ed.), *Responses to Cyber Terrorism,* Amsterdam, IOS Press, NATO Science for Peace and Security Series, 2008, 34 e ss.

[17] BVerfG 370/07 –595/07, 27.2.2008, in *CR*, 2008, 306 e ss. Per un primo commento si consenta il rinvio a R. Flor, *Brevi riflessioni*, cit., 695 e ss.

[18] Vedi 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html. Per un primo commento si consenta il rinvio a R. Flor, *Investigazioni ad alto contenuto tecnologico*, cit., 359 e ss.

[19] Vedi 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html. Cfr. R. Flor, *Indagini ad alto contenuto tecnologico,* cit., 359 e ss. Vedi anche R. Flor, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constituțională*, in Cass. pen., 5, *2011, 1952 – 1969.* In Italia, ex art. 132 D.lgs. n. 196 del 2003, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. Entro tale termine, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391 quater c.p.p. (che prevede la richiesta di documentazione alla pubblica amministrazione e stabilisce che in caso di rifiuto può essere chiesto al pubblico ministero il sequestro dei documenti), ferme restando le condizioni di cui all'art. 8, co. 2, lett. f) (in base al quale i diritti dell'interessato di accesso ai dati, ex art. 7 del Codice Privacy, non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'art. 145 dello stesso codice, se i trattamenti di dati personali sono effettuati da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni

In questo caso si trattava di norme adottate anche per rispondere alle minacce del terrorismo internazionale[20], che prevedevano l'obbligo di conservazione dei dati di traffico telefonico e telematico per un periodo di sei mesi, senza distinzioni rispetto ai presupposti di fatto inerenti alla commissione o preparazione di reati.

La sentenza della *Curtea Constituţională della* Romania del 8 ottobre 2009[21] ha affrontato alcune questioni simili a quelle trattate da quest'ultima decisione del *Bundesverfassungsgericht*.

Infine, con la sentenza del 31 marzo 2011 la Corte Costituzionale della Repubblica Ceca ha dichiarato incostituzionali le disposizioni interne di trasposizione delle direttive europee in materia di obblighi di conservazione dei dati di traffico telefonico e telematico, richiamando espressamente, nelle motivazioni, le precedenti sentenze delle Corti Costituzionali tedesca e rumena[22].

Tutte queste decisioni sono caratterizzate da una linea argomentativa comune basata sulla questione della legittimazione di metodologie tecniche di investigazione, di archiviazione dei dati e delle informazioni o di controllo ed intervento sull'operato dell'utente, anche quale modello "alternativo" di protezione dei beni giuridici, rispetto alla tutela dei diritti fondamentali dell'individuo e, più in particolare, della sfera esclusiva di estrinsecazione della sua personalità.

Alla recente sentenza della Corte di Giustizia del 24 novembre 2011 dovrà essere dedicato, invece, uno specifico paragrafo[23].

3.3. Gli elementi argomentativi comuni dei Giudici delle Leggi.

Dalle motivazioni delle decisioni del *Bundesverfassungsgericht* (2008 e 2010), della *Curtea Constituţională (2009) e della Corte Costituzionale delle Repubblica Ceca (2011)* è possibile ricavare alcuni elementi comuni.

---

telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive) per il traffico entrante. Sul riconoscimento costituzionale del diritto all'autodeterminazione informativa vedi anche la recente sentenza della Corte Costituzionale tedesca 1 BvR 1299/05, del 24 gennaio 2012, che ha dichiarato incostituzionali alcune disposizioni del *Telekommunikationsgesetz* del 22 giugno 2004 (*Bundesgesetzblatt*, 1190) in materia di accesso a dati personali, *passwords* e *pin* da parte di uffici di pubblica sicurezza, pubblici ministeri e servizi di informazioni. Vedi http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html. La decisione del 27 febbraio 2008 ha ispirato, con riferimento a natura e "dimensione" dei diritti fondamentali compromessi, la sentenza del *Bundesverfassungsgericht* sul c.d. *data retention*, che è stata a sua volta richiamata dalla sentenza della Corte Costituzionale della Repubblica Ceca, del 31 marzo 2011. Si consenta di rinviare in merito a R. Flor, *Data retention rules under attack in the European Union?*, in *Illyrius*, 1, 2012, 69-86.

[20] BGBl I S. 3083, 25 dicembre 2008.

[21] Cfr. *Decizia* 1258 del 8 ottobre 2009, in *Monitorul Oficial* n.798 – 23 novembre 2009. Su tale decisione basti il rinvio a J. Rinceanu, *Das Urteil des rumänischen Verfassungsgerichtshofs zur Verfassungswidrigkeit der Vorratsdatenspeicherung*, in *Jahrbuch für Ostrecht*, 2011, 1/52, 49 - 57.

[22] Vedi ampiamente R. Flor, *Data retention rules*, cit., 69-86.

[23] C-70/10. Su questioni analoghe vedi Corte Giustizia - Grande sezione - Sent. 29 gennaio 2008 (C-275/06); Corte Giustizia - sez. VIII, ord. 19 febbraio 2009 (C-557/07), entrambe in R. Flor, *Tutela penale e autotutela tecnologica*, cit., 423 e ss., che riporta anche il c.d. "caso Peppermint".

In tutte le sentenze i Giudici delle Leggi hanno considerato la distinzione fra le opportunità fornite dall'evoluzione tecnologica nella lotta alla criminalità ed i presupposti per il loro legittimo utilizzo. [24]

In primo luogo è innegabile il riconoscimento, esplicito o implicito, del ruolo essenziale dei *service providers*, che possono svolgere attività anche di rilevanza pubblica[25]. Pertanto, i limiti e le garanzie legate allo svolgimento di tali operazioni non possono essere lasciati al loro apprezzamento soggettivo, ma devono essere previsti dal legislatore.

In secondo luogo, considerate le potenzialità della rete non poteva non rilevare la funzione preventiva di innovativi strumenti di indagine e l'utilità pratica, nell'ambito dei procedimenti penali o di attività investigative, dell'archiviazione dei dati degli utenti relativi al traffico telematico[26].

In terzo luogo, le Corti hanno affrontato la questione della legittimazione dei mezzi di indagine, di archiviazione e di controllo dei dati di traffico telematico rispetto alla tutela dei diritti fondamentali della persona, giungendo alla [ovvia] conclusione che non sussiste un divieto assoluto di adottare soluzioni legislative limitative di tali diritti.

La qualificazione degli interventi pubblici nella sfera dei diritti individuali, però, deve non solo essere prevista dalla legge, ma la restrizione non deve eccedere un limite di stretta necessità rispetto a taluni fini essenziali alla vita di una società democratica, tra i quali è compresa l'individuazione e la punizione di colpevoli di gravi reati.

Interventi legislativi che possono comprimere in modo proporzionato i diritti fondamentali dovrebbero considerarsi legittimi solo se diretti alla tutela di importanti e predominanti beni giuridici. Il legislatore dovrebbe, dunque, operare un bilanciamento fra gli interessi contrapposti ed adottare una norma chiara e precisa, assicurando il

---

[24] Le prime hanno in genere natura neutra, mentre sono la loro "destinazione d'uso" e "modalità di attuazione", fra le molteplici applicabili, ad assumere rilievo giuridico. Così R. Flor, *Brevi riflessioni*, cit., a cui si consenta di rinviare per ulteriori riferimenti bibliografici.

[25] L'importanza del ruolo dell'ISP e della necessità di tutela dei diritti fondamentali è rinvenibile anche nelle linee guida *Human rights guidelines for Internet service providers*, sviluppate dal *Council of Europe* in cooperazione con l' *European Internet Services Providers Association* – (EuroISPA). Si consenta ancora il rinvio a R. Flor, *Tutela penale e autotutela tecnologica*, cit., 418 e ss. Sul ruolo dell'ISP nell'ambito delle attività di indagine si vedano, per quanto riguarda l'ordinamento italiano, gli artt. 14, 15, 16 e 17 del D.lgs 70/2003, di attuazione della Direttiva 2000/31/Ce sul commercio elettronico, che prevedono degli obblighi di cooperazione con l'autorità giudiziaria o amministrativa e di intervento per porre fine alle violazioni commesse nell'ambito di un servizio di accesso alla rete, ovvero di trasmissione, di memorizzazione automatica, intermedia e temporanea di informazioni fornite da un destinatario del servizio.

[26] Il *Bundesverfassungsgericht*, nella sentenza sulla c.d. *Online Durchsuchung*, non solo ha fatto riferimento alla possibilità di utilizzare Internet e le nuove tecnologie per la preparazione di attentati terroristici, ma ha anche evidenziato l'utilità preventiva del monitoraggio segreto della rete e dell'accesso segreto a sistemi informatici. E'utile ricordare, inoltre, che la sentenza della Corte Costituzionale tedesca sul c.d. *data retention* è giunta in un momento storico in cui le norme introdotte dal legislatore tedesco erano volte ad adeguare le misure di contrasto a questo fenomeno al mutato contesto comunicativo globale. Si veda, fra tutti, U. Sieber, *Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten"*, in *NStZ*, 2009, 353 - 364.

controllo sui presupposti relativi all'adozione di un atto "invasivo" ad un'autorità indipendente (*rectius* "un giudice terzo").

Infine, tutte le decisioni richiamano, seppur in modi diversi, la necessaria adozione di una regola che preveda *standards* di certezza, determinatezza e trasparenza elevati, ossia che stabilisca in modo preciso e stringente i presupposti per la compressione dei diritti fondamentali coinvolti, la cui valutazione deve essere attribuita ad un organismo indipendente (in una fase anteriore e/o successiva all'adozione delle misure investigative o di archiviazione e controllo).

E' necessario aggiungere che le Corti Costituzionali ceca e rumena hanno richiamato il riconoscimento internazionale del diritto alla riservatezza ed alla vita famigliare, protetto dall'art. 12 della Dichiarazione universale sui diritti dell'uomo, dall' art. 17 del Patto internazionale relativo ai diritti civili e politici e dall'art. 8 CEDU[27], affermando che né la Convenzione per la tutela dei diritti dell'uomo e delle libertà fondamentali né le Costituzioni nazionali vietano soluzioni legislative limitative dei diritti fondamentali. Tali limiti, però, sono legittimi se rispettano specifici requisiti, espressamente richiesti dall'art. 8 CEDU, e se l'intervento legislativo è diretto alla tutela di importanti interessi, quali possono essere la sicurezza nazionale, la salute pubblica, la difesa dell'ordine pubblico, oppure "la prevenzione dei reati". E detto intervento, però, deve essere necessario, proporzionato rispetto alla situazione che lo ha determinato, applicabile in modo non discriminatorio e non deve minare l'esistenza del diritto o della libertà fondamentale. Sotto quest'ultimo aspetto la Corte Costituzionale ceca ha richiamato espressamente le sentenze del *Bundesverfassungsgericht* e della Corte Costituzionale rumena sul *data retention*.[28]

In verità il *Bundesverfassungsgericht*, nella citata sentenza sul *data retention*, ha altresì evidenziato sia le potenzialità che le vulnerabilità dei sistemi informatici di archiviazione, anche in relazione alla natura dei dati ivi memorizzati. A parere dei Giudici tedeschi l'adozione di misure di sicurezza proporzionate che assicurino uno

[27] Sul piano del riconoscimento internazionale del diritto fondamentale alla riservatezza, infatti, l' art. 12 della Dichiarazione universale dei diritti dell'uomo, del 10 dicembre 1948, prevede che nessun individuo può essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, nè a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni. Il Patto internazionale sui diritti civili e politici delle Nazioni Unite del 1966, all'art. 17 dispone che nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. La Carta dei diritti fondamentali dell'Unione Europea (2000/C 364/01) all'art. 7 tutela il rispetto della vita privata e della vita familiare, sancendo che ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni. Il successivo art. 8 nel prevedere le specifiche garanzie per la protezione dei dati di carattere personale, al co. 3 dispone che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. L'art. 8 **(**Diritto al rispetto della vita privata e familiare) CEDU stabilisce che ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. "Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui".

[28] Cfr. su questo punto R. Flor, *Data retention rules*, cit.

standard elevato di sicurezza non può essere lasciata all'apprezzamento soggettivo del *provider* o a mere valutazioni economiche, ma deve essere il legislatore a determinare in modo trasparente i presupposti, il tipo, la natura ed il livello delle misure di sicurezza, nonché i limiti di utilizzazione dei dati, eventualmente ricorrendo all'istituzione di un organismo *ad hoc* per la regolamentazione degli standard tecnici [29].

4. La sentenza della Corte di Giustizia dell'Unione europea in materia di tutela dei diritti d'autore in Internet.

Una particolare attenzione merita la recente sentenza Corte di Giustizia dell'Unione europea [30], la quale ha affermato che l'ingiunzione diretta, da parte di un giudice ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing* in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato i diritti e le libertà tutelati dagli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea e dai corrispondenti artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[31], oltre che la libertà di impresa (*ex* art. 16 della Carta).

Questa "corrispondenza" è stata evidenziata dall'avvocato generale Pedro Cruz Villalón nelle conclusioni presentate il 14 aprile 2011, in cui ha proposto la riformulazione della questione nei termini che seguono. Il giudice del rinvio aveva

---

[29] In effetti l'ISP non è obbligato a seguire le indicazioni degli esperti in un dato momento storico in ordine alle misure idonee a garantire la sicurezza dei dati (archiviazione separata per tipologie di dati, criptazione asimmetrica, principio dei "quattro occhi" in congiunzione con procedure di autenticazione avanzate per l'accesso alle chiavi, *audit – proof recording* dell'accesso e cancellazione dei dati). Nemmeno vi è un sistema equilibrato di sanzioni che attribuisca rilevanza alle violazioni della sicurezza dei dati rispetto alle violazioni dei doveri di immagazzinamento, salvo in alcuni specifici settori. In Italia, ad esempio, si fa riferimento al D.lg. n. 196 del 2003, che prevede obblighi di adozione di misure di sicurezza minime, la cui inosservanza fa scattare la sanzione penale (in questo caso la contravvenzione di cui all'art. 169 del Decreto). Si tratta, però, di obblighi riguardanti misure di sicurezza "minime" e "idonee" che non corrispondono agli "elevati standard" richiesti dalla Corte Costituzionale tedesca.

[30] Corte di Giustizia dell'Unione europea, 24 novembre 2011 (C-70/10). Il medesimo principio è stato applicato anche dalla Corte di Giustizia in una più recente sentenza, del 16 febbraio 2012 (Corte di Giustizia dell'Unione europea, C 360/10, caso "SABAM v. Netlog"). In quest'ultimo caso i Giudici hanno ribadito che il gestore di *social network*s non può essere costretto a predisporre un sistema di filtraggio generale, riguardante tutti i suoi utenti, per prevenire l'utilizzo illecito di opere musicali e audiovisive. Tale obbligo comporterebbe una invasione sproporzionata nel diritto alla riservatezza degli utenti ed alla libertà di impresa.

[31] Su nuove tecnologie e possibile ampliamento della nozione di "domicilio" nella Convenzione vedi G. Marotta, *Innovazioni tecnologiche e diritto al rispetto del domicilio nella Convenzione europea*, in *Riv. dir. internaz.*, 2005, 4, 1044 e ss. Su CEDU e ordinamento penale italiano basti il rinvio a E. Nicosia, *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino, 2006, nonché a V. Manes, V. Zagrebelsky (cur.), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011; in particolare, sui rapporti con il diritto comunitario e con la Carta dei diritti fondamentali dell'Unione europea vedi, rispettivamente, C. Sotis, *Convenzione europea dei diritti dell'uomo e diritto comunitario*, ivi, 109 e ss. e S. Manacorda, *Carta dei diritti fondamentali dell'Unione europea e CEDU: una nuova topografia delle garanzie penalistiche in Europa?*, ivi, 147 e ss. Sui diritti fondamentali come oggetto della tutela penale si veda F. Viganò, *Obblighi convenzionali di tutela penale?*, ivi, 243 e ss.

formulato la sua prima questione pregiudiziale quale interpretazione di varie disposizioni del diritto derivato dell'Unione «alla luce degli artt. 8 e 10 della CEDU». Ex art. 6, n. 3, TUE, «[i] diritti fondamentali, garantiti dalla [CEDU] (…) fanno parte del diritto dell'Unione in quanto principi generali». Anzitutto, il medesimo art. 6 TUE inizia precisando, al n. 1, primo comma, che la Carta «ha lo stesso valore giuridico dei trattati», come la Corte non ha mancato di sottolineare negli ultimi sviluppi della sua giurisprudenza. «Poiché i diritti, le libertà e i principi enunciati nella Carta hanno quindi, di per sé stessi, un valore giuridico, oltretutto di primo rango, il ricorso ai principi generali sopra menzionati non è più necessario, nei limiti in cui i primi possono identificarsi nei secondi». Questo è stato dunque un primo elemento a favore dell'esame della questione alla luce delle disposizioni della Carta, piuttosto che con riferimento a quelle della CEDU. Inoltre, l'art. 52, n. 3, della Carta prevede che «[l]addove [essa] contenga diritti corrispondenti a quelli garantiti dalla [CEDU], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione», restando inteso che «[tale] disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa». Orbene, secondo l'avvocato generale «nelle circostanze della causa principale, i diritti garantiti dall'art. 8 della CEDU corrispondono, ai sensi dell'art. 52, n. 3, della Carta, a quelli garantiti dagli artt. 7 (Rispetto della vita privata e della vita familiare) e 8 (Protezione dei dati di carattere personale) della Carta, così come i diritti garantiti dall'art. 10 della CEDU corrispondono a quelli garantiti dall'art. 11 della Carta (Libertà di espressione e d'informazione), nonostante le differenze relative, rispettivamente, alle formulazioni impiegate e alle nozioni utilizzate». L'avvocato generale ha pertanto proposto di modificare la questione del giudice del rinvio sostituendo il riferimento agli artt. 8 e 10 della CEDU con quello agli artt. 7, 8 e 11 della Carta, in combinato con l'art. 52, n. 1, della stessa, come interpretati, ove necessario, alla luce degli artt. 8 e 10 della CEDU.

Con tale decisione la Corte di Giustizia "valorizza" i diritti fondamentali che possono trovare manifestazione nel *cyberspace*, di cui la stessa riservatezza informatica costituisce espressione, per garantire la sua prevalenza nel bilanciamento con le esigenze di tutela (nel caso di specie) della proprietà intellettuale in Internet.

Ad una più attenta lettura, inoltre, l'interesse a determinare il "destino" delle aree informatiche in cui si manifesta la personalità umana è simile alla definizione del *Recht auf informationelle Selbstbestimmung* che è stato affermato dalla giurisprudenza costituzionale tedesca.

5. Conclusioni.

La corrispondenza delle previsioni della CEDU con quelle della Carta dei diritti fondamentali dell'Unione europea, da un lato, non preclude che il diritto dell'Unione conceda una protezione più estesa.

Dall'altro lato, se la rilevanza degli interessi da proteggere è tale da giustificare la compressione dei menzionati diritti, la limitazione dovrebbe non solo essere

connotata da uno scopo legittimo, ma anche risultare idonea, necessaria ed opportuna quale mezzo per il raggiungimento di questo scopo.

Il principio di proporzione costituisce, in questo senso, il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte politico normative del legislatore, delimitandone l'area di discrezionalità.

Le importanti sentenze delle Corti Costituzionali tedesca, rumena e ceca, nonché quella della Corte di Giustizia, sembrano confermare la nascita di nuove forme di manifestazione dei diritti generali della personalità, che possono essere ricondotte al diritto all'autodeterminazione informativa ed al diritto alla riservatezza ed alla sicurezza dei dati e dei sistemi informatici.

Il primo conferisce alla persona il potere di determinare, da un lato, il trattamento dei dati e delle informazioni ad essa attinenti, ampliando la tutela del diritto fondamentale alla libertà della vita privata e, dall'altro lato, il "destino" delle "aree informatiche" (*cyberspace*) in cui si manifesta la personalità umana.

Il secondo, invece, garantisce l'interesse a non subire indebite interferenze nella sfera di rispetto e disponibilità di "spazi informatici", indipendentemente dalla qualità (natura) o dalla quantità di dati e informazioni o dalla natura o dimensione dello spazio informatico di pertinenza del o dei soggetti "titolari", nonché di tutelare l'integrità e la riservatezza dei dati e dei sistemi informatici assicurando così la correttezza e l'affidabilità dei rapporti giuridici che si instaurano nel *cyberspace*.

Le motivazioni delle citate sentenze sembrano esprimere la convergenza verso valori condivisi che connotano la società di Internet e che attingono a tradizioni comuni degli Stati dell'Unione.

Questi "valori comuni" influiscono in modo determinante nella lotta al fenomeno "criminalità informatica", che può essere condotta con successo solo se alle incriminazioni minime adottabili dall'Unione europea, ex art. 83 TFUE, si affiancano misure processuali e pre-processuali efficaci di contrasto che rispettino il nucleo essenziale dei diritti fondamentali.

Un primo (timido) passo è stato effettuato grazie alla direttiva contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che prevede disposizioni relative al blocco dell'accesso a *websites* e la rimozione delle pagine contenenti immagini pedopornografiche.

Gli *standards* normativi ed applicativi ricavabili dalle decisioni delle Corti sinora esaminate possono però già costituire un primo punto di riferimento per il legislatore europeo, che può trovare in esse delle importanti linee guida nel bilanciamento fra contrapposti interessi e in prospettiva di tutela di quel nucleo essenziale minimo dei diritti fondamentali, richiesta dall'art. 52 della Carta, delimitando l'area dell'intervento penale e contribuendo a definire le garanzie che devono essere legate alla legittima intromissione nel godimento dei diritti fondamentali per la repressione e la prevenzione almeno di gravi reati contro predominanti beni giuridici.