FRANCESCA RUGGIERI - LORENZO PICOTTI
(a cura di)

Nuove tendenze della giustizia penale di fronte alla criminalità informatica

Aspetti sostanziali e processuali

G. GIAPPICHELLI EDITORE – TORINO

Francesca Ruggieri - Lorenzo Picotti
(a cura di)

Nuove tendenze della giustizia penale di fronte alla criminalità informatica

Aspetti sostanziali e processuali

Atti del Convegno
Como, 21-22 maggio 2010

G. Giappichelli Editore – Torino

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-348-1877-0

La presente pubblicazione viene edita nell'ambito del Progetto di Rilevante Interesse Nazionale (PRIN) 2007-2009 e con il sostegno della Sezione Giovani Penalisti del Gruppo Italiano dell'Association Internationale de Droit Pénal.

Indice

pag.

pag.

pag.

Gli Autori

Diego Buso è Direttore della Divisione Seconda del Servizio Polizia Postale e delle Comunicazioni.

Francesco Cajani è Pubblico Ministero presso la Procura di Milano, *pool* reati informatici, nonché punto di contatto italiano di Eurojust per la criminalità informatica.

Eleonora Colombo è Dottoranda di ricerca in Diritto processuale penale presso l'Università degli Studi dell'Insubria.

Marcello Daniele è Professore associato di Procedura penale comparata presso l'Università di Padova.

Domenico De Natale è Assegnista di ricerca in Diritto penale presso la Facoltà di Giurisprudenza dell'Università degli Studi di Catania.

Marta Doniselli è Dottore di ricerca in Diritto processuale penale presso l'Università degli Studi dell'Insubria.

Roberto Flor è Dottore di ricerca europeo in Diritto penale dell'economia e dell'informatica, nonché assegnista di ricerca in diritto penale e professore a contratto in Diritto penale dell'informatica presso la Facoltà di Giurisprudenza dell'Università degli Studi di Verona.

Francesca Romana Fulvi è Dottore di ricerca in Diritto e procedura penale presso l'Università degli Studi di Roma "La Sapienza".

Marco Grotto è Dottore di ricerca in Diritto penale presso l'Università degli Studi di Trento.

Roberto E. Kostoris è Professore ordinario di Diritto processuale penale presso l'Università degli Studi di Padova.

Stefano Marcolini è Ricercatore confermato in Diritto processuale penale presso l'Università degli Studi dell'Insubria.

Michele Panzavolta è Lecturer presso la Faculty of Law of Maastricht University.

Claudia Pecorella è Professore associato di Diritto penale presso l'Università di Milano-Bicocca.

Lorenzo Picotti è Professore ordinario di diritto penale presso l'Università di Verona, membro del Conseil de Direction e del Comitè Scientifique dell'Association Internationale de Droit Pénal e segretario generale del Gruppo italiano AIDP.

Daniele Pistolesi è Addetto alla Prima Sezione operativa della Divisione Seconda del Servizio Polizia Postale e delle Comunicazioni.

DOMENICO RASCHELLÀ è Cultore di Diritto processuale penale presso l'Università degli Studi dell'Insubria, Como, nonché avvocato del Foro di Como.

FRANCESCA RUGGIERI è Professore ordinario di Diritto processuale penale presso l'Università dell'Insubria e Responsabile scientifico del centro Studi di Diritto penale europeo.

IVAN SALVADORI è Dottore di ricerca europeo ed Assegnista di ricerca in Diritto penale dell'informatica presso l'Università di Verona.

CARLO SARZANA DI SANT'IPPOLITO è Presidente Aggiunto Onorario della Corte di Cassazione.

Prefazione

a cura di *Francesca Ruggieri* e *Lorenzo Picotti*

Pubblichiamo le relazioni e gli interventi del Convegno che, nel maggio del 2010, per iniziativa della *Sezione dei Giovani Penalisti* del Gruppo Italiano dell'AIDP (*Association Internationale de Droit Pénal*), ha raccolto studiosi, operatori e professionisti, sul tema della *criminalità informatica.*

Il confronto tra giovani studiosi, attenti anche agli ordinamenti stranieri, magistrati, accademici e "tecnici" di ricca esperienza, ha consentito di tracciare un affresco quanto mai attuale, originale ed approfondito della materia.

In questo quadro interdisciplinare, che si estende dal diritto penale sostanziale a quello processuale, trovano un posto particolare le controverse e severe fattispecie incriminatrici della pedopornografia, anche "virtuale", con i delicati problemi di incriminazione dei fruitori e del mero possesso od accesso al materiale illecito, discendente dai precetti sovranazionali (SALVADORI, DONISELLI); nonché le tecniche di accertamento *on line* e gli obblighi strumentali di *data retention*, gravanti su tutti gli *Internet Service Providers*, peraltro da bilanciare con il necessario rispetto dei diritti fondamentali della persona, solennemente proclamati come meritevoli di massima tutela in Internet dalla più recente giurisprudenza costituzionale tedesca e romena (FLOR). Un evidente rilievo trovano così le trattazioni relative alle responsabilità penali dei fornitori di servizi in rete (DE NATALE) e la disciplina delle intercettazioni (COLOMBO, PANZAVOLTA, RASCHELLÀ).

Le attuali particolarità e la grande estensione degli scambi e dei comportamenti anche illeciti in "rete", offrono altresì il destro per analisi di carattere più generale, di tipo sia criminologico (SARZANA DI SANT'IPPOLITO), che ermeneutico, concernenti in specie le recenti disposizioni di diritto penale sostanziale (PECORELLA, GROTTO, FULVI) e processuale (KOSTORIS) emanate in Italia nel 2008, in attuazione della Convenzione *Cybercrime* del Consiglio d'Europa – risalente invero al 2001 – che sollecitano riflessioni approfondite sui nuovi mezzi di prova *on line* o digitali in senso lato (MARCOLINI, DANIELE), alla luce soprattutto delle prime, complesse, pronunce giurisprudenziali in materia (CAJANI).

* * *

La *Sezione dei Giovani Penalisti* del Gruppo italiano dell'AIDP ha colto appieno la rilevanza di queste tematiche, nel decidere di promuovere il Convegno di studio, che ha fatto emergere l'incrocio di due temi fondamentali, specifici dell'Associazione: il rilievo preponderante, in questo ambito, del quadro giuridico sovranazionale; e la novità della "sfida" che la criminalità informatica lancia ai sistemi penali, quale manifestazione del tutto inedita di una pluralità via via mutevole di comportamenti illeciti, propri di un mondo "globalizzato" e "tecnologico", che sollecita l'attenzione e l'impegno nella ricerca, nonché il necessario confronto interdisciplinare fra sostanzialisti e processualisti, soprattutto da parte dei giovani studiosi.

Casi giurisprudenziali recenti, di cui si è discusso nel Convegno – da Pirate Bay, al processo a Google per il caso Vividown – dimostrano l'urgenza di elaborare nuove categorie o, perlomeno, di adattare quelle tradizionali del diritto penale sostanziale e processuale alla realtà dell'informatica e del *cyberspace*, in cui si realizzano "condotte" o "fatti" illeciti connotati

da una peculiare dematerializzazione e delocalizzazione di atti ed effetti, che però lasciano tracce e prove "elettroniche" nello spazio virtuale, bisognose peraltro di specifici strumenti e tecniche di indagine per la loro ricerca e raccolta.

* * *

Come è stato sottolineato nella relazione d'apertura del sottoscritto (purtroppo non pubblicata nel volume), la "qualità" specifica dell'informatica è in effetti costituita dall'*automazione* dei processi di elaborazione dei dati, per conseguire un "risultato" in tempi, modi e contenuti, che attività anche molto complesse dell'uomo non potrebbero parimenti conseguire. E questa "sostituzione", per quanto interessa il diritto penale sostanziale, non investe solo gli aspetti "cognitivi" dell'attività umana, in termini di entità e rapidità delle informazioni acquisite e trattate, ma anche aspetti "decisionali", vale a dire coinvolgenti "scelte" e "manifestazioni di volontà" che possono avere un valore e un'efficacia giuridicamente rilevanti: certamente sulla base di programmi predisposti dall'uomo, ma con un'elaborazione *diretta* dei dati e delle informazioni da parte del sistema, che possono essere del tutto nuove ed indipendenti dalla previa selezione o conoscenza delle persone fisiche, e che nondimeno si pongono a fondamento di ogni "decisione" automatizzata. Si pensi, ad es., alla stipula di contratti di borsa in relazione all'andamento di valori azionari; od all'instaurazione di procedure di sicurezza, che possono incidere su attività e determinazioni di persone fisiche, in presenza di definiti od acquisiti valori d'allarme o sintomatici di situazioni pericolose; come pure all'indicizzazione o catalogazione di siti, nominativi, prodotti in relazione a richieste dell'utenza od altri parametri variabili, che assumono un rilievo sempre maggiore nel funzionamento di motori di ricerca, attività pubblicitarie personalizzate, ecc.

Perché occorre sottolineare questi aspetti nella prospettiva del diritto penale?

Perché non solo dal punto di vista concettuale o filosofico, ma anche da quello giuridico positivo, l'*automazione* connota la definizione dell'informatica o, meglio, dei "sistemi informatici" e, correlativamente, dei "dati informatici", in quanto suscettibili di o prodotti da un trattamento *automatizzato*: come risulta testualmente dall'art. 1, lettere a) e b), della Convenzione *Cybercrime* del Consiglio d'Europa, adottata a Budapest nel 2001, e dalla corrispondente norma definitoria dell'art. 1, lettere a) e b), della Decisone quadro dell'Unione europea 2005/222/GAI del 24 febbraio 2005 contro gli attacchi ai sistemi informatici.

Ebbene, l'automazione sta acquistando sempre maggior rilievo nel web 2.0, e nel prevedibile ulteriore sviluppo tecnologico-sociale del *cyberspace*, per l'interazione crescente che si ha *direttamente* con gli utenti, senza interventi contestuali ed attivi di soggetti umani che controllino o "moderino" concretamente tale interazione.

Il caso "Google-Vividown" ne è un chiaro esempio, avendo il video "postato" dagli utenti stessi acquisito e mantenuto per molto tempo i primi posti nella graduatoria "automatizzata" dei video più visitati, da cui è stato eliminato solo dopo la segnalazione dell'autorità.

Quid juris circa la responsabilità per simili "fatti", costituenti *oggettivamente* offese di beni giuridici anche molto rilevanti della persona e della collettività?

Facile è affermare la responsabilità, anche penale, degli autori materiali del video (*content-provider*) e del suo consapevole e voluto inserimento nella "bacheca elettronica" offerta da Google, ovviamente quando sia acquisibile la prova della loro identità. Le questioni sorgono però con riferimento al servizio offerto agli utenti (*utility*), tramite il quale se ne è realizzata e mantenuta la "diffusione" per notevole periodo di tempo.

È chiaro che si pongono, per i responsabili di siffatto servizio – non privo di ritorni economici, se non altro pubblicitari e futuri – rilevanti problemi d'*imputazione oggettiva* degli eventi o, comunque, degli "effetti" delle condotte commesse nel *cyberspace* non solo dagli

autori del video, ma anche proprie: sia *attive* (di organizzazione e mantenimento, pur ampiamente automatizzato, del servizio predetto, rispettando tutti gli obblighi inerenti, compresi quelli relativi all'informativa sul "trattamento di dati personali" così realizzato), che eventualmente *omissive*, in relazione ad obblighi giuridici di controllo od impedimento di eventi offensivi o di reati altrui, che potrebbero fondare una responsabilità per partecipazione, alla stregua della vigente disciplina sul concorso di persone nel reato (art. 110 segg. c.p.), ovvero *ex* art. 40, capoverso, c.p.

A tali questioni si può dare risposta ricostruendo attentamente, innanzitutto, la disciplina extrapenale applicabile, da cui possono desumersi obblighi giuridici anche penalmente rilevanti (nella specie: quella del trattamento dei dati personali *ex* d.lgs. n. 196 del 2003, c.d. Codice della privacy); ma solo parzialmente ricorrendo, poi, ai tradizionali parametri della causalità naturalistica fra fenomeni "ripetibili", secondo modelli di sussunzione sotto leggi scientifiche, ben difficilmente rinvenibili in quest'ambito.

Il diritto penale aggiunge, poi, specifiche questioni relative all'*imputazione soggettiva*, essenziale per aversi "responsabilità personale" (*ex* art. 27, comma 1, Cost.), fondata su un rimprovero *individualizzato* di colpevolezza, a titolo di dolo (o, se prevista, di colpa), che richiede ulteriori elementi di conoscenza e volontà *proprie* (o quantomeno conoscibilità ed impedibilità) rispetto al "fatto" e, quindi, anche ai comportamenti "altrui".

Non è, allora, soltanto un problema di "smaterializzazione" o di "delocalizzazione" delle condotte e degli eventi nel *cyberspace*, in cui resti però fermo e ben scolpito il ruolo del *service provider*, da un lato, e degli utenti, ed eventualmente dei terzi, dall'altro.

L'interazione crescente, che lascia ampia operatività agli utenti ed alla loro libertà d'azione, sembrerebbe a prima vista comprimere la stessa possibilità d'imputazione (oggettiva e, soprattutto, soggettiva) di reati od illeciti da essi commessi, ai fornitori di servizi non solo di *mera* "connettività", ma anche di "ospitalità" c.d. passiva (*host-provider*) in Internet.

La conclusione appare però superficiale ed inadeguata alla realtà tecnologica e sociale dell'odierno *cyberspace*: in un mondo cibernetico integrato, che va dalla telefonia mobile, ai sistemi satellitari di rilevazione delle posizioni, con accessibilità, disponibilità e trasmissibilità di dati d'ogni genere in tempo reale (compresi voce, video, musica), si moltiplicano le *utilities* e le stesse possibilità tecnologiche di offrirle e gestirle. Per cui gli attori di un siffatto *web*, sempre più dinamico ed interattivo, basato su motori di ricerca sempre più personalizzati ed intrusivi, non possono certo restare "immunizzati" rispetto alle conseguenze delle loro azioni (imprenditoriali o meno) ed agli effetti su larga scala, che sistematicamente impostano, sviluppano, adeguano, aggiornano, estendono.

Si tratta, invece, di rivedere e ricostruire, nell'ambito rigoroso dei principi penalistici e della disciplina giuridica vigente – solo se necessario proponendone eventuali modifiche – un sistema coerente d'imputazione (oggettiva e soggettiva), adeguato alla realtà dell'*automazione* dei sistemi di trattamento e di circolazione dei dati, la cui adozione non esclude di per sé il mantenimento del "dominio" dell'uomo (e quindi la sua responsabilità, se del caso anche penale) sui processi che attiva, gestisce, utilizza, controlla, aggiorna, adegua, con scopi leciti (o talora anche illeciti), comunque teleologicamente strutturati.

In questa riflessione giuridico-dogmatica, che investe categorie fondamentali del diritto penale (l'azione, l'omissione, l'evento, la causalità, il dolo, il concorso di persone, ecc.), da filtrare attraverso il significato "sociale" dell'esecuzione di un algoritmo, si deve collocare in primo piano la considerazione del contesto giuridico internazionale, in cui le nuove esigenze possono trovare ampia ed equilibrata ricezione, come ha già dimostrato largamente la Convenzione *Cybercrime* del Consiglio d'Europa, proprio in quanto prevalga una prospettiva sovranazionale di bilanciamento ed armonizzazione, rispetto a singoli interessi "di parte" o di *lobbies* corporative: prospettiva che all'interno dell'Unione europea vede oggi l'operatività di

efficaci strumenti di ravvicinamento legislativo, vincolanti gli Stati membri, grazie all'attribuzione di competenze "dirette" in materia penale, da esercitare mediante direttive in settori di criminalità grave e transnazionale, fra cui è espressamente menzionata la "criminalità informatica" (nuovo art. 83, par. 1, del Trattato sul funzionamento dell'Unione europea).

* * *

In tal modo si delinea un orizzonte istituzionale chiaro per i giovani studiosi del diritto e della procedura penale, in cui si deve collocare la valutazione critica dell'ordinamento nazionale, valorizzando il metodo della comparazione giuridica e l'approfondita conoscenza delle fonti internazionali, cui l'AIDP ha sempre dedicato specifica attenzione, al fine di far progredire la scienza e – ci si augura – anche la prassi del sistema penale, tenendo il passo incalzante dell'evoluzione tecnologica e sociale.

Freiburg im Breisgau, luglio 2011

Introduzione

Considerazioni sull'internet degli oggetti e sul *cloud computing*

di *Carlo Sarzana di Sant'Ippolito*

Ringrazio anzitutto gli organizzatori del presente Convegno, e particolarmente la professoressa Ruggeri ed il professor Picotti, per il gradito invito a presiedere la seduta iniziale di questo importante Convegno. Dato il titolo della Sezione, credo sia opportuno accennare ai più recenti sviluppi della tecnologia informatica in relazione ai rischi sociali e giuridici derivanti dall'uso di tali tecnologie, particolarmente per quanto riguarda la sicurezza informatica, la protezione della *privacy* e la tutela dei dati personali.

Ripeto qui per inciso ciò che da tempo vado sostenendo, e cioè che in un settore, quale quello informatico nel quale le nuove tecnologie irrompono, creando necessità, a volte urgenti, di un inquadramento dei nuovi fenomeni nel campo del diritto, è divenuto difficile stare realmente al passo con la situazione giacché occorrono doti di costante attenzione e capacità, di osservazione delle nuove realtà, attenzione e capacità che devono essere accompagnate, ai fini di una comprensione e di un esatto inquadramento del complesso fenomeno, da una sensibilità insieme giuridica, sociologica e criminologica.

Ciò premesso passo ad esaminare, molto succintamente alcuni dei problemi relativi ai rischi sopraccennati. In proposito rilevo anzitutto che da qualche tempo la pubblicistica specializzata, i legislatori di vari Paesi del mondo ed alcune organizzazioni internazionali si stanno occupando delle conseguenze tecniche, giuridiche e sociali derivanti dallo sviluppo del cosiddetto "*INTERNET degli oggetti"* (**IdO**) chiamato anche "Informatica ubiquitaria" o "Intelligenza ambientale" con riferimento a determinate tecnologie (*R.F.I.D., TCP/IT, BLUETOOTH*, ecc.), che, collegate insieme, consentono di identificare oggetti, raccogliere dati, trattarli e trasferirli.

Già in occasione della Conferenza Europea sull'argomento "*INTERNET del futuro*" tenutasi nell'ottobre del 2008 durante il *Summit* di Nizza dei Ministri dell'Unione Europea che si occupano dei problemi della società dell'informazione, è emersa la preoccupazione di vedere crescere i problemi relativi alla "*governance*" europea delle infrastrutture relative e si è prospettata la possibilità di attuare, tra l'altro, il c.d. *silenzio dei chips*.

L'argomento è stato oggetto di recente di un'importante comunicazione della Commissione U.E. al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale, del 18 giugno 2009, dal titolo *L'INTERNET degli oggetti*: *un piano di azione per l'Europa* (COM/2009/278 fin.). La Commissione ha rilevato che l'*Internet degli oggetti* è composto da una serie di nuovi settori integrati che operano con infrastrutture proprie e che poggiano in parte sulle infrastrutture Internet esistenti, precisando che l'IdO può essere messa in relazione con nuovi servizi e riguarda tre modi principali di comunicazione che possono essere stabiliti in ambienti ristretti (*Intranet degli oggetti*) o pubblicamente accessibili (*Internet degli oggetti*) e cioè comunicazioni: a)da oggetto a persona; b) da oggetto ad oggetto; c) da macchina a macchina (M2M).

La Commissione ha precisato, poi, che l'**IdO** attualmente riguarda applicazioni quali:

- telefoni cellulari con accesso a internet, dotati di macchina fotografica;
- numeri di serie unici sui prodotti farmaceutici (in forma di codici a barre);
- sistemi intelligenti di misurazione dell'elettricità per fornire ai consumatori informazioni in tempo reale sui consumi;
- «oggetti intelligenti» nel settore della logistica (eFreight), nel settore manifatturiero o nella distribuzione commerciale.

La Commissione non ha potuto fare a meno di rilevare che la realizzazione della connessione degli oggetti solleva particolari questioni, quali – ad es. – l'identificazione dell'oggetto, l'autorità responsabile dell'attribuzione dell'identificatore, i mezzi per rilevare le informazioni relative all'oggetto, la garanzia della sicurezza delle informazioni, il quadro etico e normativo dell'internet degli oggetti, i meccanismi del controllo, ecc. In argomento la Commissione ha sottolineato che lo sviluppo dell'IdO deve rispettare la vita privata e la protezione dei dati personali: per tutelare la sicurezza delle informazioni la Commissione ha chiesto agli Stati di rafforzare la sorveglianza e la protezione delle infrastrutture critiche informatiche [1].

Una delle più importanti realizzazioni dell'IdO è rappresentata dalla tecnologia R.F.I.D. (le c.d. *targhette intelligenti*): si tratta di sistemi che utilizzano le onde radio per la identificazione di oggetti, cose, animali e persone, utilizzando la lettura a distanza dei *chips* da parte di appositi strumenti di lettura. In tal modo vengono catturate, per così dire le *informazioni contenute* in una particolare etichetta. Il *tag R.F.I.D.* è tipicamente composto da un *micro chips* e da una antenna: in certi casi anche da una batteria.

La tecnologia R.F.I.D. è stata oggetto di una recente importante Comunicazione della Commissione U.E. (2009/387/CE) del 12 marzo 2009 che tratta, tra l'altro, dell'argomento relativo alla messa in opera dei principi relativi al rispetto della vita privata ed alla protezione dei dati nelle applicazioni relative all'identificazione mediante radiofrequenza, nella quale si afferma (*considerando n. 20*) che nel settore del commercio al dettaglio una valutazione degli impatti sulla protezione della vita privata e dei dati personali, dei prodotti contenenti etichette venduti ai consumatori dovrebbe fornire le necessarie informazioni per determinare eventuali minacce alla stessa vita privata o alla protezione dei dati personali. A questo riguardo la Commissione ha emanato apposite raccomandazioni [2].

---

[1] A proposito dell'IdO un autore francese MARC-OLIVIER PADIS in un articolo dal titolo *Homo numericus – L'Internet e les nouveaut outil informatique*, ha esaminato le conseguenze di quello che lui chiama "*La dispersion dell'Internet hors de sa sphere d'origine*" e, tra l'altro, ha osservato che "*… il ne s'agira plus alors de dérober un peu de notre tempe réel pour aller vivre dans le monde de simulation ou de compenser oginariament une réalité dècevant dans de mondes parallèles mais de vivre dans une "réalité augumentée*".

[2] *Applications RFID utilisées dans le commerce de détail*

9. Au moyen d'un signe européen commun élaboré par des organismes européens de normalisation avec l'aide des parties concernées, les exploitants doivent informer les personnes de la presence d'étiquettes placées sur les produits ou incorporées à ceux-ci.

10. Lors de la réalisation de l'évaluation d'impact sur la protection des donne et de la vie privée visée aux points 4 et 5, l'exploitant d'application doit déterminer précisément si les étiquettes placées sur des produits ou incorporées à des produits vendus aux consommateurs par des détaillantes qui ne sont pas exploitants de cette application présentent un risque probable pour la vie privée ou la protection des donne à caractère personnel.

11. Les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application à moins que les, consommateurs, après avoir pris connnaissance de la politique d'information visée au point 7, acceptent que les étiquettes restent opérationnelles. Par désactivation des etiquettes, on entend tout processus qui interrompt les interactions d'une etiquette avec son environnement et qui n'exige pas de participation active du consommateur. La dèsactivation ou le retrait des etiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateurs doivent pouvoir verifier que la désactivation ou le retrait sont effectifs.

12. Le point 11 ne s'applique pas s'il resort de l'évaluation d'impact sur la protection des données et de la vie privée que les etiquettes utilisées dans une application de détail et restant opérationnelles au-delà du point

L'ENISA, e cioè l'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione, ha recentemente analizzato i rischi associati allo scenario futuro dello sviluppo dell'IdO con particolari riferimenti ai viaggi aerei[3], formulando raccomandazioni apposite per quanto riguardava la *policy*, la ricerca e gli aspetti legali connessi.

I più importanti rischi enunciati nel *paper* riguardavano:

a) *failure of reservation, check-in and trading procedures*;
b) *problems in issuing/enabling electronic visas*;
c) *loss/violation of citizen/passegger privacy*;
d) *compliance and abuse of state-owned citizen/passegger database*;
e) *repurposing of data/mission crep*;
f) *Health processes-related concerns*;
g) *user frustration and low user acceptance*;
h) *aggressive profiling and social sorting leading to social exclusion*;
i) *legislation lagging behind rapid tecnological advancement*;
l) *non-compliance with date protection legislation*.

Devo ricordare a questo punto per inciso che, già moltissimi anni fa, nei miei primi scritti ed interventi, avevo accennato ai profili di vulnerabilità della società informatizzata ed in particolare ai possibili attentati ai sistemi "*life support*", o di diagnosi elettronica ed ai possibili errori nella gestione della relativa strumentazione[4]. In realtà lo sviluppo dei sistemi in questione ha accresciuto i problemi di sicurezza dei sistemi informatici, già notevoli a causa dei *virus* e degli *worms*, in quanto gli attacchi o i malfunzionamenti derivanti da errori o negligenze possono riguardare processi vitali per gli interessati giacché per molti pazienti, come ad esempio i cardiopatici, funzionano veri e propri sistemi computerizzati che raccolgono e forniscono informazioni vitali per il funzionamento ad esempio di *pacemake*r o *defibrillatori*: pertanto un'informazione erronea nei dati registrati nei *chips* e concernenti le cure, e comunque la propria storia clinica, potrebbe avere conseguenze serie sulla vita dei pazienti[5]. Non si deve trascurare poi il rilievo relativo al fatto che potrebbe verificarsi una diffusione incontrollata di dati sensibili, in considerazione del fatto che lo sviluppo delle tecnologie consente alle apparecchiature lo scambio di dati e informazioni con l'esterno, oggetto di possibile intercettazione nel circuito della Rete, con conseguenze potenzialmente irreparabili.

Ciò premesso deve dirsi che anche in Italia si sta verificando una tendenza all'introduzione dei R.F.I.D., definiti da un giornale specializzato (Il Corriere delle Comunicazioni, n. 19 del 9.11.2009) come "*oggetti prêt-à-porter*". Lo stesso legislatore italiano, nell'intento di proteggere alcuni prodotti nazionali, ha introdotto, sembra senza tener alcun conto della sopracitata comunicazione della Commissione U.E., un sistema di etichette intelligenti. Il Parlamento ha infatti approvato la legge n. 55 dell'8 aprile 2010 recante il titolo *Disposizioni*

de vente ne presentment pas de risque probable pour la vie privée ou la protection des données à caractère personnel. Néanmoins, les détaillants doivent metre gratuitement à disposition un moyen aisé de désactiver ou de retirer, immédiatement ou ultérieurement, ces etiquettes.

13. La désactivation ou le retrait des etiquettes ne doit impliquer aucune reduction ni cessation des obligations légales du détaillant ou du fabricant envers le consommateur.

14. Les points 11 et 12 ne s'appliquent qu'aux détaillants qui sont exploitants.

[3] Flying 2.0 – *Enabling automated air travel by identifing and addressing the challenges of IoT and R.F.I.P. technology*, aprile 2010.

[4] Rinvio in proposito alla prima edizione (Milano, 1994) del mio testo dal titolo di allora *Internet e diritto penale*.

[5] Cfr., da ultimo, l'articolo di A. RUSTICHELLI, *Quando l'hacker attacca il pace-maker*, in *Affari e Finanza*, 7 giugno 2010.

concernenti la commercializzazione dei prodotti tessili, delle pelletterie e calzaturieri allo scopo di permettere l'etichettatura dei prodotti *made in Italy* ...[6].

Rilevo, per inciso, che una recentissima applicazione dell'IdO è stata attuata in occasione dell'esposizione a Torino della Sindone, ad opera di una società multinazionale, la *Concet Reply,* che ha messo a punto una infrastruttura in grado di rilevare attraverso particolari sensori e telecamere termiche il succedersi dei pellegrini, di valutarne il flusso e la direzione e. in caso di necessità, di intervenire tempestivamente per mettere in atto le procedure di controllo necessarie[7].

Passando ora ad altro argomento rilevo che, come già illustrato in altra sede[8], l'uso delle apparecchiature WiFi non appare sicuro quanto alla protezione delle informazioni e dei dati. Di recente è scoppiato il c.d. caso Google giacché i suoi incaricati, nell'applicazione del servizio *mapping* denominato *Street View*, avrebbero, si sostiene indiscriminatamente, intercettato comunicazioni di sistemi WiFi non protetti, rilevando indirizzi, percorsi, e-mail, passwords, etc. degli utenti. Alcuni Garanti per la protezione dei dati personali di Paesi europei, come la Germania, la Spagna, l'Irlanda e la Svizzera, ma anche l'Italia, hanno aperto un'apposita inchiesta. Secondo un quotidiano italiano (*Il Sole 24 Ore*) Google Italia avrebbe ammesso che le *Google cars* sono in grado di captare le reti *wireless* non protette e gli apparati di reti mobili e di catturare frammenti di comunicazioni elettroniche. Per quanto riguarda l'Italia il Garante per la protezione dei dati personali avrebbe chiesto a *Google* di conoscere la data di inizio della raccolta delle informazioni (di tutte le informazioni, comprese le immagini), e finalità per le quali erano state registrate, la durata e l'indicazione degli archivi erano state conservate. In attesa della risposta della società di *Mountain View* il Garante ha imposto a *Google* di sospendere il trattamento dei dati captati dalle *reti wireless* e dai telefonini, nonché di chiarire se quelle informazioni fossero accessibili a terzi o fossero state cedute; infine, se per catturarle fossero stati utilizzati *software* particolari.

Passo ora ad accennare all'ultimo grido in fatto di applicazioni informatiche: mi riferisco al c.d. *cloud computing*.

Cos'è il cloud computing?

Non si tratta di una nuova tecnologia: si tratta di una nuova metodologia dell'infrastruttura IT tramite la banda larga, concretandosi in una automazione dei servizi di gestione. Esistono in-

[6] L'articolo 2 della legge, al primo comma, si occupa delle norme di attuazione, stabilendo che: "... 1. *Con decreto del Ministro dello sviluppo economico, di concerto con il Ministro dell'economia e delle finanze e con il Ministro per le politiche europee, da emanare entro quattro mesi dalla data di entrata in vigore della presente legge, previa notifica ai sensi dell'articolo 8, paragrafo 1, della direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, sono stabilite le caratteristiche del sistema di etichettatura obbligatoria e di impiego dell'indicazione «Made in Italia», di cui all'articolo 1, nonché le modalità per l'esecuzione dei relativi controlli, anche attraverso il sistema delle camere di commercio, industria, artigianato e agricoltura. 2. Il Ministro della salute, di concerto con il Ministero dello sviluppo economico e previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, adotta, entro tre mesi dalla data di entrata in vigore della presente legge, un regolamento recante disposizioni volte a garantire elevati livelli di qualità dei prodotti e dei tessuti in commercio, anche al fine di tutelare la salute umana e l'ambiente, con cui provvede, in particolare: omissis ... ... d) a stabilire l'obbligo della rintracciabilità dei prodotti tessili e degli accessori destinati al consumo in tutte le fasi della produzione, della trasformazione e della distribuzione*".

[7] Cfr. l'articolo di C. La Via, *L'Internet degli oggetti a servizio della Sindone*, 7 maggio 2008, in *www.wired.it/news/archivio/2010.*

[8] Cfr. il mio testo *Internet, informatica e diritto penale*, Milano, 2010, p. 693 ss.

dubbiamente dei benefici del *cloud computing* in quanto esso consente di ridurre notevolmente i costi associati alle forniture dei servizi: infatti appaiono sempre più numerose le aziende sedotte dalle offerte delle società che forniscono i servizi di *cloud computing*, servizi che vengono ovviamente presentati come estremamente vantaggiosi dal punto di vista economico.

Sono tre le applicazioni principali del *cloud computing* e cioè:

S a a s (*Software come servizio*)

Tale applicazione raggruppa la fetta più ampia del mercato relativo: essa può essere di qualunque tipo dalla gestione delle e-mail alle complesse applicazioni (tipo *google doc*) sino ad una serie di prodotti per la collaborazione *on line* (tipo *Rotus Live*).

Pa a s (*Piattaforma come servizio*)

Essa fornisce al consumatore un ambiente di *runtime* per le sue applicazioni, permette eventualmente un parziale controllo nell'ambito in cui le applicazioni vengono eseguite.

La piattaforma in questione è quindi tipicamente un *framework* applicativo.

I a a s (*Infrastrutture come Servizi*)

Tale applicazione fornisce quello che può definirsi come la fornitura di risorse computerizzate, di connettività, ecc. Il consumatore-utente ha il diretto controllo sul sistema operativo, sullo *storage*, etc. e può effettuare il *deployment*.

In questo tipo di servizio gli utenti pagano in funzione dell'utilizzo che faranno delle risorse: viene quindi anche chiamato *utility computing*.

L'aspetto caratteristico del *cloud computing* è che il fenomeno è connesso alla possibilità, sfruttando la velocità della banda larga, di utilizzare *hardware* e *software* ubicati, dal punto di vista della localizzazione geografica, in una qualunque parte del mondo.

Tuttavia vi è il rovescio della medaglia e cioè esistono rischi e pericoli nell'uso e nella gestione del *cloud computing*. Varie organizzazioni hanno esaminato il problema, tra cui la citata l'ENISA, l'Ente Europeo che dovrebbe occuparsi della sicurezza informatica, che ha redatto un apposito studio dal titolo *Cloud computing – Benefit, risk and recommendations for IT security*. L'ENISA, in particolare, ha elencato e descritto 35 rischi dei quali ben 23 specifici al *cloud computing*.

Più particolarmente, secondo lo studio, i rischi organizzativi sarebbero 7, quelli tecnici 11, quelli legali 15. Le vulnerabilità del sistema sarebbero ben 38! In effetti, nonostante le grandi campagne pubblicitarie condotte dalle imprese che commercializzano il sistema, non sembra che, almeno per il momento, l'ambiente interessato si sia dimostrato molto recettivo.

Va detto a questo proposito che la società Forrestar Researce inc., una società di ricerca indipendente, ha effettuato una indagine *ad hoc*, interpellando oltre duemila IT *executive* e *decision's makers* in tema di IT, in Canada, Francia, Germania, UK e USA. I soggetti interpellati hanno mostrato uno scarso interesse al sistema *pay as pay hosting* dei servizi virtuali e degli altri servizi offerti dal *Cloud Computing*. Soltanto il 3% ha dichiarato di usare il sistema: la percentuale è rimasta fissa rispetto all'anno precedente.

Per quanto riguarda il profilo giuridico del servizio, alcuni pubblicisti italiani hanno cercato di inquadrare il *cloud computing* nel sistema giuridico vigente.

Secondo una prima tesi [9], la prevalenza di una prestazione di fare, avente ad oggetto la fornitura di uno o più servizi s*oftware* o di altra natura, unitamente alla presenza di un'organizzazione dotata di mezzi e gestione propria e al pagamento di un compenso, sono tutti elementi che farebbero propendere per la configurabilità di un "appalto di servizi" sia pure avente ad oggetto prestazioni continuative o periodiche.

Secondo altra tesi [10], sarebbe da escludere la natura di appalto di servizi in quanto si tratterebbe invece di un contratto atipico.

Va detto, a questo punto, che il fenomeno del *cloud computing* ha indubbiamente destato l'interesse del mondo imprenditoriale, apparendo strategico anche per molte grandi aziende come *Google, Amazon, IBM* e per la stessa *Microsoft,* aziende che forniscono la possibilità di creare e gestire documenti di testo, fogli di calcolo e molti altri servizi utilizzando siti Web.

Tuttavia l'organizzazione denominata *Electron Privacy Information Center* ha, di recente, rivolto un appello al Congresso USA, affermando che occorreva bloccare i richiami, immotivati e pericolosi, al *cloud computing* e le sue promesse: le *appliance* di *google* avrebbero dovute essere tenute sotto chiave sino a quando non l'organizzazione non sarebbe stata in grado di offrire garanzie sufficienti agli utenti. In pratica l'organizzazione sopra indicata ha chiesto alla FTC (*Federal Tecnological Commission*) di impedire a *Google* di continuare a somministrare le proprie *appliance* fintanto che la società non sarebbe stata in grado di dimostrare che le sue pratiche erano adeguate, sicure e rispettose della *privacy* [11].

Per il momento la FTC ha deciso di chiamare a raccolta le aziende attive nel *cloud computing*, onde interpellarle al fine di stabilire se fosse più o meno opportuno rendere le regolamentazioni più stringenti.

Di *cloud computing* si parla anche fuori degli Stati Uniti, ad es. in seno all'OCSE. Nell'ottobre scorso (2009) l'Unione Europea ha aperto un tavolo di consultazione per l'eventuale revisione della Direttiva sulla protezione dei dati personali che dovrebbe essere ammodernata per prendere in considerazione, tra l'altro, i rischi del *cloud computing*.

Non può non rilevarsi a questo punto che critiche incisive all'uso del *cloud computing* sono state formulate dal noto *hacker* Richard Stallman, fondatore della *Free Software Fondation*, che lo ha definito come una mossa tipicamente pubblicitaria che metterebbe i dati degli utenti su *server* remoti, in balia dei fornitori dei *server* stessi [12].

---

[9] Cfr. S. BENANDI, *Software as a Service (Saas): aspetti giuridici e negoziali*, in *www.stefanobenandi.com/software-as-a-service-aspettigiuridici*.

[10] Cfr. F. NICOLA, *I nuovi paradigma della rete. Distribued computing, cloud computing, computing paradigms: abstract sugli aspetti e profili giuridici*, in *www.diritto.it/art.php?file=/archivio/27973.html* vedi anche R. FREATO-S. COSSINCARE, *SLA in aspetti legali* in *www.beccloud.it/*. Vedi, *amplius*, l'articolo di A. FUPU, A. TESSALONITOKOS, *La spécificités du contrat informatique relatif au software as a service (Saas)*, in *Expertises*, settembre 2009, p. 308 ss., cui *adde*, H. CARADOU, *Le droit dans les nuages*, in *ivi*, luglio 2010, p. 251; Above the cloud, di autori vari, in *http://berkeleyclouds.blogspot.com* dell'11 giugno 2009; *La révolution du cloud computing*, di P. DESMDT, in *www.usinenouvelle.com/article/la-revolution-du-cloud-computing.*

In materia di rischi derivanti dall'uso del *cloud computing* vedi anche il *paper* dal titolo *The drivers for web security in the cloud* di F. HOWARD del febbraio 2010, cui *adde* INFO-WORD, *Cloud Computing deep dive*, special report del settembre 2009. Vedi anche il *paper* dal titolo *From virtualization vs security to virtualization based security*, dell'ISACA, Intel Corporation del 2007. Infine vedi il *paper* dal titolo *What the ideal cloud-based web security service should provide*, di F. HOWARD, febbraio 2010.

[11] Cfr. MARUCCI, *USA, Cloud computing sul banco degli imputati* in *www.punto-informatico.it* del 19 marzo 2009.

[12] R. STALLMAN in un'intervista al *Guardian* ha dichiarato testualmente che "*… il cloud computing è roba di stupidi e utilizzare applicazioni web come Gmail di Google è anche peggio della stupidità stessa …*" e ha aggiunto: "*… Un motivo per cui non dovresti usare applicazioni web per il tuo lavoro è che ne perdi il controllo*", "*E lo stesso vale per i programma proprietari. Se usi programma proprietario o il web server di qualcun altro, sei nelle mani di chiunque abbia sviluppato quel software*". Stallman ha anche liquidato lo *hype* del *cloud*

Per concludere devo dire che non mi sento di dare torto alle critiche ed ai giudizi di Stallman … In effetti è noto che le innovazioni tecnologiche si prestano benissimo a grosse operazioni di *marketing*: non appena appare infatti una nuova tecnologia informatica o una nuova applicazione, alcune grandi imprese, specie multinazionali, si lanciano all'assalto del mercato. Strategie e tattiche sono le consuete … i soggetti del *management* e quelli delle pubbliche relazioni elaborano articolate strategie mediatiche, cercando anche, nell'ambito di un elaborato programma di penetrazione, di individuare nel settore privato ma specialmente in quello pubblico, i possibili *decision makers* (tecnici, burocrati e politici) per quanto riguarda la scelta e l'adozione delle nuove tecnologie e per gli acquisti relativi. Una volta individuati tali soggetti li si contattano e li si corteggiano, cercando di creare in tutti i modi una specie di aggregazione culturale, Seguono poi pseudo convegni scientifico-culturali, in realtà finalizzati a reclamizzare la bontà dei prodotti ed i vantaggi delle innovazioni proposte. In pratica i problemi, quasi sempre esistenti, relativi principalmente alla sicurezza delle innovazioni ed alla tutela dell'ambiente, vengono disinvoltamente ficcati "sotto il tappeto", ignorati o minimizzati e, naturalmente, vengono viste come vere "bestie nere" gli esperti indipendenti che cercano, veri *Grilli Parlanti*, di aprire gli occhi ai possibili acquirenti per quanto riguarda i pericoli concernenti la sicurezza e la *privacy* nell'uso e nella gestione dei prodotti. Questo, sia detto per inciso, si è puntualmente verificato in Italia per quanto riguardava l'introduzione del Voip, del RFID, del WiFi, delle applicazioni biometriche nell'ambito delle P.A. ed ora si sta verificando anche per la promozione del *cloud computing* e la sua adozione nel settore pubblico. Staremo a vedere!

Vi ringrazio per la Vostra attenzione.

computing come "*Una completa idiozia. Al peggio, una campagna di marketing in un'industria legata alle mode anche più di quella dell'abbigliamento femminile*". Vedi anche in argomento l'intervento reso da STALLMAN in occasione di una visita all'Università delle Calabrie, riportato nell'articolo dal titolo *Richard Stallman: l'ultimo degli hacker*, in *www.linuks-magazine.it* nel quale ha sostenuto, senza mezzi termini che "*… il cloud computing limita, e non poco, le nostre libertà soprattutto in tema di sicurezza e di privacy*".

Infine vedi l'articolo di B. WAFFING, *Richard Stallman: cloud computing a trap*, in *www.linuks-magazine.com*, 1° ottobre 2008.

CAPITOLO 1

Possesso di pornografia infantile, accesso a siti pedopornografici, *child-grooming* e tecniche di anticipazione della tutela penale[1]

di *Ivan Salvadori*

SOMMARIO: 1. Introduzione. – 2. Le fonti regionali ed internazionali nella lotta alla pedopornografia. – 3. Il reato di possesso di materiale pedopornografico. Cenni di diritto comparato. – 4. Il mero reato di accesso a materiale pedopornografico. – 5. Il reato di adescamento di minori *on line* (*child-grooming*). – 6. Considerazioni finali.

1. Introduzione

Se da un lato le reti di comunicazione ed in specie Internet hanno favorito la realizzazione di rapporti sociali, economici e giuridici tra gli internauti, dall'altro hanno permesso a soggetti malintenzionati e veri e propri criminali informatici di sfruttare le molteplici possibilità di anonimato in rete ed i costi molto ridotti di connessione per commettere attività illecite di varia natura (frodi, clonazione di carte di credito, accessi abusivi, danneggiamenti informatici, ecc.). Recenti studi hanno dimostrato in particolare come la diffusione di Internet abbia facilitato anche la produzione, la diffusione e la messa a disposizione in tempo reale di pornografia infantile[2].

Molte sono ad oggi le iniziative adottate a livello regionale (Unione Europea, Commonwealth, OAS, ecc.) ed internazionale (ONU, ITU, Consiglio d'Europa) per contrastare l'abuso e lo sfruttamento sessuale dei minori, che si realizza anche attraverso le nuove tecnologie.

Per dare esecuzione agli obblighi di fonte sovranazionale, la maggior parte degli Stati ha adottato nel diritto penale nazionale delle norme *ad hoc* per reprimere l'odioso fenomeno della pornografia infantile. Quasi tutti gli Stati europei puniscono oggi le condotte di diffusione, produzione, distribuzione, ed anche il mero possesso o la detenzione di materiale pedopornografico. Alcuni Paesi, in linea con le più recenti tendenze politico-criminali sovranazionali, sanzionano altresì gli ulteriori atti prodromici di accesso, attraverso le tecnologie dell'informazione, a materiale pedopornografico e di adescamento di minori in Internet (o c.d. *child-grooming*).

Gli sforzi realizzati dagli organismi sovranazionali e dai legislatori nazionali per contrastare la pornografia infantile non possono che essere condivisi. Qualche dubbio sorge tuttavia rispetto all'impiego di determinate tecniche di tutela, ed in specie quelle volte ad incriminare meri atti preparatori alla commissione di reati di sfruttamento e prostituzione minorile. Dati i limiti del presente lavoro, in questa sede ci si limiterà a formulare delle brevi considerazioni

[1] Il presente contributo è frutto dell'attività di ricerca svolta nell'ambito del Progetto di Ateneo *Criminalità informatica ed accertamento penale* (codice CPDA084200/08), finanziato dall'Università degli Studi di Padova.

[2] V. per esempio U.S. Dep't of Justice, Child Exploitation & Obscenity Section (CEOS), *http://www.justice.gov/criminal/ ceos/childporn.html*.

sulla conformità delle recenti tendenze politico-criminali nella lotta alla pornografia infantile ai principi fondamentali del diritto penale, ed in specie a quelli di offensività e di proporzione.

Nella prima parte del presente contributo si richiameranno le più importanti iniziative adottate da organismi sovranazionali per combattere la pornografia infantile ed in particolare ci si soffermerà su quelle che impongono agli Stati di incriminare anche meri atti preparatori alla commissione di più gravi reati contro i minori (par. 2). Successivamente si passerà ad analizzare in prospettiva comparata le tecniche di formulazione adottate a livello nazionale per dare attuazione agli obblighi sovranazionali di incriminazione del possesso di materiale pornografico (par. 3), dell'accesso a siti pedopornografici (par. 4) e dell'adescamento di minori in rete o c.d. *child-grooming* (par. 5). L'obiettivo sarà quello di individuare la *ratio* che sta alla base del ricorso a forme di anticipazione della tutela penale. In conclusione si formuleranno delle considerazioni finali sulla conformità delle scelte politico-criminali di sanzionare i menzionati atti preparatori rispetto ai fondamentali principi penalistici (par. 6).

2. Le fonti regionali ed internazionali nella lotta alla pedopornografia

Tra le principali iniziative adottate a livello sovranazionale nella lotta alla pedopornografia vanno menzionate, oltre alla Convenzione sui Diritti dell'infanzia del 1989[3] ed al Protocollo Opzionale sui diritti del minore rispetto alla pornografia minorile e alla prostituzione delle Nazioni Unite adottato a New York nel 2000[4], la Raccomandazione del Consiglio d'Europa R(2001)16 sulla protezione dei minori contro lo sfruttamento sessuale[5] e la Decisione quadro dell'Unione europea 2004/68/GAI, sulla lotta allo sfruttamento sessuale dei minori e la pornografia infantile[6]. Di particolare importanza sono poi la Convenzione *Cybercrime* del 2001[7] e sopratutto la recente Convenzione di Lanzarote del 2007 del Consiglio d'Europa sulla protezione dei minori contro lo sfruttamento sessuale e l'abuso sessuale, che rappresenta oggi uno degli strumenti più avanzati a livello internazionale nella lotta alla pornografia infantile[8].

Già nella Raccomandazione R (2001)16, si prevedeva l'obbligo per gli Stati membri di sanzionare, oltre agli atti non autorizzati ed intenzionali di produzione, offerta e messa a disposizione di materiale pedopornografico, anche quelli preparatori del possesso e del procurare per sé o per altri tale materiale.

[3] Il testo della Convenzione è disponibile al sito *http://www2.ohchr.org/english/law/crc.htm.*

[4] Il testo del Protocollo Opzionale è disponibile al sito*: http://www2.ohchr.org/english/law/crc-sale.htm.*

[5] Il testo della Raccomandazione è disponibile sul portale del Consiglio d'Europa al sito: *https://wcd.coe.int/ViewDoc.jsp?id=234247&BackColorInternet=9999CC&BackColorIntranet=FFBB 55&Back Color ogged=FFAC75.*

[6] Il testo della Decisione Quadro 2004/68/GAI è disponibile al sito: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?Uri=CELEX:32004F0068:EN:HTML*.

[7] Il testo della Convenzione di Budapest adottata il 23 settembre 2001 ed entrata in vigore il 1° luglio 2004, è consultabile al sito: *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG*. Ad oggi sono trentadue gli Stati che hanno ratificato la Convenzione fra cui l'Italia. Sugli strumenti di ratifica v. *http://conventions.coe.int/ Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF= &CL=ENG*.

[8] Il testo della Convenzione di Lanzarote, entrata in vigore il 1° luglio 2010, è disponibile al sito *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=17/06/2010&CL=ENG*. La Convenzione è stata ad oggi sottoscritta da quarantadue Paesi e ratificata da quindici Paesi, ma non dall'Italia. Sul numero aggiornato delle ratifiche v. il *database* del Consiglio d'Europa al sito *http://conventions.coe.int/Treaty/Commun/QueVoulez Vous.asp?NT=201&CM= 8&DF=21/06/2010&CL=ENG*.

L'art. 9 della Convenzione *Cybercrime* del Consiglio d'Europa prescrive agli Stati membri di punire la produzione, la distribuzione, la diffusione, la messa a disposizione, l'acquisto ed il possesso di materiale pedopornografico. Rispetto alla Raccomandazione R (2001)16, la Convenzione *Cybercrime* lascia, però, agli Stati membri la facoltà di non sanzionare, in tutto o in parte, il mero possesso o il procurare per sé o per altri materiale pornografico (art. 9, par. 4, CoC). L'art. 9, par. 2, CoC, stabilisce che nella nozione di pornografia infantile rientri non solo il materiale reale, ma anche quello realistico e virtuale [9].

Ben più avanzate sono le scelte di politica criminale cui si ricorre nella recente Convenzione di Lanzarote. Con riguardo alla repressione degli illeciti in materia di pornografia infantile, l'art. 20 della Convenzione, in linea con le precedenti raccomandazioni, prevede l'obbligo per gli Stati membri di sanzionare la produzione, la messa a disposizione, la diffusione, l'offerta ed il possesso di materiale pedopornografico. Rispetto alla Convenzione *Cybercrime*, si restringe, però, il margine di discrezionalità degli Stati membri con riguardo all'incriminazione del possesso di materiale pornografico infantile. In base all'art. 20, par. 3, della Convenzione, agli Stati membri è infatti lasciata la facoltà di non punire il possesso di pedopornografia soltanto nei casi in cui abbia ad oggetto rappresentazioni simulate o immagini realistiche di minori non esistenti o comunque immagini prodotte dagli stessi minori con il loro consenso e per un utilizzo privato.

La Convenzione di Lanzarote prevede inoltre l'incriminazione di due atti ulteriormente preparatori: il mero accesso consapevole, attraverso le tecnologie dell'informazione e della comunicazione, a siti pedopornografici (art. 20, par. 1, lett. f) ed il c.d. *child-grooming* (art. 23).

Tra le iniziative legislative adottate dall'Unione europea nella lotta alla pornografia infantile merita richiamare in questa sede la Decisione Quadro 2004/68/GAI, che impone agli Stati membri l'obbligo di sanzionare penalmente una serie di illeciti in materia di "sfruttamento sessuale dei minori" (art. 2) e di "pornografia infantile" (art. 3) e, tra quest'ultimi, anche il *possesso* di materiale pornografico minorile, tra cui è incluso anche quello "virtuale" ed "apparente" (art. 1, lett. b, ii) e iii).

Il breve quadro fin qui delineato sulle fonti sovranazionali nella lotta alla pedopornografia deve oggi essere aggiornato alla luce della recente proposta di direttiva della Commissione europea sulla lotta contro l'abuso sessuale e allo sfruttamento sessuale dei minori e contro la pornografia minorile, destinata a sostituire la Decisione Quadro 2004/68/GAI [10]. Nella proposta vengono previste nuove forme di anticipazione della tutela penale. In particolare si prevede l'obbligo per gli Stati membri di punire, oltre all'acquisto ed il possesso di materiale pedopornografico (art. 5, par. 2), anche il mero accesso, attraverso le nuove tecnologie, a siti pedopornografici (art. 4, lett. e) ed il c.d. *child-grooming* (art. 6).

Rispetto alle menzionate fonti sovranazionali, la proposta di direttiva si caratterizza non solo per la maggior forza vincolante, non essendo prevista la facoltà per i legislatori nazionali di formulare riserve sulle scelte di incriminazione, ma anche per l'ulteriore anticipazione della tutela penale. Oltre ai menzionati atti preparatori del possesso di immagini di minori abusati,

[9] Come si afferma nel Rapporto esplicativo alla Convenzione di Lanzarote, la nozione di pedopornografia abbraccia "*depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer*" (*Explanatory Report*, p. 101).

[10] Il testo della proposta di Direttiva del Parlamento europeo e del Consiglio, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la Decisione Quadro 2004/68/GAI (COM (2010) 94 def.), è disponibile al sito *http://eur-lex.europa.eu/LexUriServ.do?uri=CELEX:52000PC0854 (02):EN:HTML*.

dell'accesso a siti pedopornografici e dell'adescamento *on line* per scopi sessuali, essa prevede l'obbligo per gli Stati membri di sanzionare già il *tentativo* di acquistare e possedere materiale pedopornografico (art. 7, par. 2), l'organizzazione di viaggi finalizzati a commettere abusi sessuali a danno di minori (art. 7, par. 3, lett. b) e la diffusione di materiale che *propaganda* la possibilità di commettere reati di sfruttamento minorile, di pedopornografia e di adescamento (art. 7, par. 3, lett. a).

Quest'ultima disposizione rappresenta un'evidente manifestazione di un diritto penale c.d. pre-preventivo, che sanziona la mera formazione di un atteggiamento criminale interiore in altri soggetti. Essa prevede che gli Stati puniscano la diffusione di materiale che *propaganda* non solo la possibilità di acquistare o detenere materiale pedopornografico, ma anche di *accedere* a pagine *web* contenenti materiale di analoga natura.

3. Il reato di possesso di materiale pedopornografico. Cenni di diritto comparato

In linea con le indicazioni di fonte sovranazionale, la maggior parte degli Stati europei punisce oggi il possesso o la detenzione di materiale pornografico minorile [11].

Il codice penale tedesco sanziona oltre al possesso ("*Besitz*") di materiale pedopornografico (§ 184b, par. 4.2, StGB), anche il fatto di chi si procura ("*sich verschaffen*") tale materiale (§ 184b, par. 4.1, StGB) [12]. Secondo autorevole dottrina si tratta di un delitto di omissione propria, avente natura permanente [13]. Il possesso consiste nel "causare" o nel mantenere un rapporto di effettiva signoria sul materiale posseduto [14]. Tale relazione implica pertanto la possibilità da parte del possessore di accedere e disporre del menzionato materiale.

Nel diritto penale tedesco la nozione di possesso viene interpretata in senso più ampio rispetto a quella elaborata in ambito civilistico, per abbracciare i casi non solo di possesso immediato, ma anche mediato, purché il possessore abbia la possibilità di disporre del materiale [15]. Si pensi per esempio al soggetto che possieda le chiavi di una cassaforte nella quale sono conservate immagini pornografiche minorili. Lo stesso dicasi nel caso in cui un soggetto possieda una *password* che gli permetta di accedere ad un *computer,* che contiene *file* di analogo contenuto [16]. Anche la sola possibilità di controllare temporaneamente il materiale archiviato in un sistema informatico sarebbe sufficiente ad integrare, secondo parte della dottrina, la fattispecie di possesso di materiale pornografico.

Il § 184b, par. 4.1, StGB punisce anche chi *si procura* ("*sich verschaffen"*) analogo materiale. Tale ipotesi abbraccia non solo l'acquisizione temporanea del possesso, ma anche le forme di appropriazione unilaterale del materiale (ad es. mediante il furto) [17].

---

[11] Per un'analisi in prospettiva comparata sia consentito rinviare a I. SALVADORI, *Legal problems of possession and viewing child pornography in the Internet*, in J. HERCZEG-E. HILGENDORF-T. GRIVNA (Hrsg.), *Internet kriminalität und die neuen Herausforderungen der Informationsgesellschaft des 21. Jahrunderts*, Praha, 2010, p. 55 ss.

[12] § 184b(4) StGB: "*Wer es unternimmt, sich den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer die in Satz 1 bezeichneten Schriften besitzt*".

[13] T. LENCKER-W. PERRON, § 184 StGB, in A. SCHÖNKE-H. SCHRÖDER (Hrsg.), *Strafgesetzbuch*, *Kommentar*, 26ª ed., München, 2001, p. 1520.

[14] BT-DRUCKS, 12/3001, 5. In dottrina v. K. ECKSTEIN, *Besitz als Straftat*, Berlin, 2001, p. 109 ss.

[15] Cfr. T. LENCKER-W. PERRON, § 184 StGB, p. 1521. *Contra* K. ECKSTEIN, *Besitz*, cit., p. 112, il quale ritiene che non sia sufficiente la possibilità di controllare il materiale, ma occorra che vi sia un controllo di fatto sul materiale stesso per poter parlare di possesso.

[16] T. LENCKER-W. PERRON, § 184 StGB, p. 1521.

[17] T. LENCKER-W. PERRON, § 184 StGB, p. 1521.

Anche il legislatore francese, in linea con le raccomandazioni di fonte sovranazionale, ha sanzionato la mera detenzione di materiale pornografico infantile. L'art. 227-23-5, introdotto nel *Code Pénal* con la legge 305/2002, punisce, con la pena della reclusione fino a 2 anni e l'ammenda, la detenzione di immagini o rappresentazioni pedopornografiche [18].

Nel diritto penale francese la nozione di detenzione è interpretata in senso più ampio rispetto a quella civilistica. Dottrina e giurisprudenza maggioritaria riconducono al concetto di detenzione anche i casi c.d. di "*longa manu"*, vale a dire le ipotesi in cui, sebbene il materiale sia custodito presso un terzo, il soggetto ne mantenga comunque la disponibilità [19]. Ne consegue, che l'internauta che salva su un determinato *server* delle immagini o dei video pedopornografici e mantenga la possibilità di accedervi, sarà penalmente sanzionato ai sensi dell'art. 227-23-5 *Code Pénal* [20].

La detenzione di materiale pedopornografico è punita anche in Italia. L'art. 600-*quater* c.p. sanziona oltre alla "*detenzione*", anche il fatto di "*procurarsi*" materiale pornografico realizzato utilizzando minori degli anni diciotto. Il secondo comma dell'art. 600-*quater* c.p. prevede un aumento della pena nel caso in cui il soggetto detenga o si procuri materiale pedopornografico di ingente quantità. È quest'ultima una soglia indeterminata, che solleva forti perplessità circa il rispetto dei principi penalistici di tassatività e di precisione [21].

L'ipotesi tipica del "procurarsi" abbraccia tutti quei comportamenti destinati a far entrare nella sfera di disponibilità del soggetto il materiale pornografico minorile. Si pensi per esempio a tutti le condotte volte a procurarsi il menzionato materiale, che si possono facilmente realizzare in Internet (mediante *download*, utilizzo di programmi di *file-sharing*, P2P, ecc.)

Il possesso di materiale pornografico minorile viene punito anche in molti altri Stati europei ed extra-Europei, come ad esempio in Spagna (art. 189.2 CP), in Belgio (art. 383-*bis*, par. 2, *Code Penal*), in Austria (§ 207a, par. 3, StGB), in Romania (art. 51, L. 161/2003), in Messico (artt. 202, 202-*bis* CP), in Colombia (art. 218 CP), in Argentina (art. 128. 2 CP), in Canada (Section 163.1(4) *Criminal Code*) ed anche negli Stati Uniti d'America, a livello tanto federale (§ 2252A US Code) quanto statale (ad es. in Alaska, Florida, Tennessee, ecc.).

4. Il reato di mero accesso a materiale pedopornografico

L'orientamento giurisprudenziale prevalente in molti Stati europei sostiene che la mera visualizzazione di materiale pedopornografico disponibile in Internet, senza la consapevolezza che a seguito della navigazione in rete una copia delle immagini visualizzate venga automaticamente salvata dal *browser* nella memoria temporanea del sistema informatico (c.d. copie *cache*), non integri gli estremi del delitto di possesso di materiale pedopornografico [22].

[18] Art. 227-23-5 Code Pénal: "*Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende*".

[19] In argomento v. L.A. TIRELLI, *La répression pénal des consommateurs de pédopornographie á l'heure de l'Internet*, Geneve, 2010.

[20] L.A. TIRELLI, *La répression pénal*, cit.

[21] In argomento v. F. BRICOLA, *Le aggravanti indefinite. Legalità e discrezionalità in tema di circostanza del reato*, in *RIDPP*, 1964, 1019 ss. Sulla configurabilità dell'aggravante prevista dall'art. 600-*quater*, comma secondo, c.p. v. Cass., sez. III Pen., n. 17211 del 31 marzo 2011 (dep. 3 maggio 2011).

[22] Nella giurisprudenza italiana v., ad es., Trib. Brescia, sez. II pen., 22 aprile 2004, sent. n. 1619/2004, laddove si afferma che l'art. 600-*quater* c.p. "*punendo chi 'si procura o dispone' di materiale illecito, e non chi, semplicemente, lo visiona, consente lo svolgimento della pretesa punitiva non nei confronti di tutti coloro che,*

Come si è correttamente sostenuto, il possesso si configura soltanto nei casi in cui l'internauta, oltre ad essere consapevole dell'esistenza di una copia del materiale visionato nella memoria *cache* del proprio sistema, sia anche in grado di accedervi [23].

Questa impostazione, seppur corretta, ha portato ad una disparità di trattamento tra gli utenti in possesso di un discreto livello di conoscenze sul funzionamento dei sistemi e dei programmi *browser* per la navigazione in Internet e quelli privi di una minima alfabetizzazione informatica [24]. Gli internauti inconsapevoli del funzionamento del *browser* e dell'esistenza delle copie *cache* possono, infatti, accedere e visualizzare immagini e video pornografici in Internet senza alcuna conseguenza sul piano penale. Lo stesso dicasi con riguardo alle condotte di quei soggetti che accedono ai siti pedopornografici utilizzando *computer* di terzi soggetti o da postazioni pubbliche (ad es., *Internet Point*, biblioteche, ecc.). Tali utenti, anche nell'ipotesi in cui fossero consapevoli che le immagini visionate si salvano nei c.d. *file* temporanei di Internet, non potrebbero rispondere del reato di possesso di materiale pedopornografico, in quanto non hanno per un tempo apprezzabile la disponibilità e di conseguenza la possibilità di accedere al materiale temporaneamente salvato sul sistema informatico altrui.

Con l'obiettivo di superare questa evidente disparità di trattamento negli ultimi anni sempre più Stati europei ed extra europei hanno ritenuto opportuno punire, in linea con la tendenza politico-criminale che si è affermata a livello sovranazionale (v. *supra*, par. 2), la condotta di accesso consapevole a materiale pornografico infantile, realizzato attraverso le tecnologie informatiche e della comunicazione.

L'accesso consapevole a siti pedopornografici è penalmente sanzionato, per esempio, in Canada nel 2002. Il § 163.1(4.1) del Codice federale canadese punisce chiunque accede consapevolmente a materiale pedopornografico con il fine di visionarlo o di diffonderlo ad altri [25]. Il § 2252(a)(4) del codice federale statunitense sanziona dal 2007 chiunque accede consapevolmente ad uno o più libri, riviste, periodici, film a contenuto pedopornografico o ad altro materiale analogo con il fine di prenderne visione [26]. Tale condotta è punita anche a livello statale (ad es. in Nevada, Ohio e New Jersey) [27].

---

navigando in internet, 'entrino in contatto', semplicemente, con immagini aventi quel contenuto, ma coloro che 'se ne approprino', 'salvandole' e veicolandole o sul disco fisso del p.c. o su altri supporti, con esso interfacciabili, che ne consentano la visione o comunque la riproduzione. Lo 'scaricamento' dei materiali, ovviamente, deve essere consapevole e volontario, dovendosi escludere profili di responsabilità penale nei casi in cui il materiale rinvenuto sul p.c. costituisca la mera traccia di una trascorsa consultazione del web, creata dai sistemi di salvataggio automatico del personal computer". Nella giurisprudenza statunitense v. *United States v. Stulock*, 308 F. 3d 922 (8th Cir. 2002) In argomento v. anche I. SALVADORI, *Legal problems of possession*, cit., p. 55 ss.

[23] Nella giurisprudenza statunitense v., ad es., *Unitd States v. Stulock*, cit.; *United States v. Kuchinski*, 469 F. 3d 853 (9th Cir. 2006).

[24] In argomento v. I. SALVADORI, *Legal problems of possession*, cit., p. 55 ss., ed ivi riferimenti alla dottrina e giurisprudenza straniera.

[25] Sec. 163.1 (4.1) Canadian Criminal Code: "*every person who accesses any child pornography is guilty of (a) an indictable offence and liable to imprisonment for a term not exceeding five years and to a minimum punishment of imprisonment for a term of forty-five days; or (b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of fourteen days*".

[26] 18 U.S.C. § 2252(a)(4): "*in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction*".

[27] Cfr. I. SALVADORI, *Legal problems of possession*, cit.

L'accesso ai menzionati siti è sanzionato dal 2007 anche in Francia. L'art. 227-23-5 *Code Pénal* punisce "chiunque consulta abitualmente pagine *web*, che mettono a disposizione materiale pedopornografico"[28].

Come si è già avuto modo di accennare (v. *supra*, par. 2), anche il Consiglio d'Europa ha recentemente affermato l'obbligo di sanzionare la condotta di mero accesso, a mezzo di tecnologie dell'informazione e della comunicazione, a materiale pornografico minorile. L'art. 20, par. 1, lett. f) della Convenzione di Lanzarote limita la rilevanza penale alle sole condotte di accesso intenzionale a siti pedopornografici. Come si sostiene nel rapporto esplicativo della Convenzione, il carattere intenzionale dell'accesso può dedursi, per esempio, dalla frequenza con cui il soggetto consulta in rete il materiale o dal ricorso a servizi a pagamento, onde escludere la rilevanza penale del mero accesso fortuito o inconsapevole[29].

La *ratio* della norma è quella di punire gli internauti che si limitano a visionare il materiale illecito disponibile in rete, senza salvarne una copia sul proprio *computer*. Simili sono le motivazioni addotte dalla Commissione europea per giustificare l'introduzione, nella recente proposta di direttiva COM (2010) 94 def., dell'obbligo di sanzionare l'accesso consapevole alla pornografia minorile (art. 4, lett. e). Scopo della disposizione è quello di sanzionare le condotte degli utenti che accedono al materiale *on line* senza scaricarlo sul proprio *computer* e che in molti ordinamenti giuridici non possono essere sussunte nel reato di possesso di materiale pedopornografico per le ragioni sopra esaminate.

5. Il reato di adescamento di minori *on line* (*child-grooming*)

Altro paradigmatico atto preparatorio alla commissione di reati di abuso sfruttamento sessuale dei minori è rappresentato dal reato di adescamento di minori in rete o c.d. *child-grooming*.

L'art. 23 della Convenzione di Lanzarote prescrive agli Stati membri l'obbligo di sanzionare l'adescamento di minori per scopi sessuali ("*solicitation of children for sexual purposes*"), vale a dire la condotta di chi, attraverso le tecnologie dell'informazione e della comunicazione, propone ad un minore un incontro con il fine di commettere atti e dunque reati sessuali, qualora a tale proposta conseguano condotte materiali finalizzate a realizzare tale incontro[30].

Sostanzialmente identica è la formulazione del reato di *child-grooming* previsto dalla recente proposta di direttiva della Commissione europea. L'art. 6 della proposta prevede l'obbligo per gli Stati membri di sanzionare la condotta dell'adulto che propone, a mezzo di tecnologie dell'informazione e della comunicazione, a un minore che non ha raggiunto l'età del consenso sessuale prevista dalla normativa nazionale di incontrarlo con l'intento di commettere un abuso sessuale, se la proposta sia stata seguita da atti materiali finalizzati a tale incontro.

La condotta di *child-grooming* viene già penalmente sanzionata in molti Stati europei ed

[28] Art. 227-23-5 Code Pénal: "*Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende*".

[29] *Explanatory Report*, cit., p. 140.

[30] Art. 23 Convention of Lanzarote: "*Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting*".

extra-europei[31]. L'art. 172.1 del codice penale canadese sanziona dal 2007 la condotta di chi comunica, attraverso un sistema di informazione, con un minorenne al fine di commettere un reato sessuale[32]. Il *child-grooming* è sanzionato anche negli Stati Uniti d'America. Il § 2422 (b) del codice federale statunitense sanziona chiunque impiega la posta od altro mezzo analogo per indurre un minore a subire un atto sessuale[33]. Sostanzialmente simile è la fattispecie di adescamento *on line* di minori (o "*electronic solicitation of children*") prevista in molti Stati americani[34].

L'adescamento di minori in rete è punito anche in Inghilterra e Galles. La sec. 15 del *Sexual offences Act* del 2003 punisce l'adulto che tenta di incontrarsi con un minore per commettere atti sessuali[35].

Anche il legislatore spagnolo, con la recente legge organica n. 5/2010, di riforma del codice penale, ha sanzionato l'adescamento di minori (o "*ciber-acoso*")[36]. Il nuovo art. 183-*bis* c.p. punisce la condotta di "*chi contatta, attraverso Internet, per telefono o con altri mezzi tecnologici, un minore di 13 anni, proponendogli di fissare un incontro al fine di commettere delitti di sfruttamento sessuale a danno del minore, purché a tale proposta seguano atti materiali finalizzati a tale incontro*"[37]. Al secondo comma dell'art. 183-*bis* c.p. si prevede un au-

[31] Per un'analisi comparata v. K. KWANG RAYMOND CHOO, *Online child grooming: a literature review on the misuse of social networking sites for sexual offences*, *Australian Institute of Criminology*, 2009; S. OST, *Child pornography and sexual grooming*, Cambridge, 2009.

[32] Sec. 172.1 (1) Canadian Criminal Code: "*every person commits an offence who, by means of a computer system within the meaning of subsection 342.1(2), communicates with (a) a person who is, or who the accused believes is, under the age of eighteen years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155 or 163.1, subsection 212(1) or (4) or section 271, 272 or 273 with respect to that person; (b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 280 with respect to that person; or (c) a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person*".

[33] 18 U.S.C. § 2422: (b): "*Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life*".

[34] Per un quadro della legislazione statale americana in materia di *child-grooming* v. il sito *http://www.ncsl.org/default.aspx?tabid=13448*.

[35] Sec. 15(1) Sexual Offences Act: "*A person aged 18 or over (A) commits an offence if (a) having met or communicated with another person (B) on at least two earlier occasions, he (i)intentionally meets B, or (ii) travels with the intention of meeting B in any part of the world, (b) at the time, he intends to do anything to or in respect of B, during or after the meeting and in any part of the world, which if done will involve the commission by A of a relevant offence, (c) B is under 16, and (d) A does not reasonably believe that B is 16 or over*".

[36] Più in generale, sui nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010 sia consentito rinviare a I. SALVADORI, *Los nuevos delitos informáticos introducidos en el Código Penal español con la ley orgánica n. 5/2010. Perspectiva de derecho comparado*, in *Anuario de Derecho Penal y Ciencias Penales*, 2010 (in corso di pubblicazione), ed ivi riferimenti bibliografici.

[37] Art. 183-*bis* CP: "*El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño*". Per un primo commento all'art. 183-*bis* CP v. T.S. VIVES ANTON-E. ORTS BERENGUER-J.C. CARBONELL MATEU-J.L. GONZALEZ CUSSAC-C. MARTINES-BUJAN PEREZ, *Derecho*

mento della pena nel caso in cui il contatto con il minore avvenga attraverso coazione, inganno o intimidazione.

In Italia la condotta di *child-grooming* non è, *de jure condito*, penalmente rilevante. Va detto però che il 23 marzo 2009 è stato presentato alla Camera dei Deputati, su iniziativa del Ministro degli Affari Esteri, del Ministro della Giustizia e del Ministro delle Pari Opportunità, il disegno di legge n. 2326, di "*ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguamento dell'ordinamento interno*", che prevede, tra l'altro, l'introduzione nel codice penale di un nuovo art. 609-*undecies* per punire l'adescamento di minori. Il disegno di legge è stato approvato con modifiche alla Camera lo scorso 11 gennaio 2011 ed attualmente è in fase di esame nelle Commissioni riunite 2a (Giustizia) e 3a (Affari Esteri ed immigrazione) del Senato [38].

L'art. 609-*undecies* c.p., nell'ultima formulazione modificata dalla Camera (d.d.l. 2326-b), sanziona "*chiunque, allo scopo di commettere i reati di cui agli artt. 600, 600-bis, 600-ter e 600-quater c.p., anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies c.p., adesca un minore di anni sedici*".

Per superare le difficoltà già sorte in giurisprudenza con riguardo all'interpretazione del concetto di adescamento, richiamato dall'art. 600-*ter*, terzo comma, c.p., il legislatore ha ritenuto di definire espressamente tale nozione. In base all'art. 609-*undecies*, secondo comma, c.p., previsto dal d.d.l. 2326-b, per adescamento si intende "*qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione*".

L'art. 609-*undecies* c.p. si configura come una fattispecie a dolo specifico [39]. Ne consegue che la condotta oggettiva di adescamento dove essere strumentale al perseguimento di uno dei fini tipizzati dal legislatore, vale a dire la riduzione o il mantenimento in schiavitù di un minore (art. 600 c.p.), l'induzione alla prostituzione (art. 600-*bis* c.p.), l'utilizzo del minore per esibizioni pedopornografiche o per la produzione di analogo materiale (art. 600-*ter* c.p.) o per procurarsi o detenere materiale pornografico (art. 600-*quater* c.p.), anche se virtuale (art. 600-*quater*.1 c.p.), l'organizzazione o la propaganda di viaggi finalizzati alla fruizione di attività di prostituzione minorile (art. 600-*quinquies* c.p.), la realizzazione di una violenza sessuale (art. 609-*bis* c.p.) o di atti sessuali con minorenne (art. 609-*quater* c.p.), la corruzione di monorenne (art. 609-*quinquies* c.p.) o la violenza sessuale di gruppo (art. 609-*octies* c.p.).

L'elemento finalistico della fattispecie è descritto in modo più ampio rispetto a quello dell'art. 23 della Convenzione di Lanzarote, che si riferisce soltanto alla finalità di produrre materiale pedopornografico o di utilizzare un minore per esibizioni pornografiche (art. 20) e a quello dell'art. 6 della proposta di direttiva COM (2010) 94 def., che abbraccia soltanto la produzione di materiale pedopornografico e la commissione di atti sessuali con minori.

Il fatto tipico dell'adescamento deve costituire un mezzo teleologicamente orientato a perseguire uno dei menzionati fini tipizzati dal legislatore. Essendo il fine tipizzato un elemento costitutivo della tipicità (fatto base dell'adescamento e fine soggettivo), ne consegue che il nesso teleologico (tra il fatto base dell'adescamento ed il fine soggettivo perseguito)

penal, *Parte especial*, III ed., Valencia, 2010, pp. 269-271; J.J. QUERALT JIMENEZ, *Derecho penal español, Parte especial*, VI ed., Barcelona, 2010, p. 240 ss.

[38] Ulteriori informazioni sull'iter del d.d.l. n. 2326 del 2009 sono disponibili sul portale del Senato al sito *http://www.senato.it/leg/16/BGT/Schede/Ddliter/36302.htm.*

[39] Sulla struttura delle fattispecie a dolo specifico v., tra tutti, L. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993.

dovrà essere dimostrato già al momento dell'accertamento della condotta realizzata in rete dall'adulto[40]. Ciò esclude che il giudice possa ricorrere ad illegittime presunzioni o al mero apprezzamento semantico delle parole utilizzate nel tentativo di acquistare, attraverso l'impiego dei mezzi tecnologici, la fiducia del minore per convincerlo ad accettare l'invito ad un incontro. Nel provare la finalità di commettere uno dei delitti sessuali richiamati dalla fattispecie, l'organo giudicante dovrà tener conto anche di indici rivelatori ulteriori rispetto alla mera realizzazione oggettiva della condotta, che risultino idonei a dimostrare la sua strumentalità al perseguimento di una delle finalità illecite richiamate dalla norma. A tal fine il giudice potrà ricorrere ad elementi ulteriori rispetto al mero comportamento materiale, quali per esempio il contesto in cui si realizza la condotta (ad esempio una *chat-room* di pedofili), ed altri elementi idonei a dimostrare fin dall'inizio che la sua condotta è stata posta in essere quale mezzo per perseguire quel fine.

6. Considerazioni finali

Da questa breve analisi comparata delle legislazioni penali nazionali e dal richiamo alle più recenti fonti sovranazionali emerge in modo chiaro come sia sempre più frequente nella lotta alla pornografia infantile il ricorso a forme di anticipazione della tutela penale. Paradigmatiche, come si è visto, sono le fattispecie di mero possesso di materiale pornografico minorile, di accesso, mediante le tecnologie dell'informazione e della comunicazione, a siti pedopornografici e di adescamento di minori *on line* (o *child-grooming*). L'incriminazione di questi atti preparatori alla commissione di più gravi reati di sfruttamento sessuale dei minori e di pornografia infantile sollevano notevoli perplessità dal punto di vista dogmatico e politico-criminale.

Rispetto al reato di possesso di materiale pedopornografico, risulta difficile determinare il concreto interesse giuridico protetto dalla norma[41]. Quest'ultimo non può di certo essere individuato nell'integrità sessuale dei minori vittime di abuso sessuale. È evidente, infatti, che il possesso di materiale pedopornografico prodotto attraverso l'abuso e lo sfruttamento di minori è un atto che si colloca in una fase temporalmente successiva rispetto alla concreta lesione dell'integrità sessuale e fisica dei minori, oggetto della rappresentazione pornografica.

Tre sono in sintesi le principali motivazioni addotte dalla dottrina per legittimare l'incriminazione del possesso di materiale pornografico minorile.

Secondo un primo orientamento, il possesso di materiale pedopornografico ne stimolerebbe la produzione e di conseguenza anche gli atti di abuso e di sfruttamento dei minori per produrli. Si è così sostenuto che chi possiede immagini pedopornografiche sarebbe (indirettamente) responsabile anche degli atti di produzione del materiale, dal momento che in quest'ambito vi è un forte vincolo tra offerta e domanda[42].

Questa argomentazione non può essere condivisa. È evidente che l'essere in possesso di pornografia infantile non implica necessariamente l'aver partecipato alla lesione dell'integrità sessuale dei minori strumentale alla produzione del materiale stesso. In questi casi il posses-

[40] Sull'accertamento del fine specifico, quale elemento costitutivo della tipicità, v. L. PICOTTI, *Il dolo specifico*, cit., 505.

[41] In argomento v. N. PASTOR MUÑOZ, *Los delitos de posesión y los delitos de estatus: una aproximación político-criminal y dogmática*, Barcelona, 2005, p. 90 ss.; nonché A. CADOPPI, *Sub art. 600 quater c.p.*, in ID., *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, 229-230.

[42] F.C. SCHROEDER, *Pornographieverbot als Darstellungschutz?*, in *Zrp*, 1990, p. 299 ss., ID., *Das 27. Strafrechtsänderungsgesetz – Kinderpornographie*, in *NjW*, 1993, p. 2582 ss.

sore potrebbe eventualmente essere punito per aver indotto un'altra persona a produrre il materiale con il fine di poterlo poi acquistare o di procurarlo per sé o per altri. Ma la *ratio* dell'incriminazione del possesso di materiale pornografico infantile non è certo quella di punire l'istigazione alla produzione. In questo caso si dovrebbe piuttosto configurare in capo al possessore una responsabilità a titolo di partecipazione morale, in quanto con la sua condotta egli ha determinato o comunque rafforzato il proposito criminoso altrui di produrre il materiale pedopornografico.

Forti perplessità solleva anche quell'orientamento che giustifica l'incriminazione del possesso di materiale pornografico minorile con il fine di evitare la commissione da parte del possessore di futuri reati sessuali a danno di minori[43]. Ad oggi mancano, infatti, seri studi scientifici che dimostrino con un certo grado di certezza l'esistenza di un nesso tra possesso di immagini e video pedopornografici ed il pericolo che in futuro il soggetto possa commettere abusi sessuali a danno di minori.

Più corretta sembra essere quella posizione, che in linea con le fonti sovranazionali, ritiene che il possesso debba essere punito in quanto non solo stimola la produzione e la domanda di tale materiale, ma perpetua l'offesa alla dignità dei minori vittime di tali reati[44]. La *ratio* dell'incriminazione del possesso risponderebbe pertanto ad una logica "post-consumativa", simile a quella che sta alla base del delitto di ricettazione[45]. Da un lato, ogniqualvolta il possessore di materiale pedopornografico usufruisca delle immagini in suo possesso, perpetua la lesione alla libertà ed alla dignità dei minori; dall'altro lato egli contribuisce al mantenimento e all'espansione di una nuova industria che ha come oggetto e presupposto la commissione di gravi reati sessuali a danno di minori. Ma se tale argomentazione permette di giustificare l'incriminazione del possesso di pedopornografia reale, altrettanto non si può dire rispetto alla pornografia minorile virtuale. In quest'ultimo caso è evidente come non vi sia alcuna lesione della libertà e della dignità di minori in "carne ed ossa" e resta da dimostrare che il possesso di immagini realizzate al *computer* stimoli il mercato della pornografia reale.

Forti perplessità solleva anche la scelta politico-criminale di punire l'accesso a siti pedopornografici. Innanzitutto si tratta di un mero reato di opinione, espressione di un diritto penale orientato ad una funzione meramente preventiva. La fattispecie abbraccia atti ambigui ed indeterminati, che hanno senza dubbio una forte valenza immorale, ma che non sono di per sé meritevoli di sanzione penale, in quanto non costituiscono una lesione o messa in pericolo concreto di un bene giuridico.

L'incriminazione della visualizzazione di materiale pornografico minorile contrasta inoltre con i fondamentali principi di diritto penale, ed in specie con quelli di offensività e proporzione. Dal mero accesso a materiale pedopornografico sorge il pericolo che l'utente procuri per sé o per altri immagini o video di minori, con l'ulteriore pericolo che, una volta ottenuto il materiale, possa offrirlo, metterlo a disposizione o diffonderlo ad altri utenti. Si tratta pertanto di un reato di pericolo indiretto che non punisce un atto di per sé illecito, ma il puro pen-

[43] A sostegno di tale orientamento v., ad es., le argomentazioni di L.S. SMITH, *Private possession of child pornography: narrowing at home privacy rights*, in *Ann. Surv. Am. L.*, 1991, p. 1043 ss.

[44] Secondo autorevole dottrina, la dimensione oggettiva del possesso di materiale pedopornografico virtuale andrebbe, quindi, riassunta "nel reale scambio o circolazione di messaggi comunicativi che pubblicizzano (propagandando o rendendo oggettivamente disponibili al pubblico) "modelli" di comportamento e di relazioni interpersonali, in cui è annullata la dignità e la libertà individuale dei fanciulli": così L. PICOTTI, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici*, in M. BERTOLINO, G. FORTI (a cura di), *Scritti per Federico Stella*, Napoli, 2007, 1320.

[45] In tal senso v., ad es., E. GIMBERNAT ORDEIG, *Prologo a la 5a ed del Código Penal*, Madrid, 2000, p. 19. In argomento v. anche N. PASTOR MUÑOZ, *Los delitos de posesión*, cit., p. 95 ss.

siero, *rectius* il sospetto che l'internauta acceda a dette immagini per procurarsi il materiale e poi diffonderlo ad altri. Tale delitto contrasta pertanto con il principio di offensività, dal momento che si sanziona un comportamento estremamente lontano dalla lesione o messa in pericolo concreto di un bene giuridico.

Va pertanto condivisa la scelta del legislatore italiano di avvalersi della facoltà concessa dalla Convenzione di Lanzarote di non sanzionare, come previsto nel menzionato disegno di legge n. 2632-b/2009, di ratifica della Convenzione stessa, il reato di accesso a siti pedopornografici, giustificando tale decisione per "i dubbi di costituzionalità di una norma [quella di accesso] che sanziona una condotta che potrebbe essere anche del tutto casuale" oltre che per le difficoltà probatorie, dal momento che non prevede in qualche modo lo scarico (*download*) del materiale visionato".

Resta infine da analizzare la legittimità dell'incriminazione delle condotte di *child-grooming*. Dalla breve analisi comparata (vedi *supra*, par. 5) è emerso come il reato di adescamento di minori presenti una tipica struttura di atto preparatorio alla commissione di più gravi reati contro la integrità e la dignità dei minori.

Non vi è dubbio che, anticipando la soglia del penalmente rilevante già alla fase delle condotte di mero adescamento in rete, si permetterebbe all'autorità giudiziaria di intervenire prima che il criminale possa commettere un delitto sessuale a danno di un minore. E proprio per l'importanza dell'interesse giuridico dell'integrità fisica e sessuale del minore risulterebbe ammissibile una tale anticipazione della tutela penale. Non sempre, però, la tecnica di formulazione della fattispecie di *child-gooming* appare essere rispettosa dei fondamentali principi di diritto penale. Ed è questo il caso del delitto di *grooming* previsto dall'art. 609-*undecies* c.p., del disegno di legge 2326-b/2009 di ratifica ed esecuzione della Convenzione di Lanzarote.

Innanzitutto la formulazione della fattispecie risulta essere indeterminata. Essa non richiede, come previsto per esempio dalla Convenzione di Lanzarote e dalla proposta di direttiva COM (2010) 94 def., che alla condotta di adescamento realizzata in rete faccia seguito un incontro con il minore o comunque vengano posti in essere concreti atti materiali finalizzati a realizzare tale incontro. Manca pertanto la previsione, quale requisito tipico della fattispecie, della sussistenza di un pericolo preciso e attuale per la realizzazione degli atti più gravi di sfruttamento sessuale a danno del minore, che deve necessariamente sussistere per legittimare l'incriminazione di atti preparatori [46].

E del tutto inutile, al fine di superare l'indeterminatezza della fattispecie, prevista dal ddl. 2326-b/2009, è la previsione della nozione di adescamento, al secondo comma dell'art. 609-*undecies* c.p., quale formulata nel citato d.d.l. Essa richiede soltanto la *direzione* della condotta a carpire la fiducia del minore, ma non la sua *idoneità* a raggiungere tale risultato. Onde superare i dubbi di legittimità di una simile definizione, è pertanto auspicabile che il legislatore provveda, in fase di discussione del disegno di legge, ad affiancare al requisito espresso della *direzione* degli atti di adescamento anche quello della loro *idoneità* a raggiungere il risultato cui sono diretti. In questo modo si eviterebbe che anche atti preparatori del tutto inidonei a mettere in pericolo il bene giuridico protetto possano essere ricondotti nell'alveo del delitto di adescamento di minori, di cui all'art. 609-*undecies* c.p. menzionato.

[46] In tal senso v. la risoluzione dell'AIDP, adottata ad Istanbul nel settembre 2009, su l'*Espansione delle forme di preparazione e di partecipazione al reato*, disponibile (in francese, inglese e spagnolo) in *Revue internationale de droit pénal*, 2006, 3-4, 613 ss.

CAPITOLO 2

La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del *Bundesverfassungsgericht* e della *Curtea Constituțională* su investigazioni ad alto contenuto tecnologico e *data retention*

di *Roberto Flor*

SOMMARIO: 1. Introduzione. – 2. La sentenza del *Bundesverfassungsgericht* sulla c.d. *Online Durchsuchung*. – 3. La sentenza del *Bundesverfassungsgericht* sul c.d. *data retention*. – 4. La sentenza della *Curtea Constituțională* della Romania sul c.d. *data retention*. – 5. Gli elementi argomentativi comuni dei Giudici delle Leggi. – 6. Conclusioni. Il contenuto essenziale del diritto fondamentale come rapporto fra libertà e limite nella Carta dei diritti dell'Unione Europea.

1. Introduzione

Internet ed i nuovi prodotti tecnologici rappresentano non solo un'opportunità per nuovi modi e tipi di comportamenti di rilievo penale, ma anche una nuova frontiera di lotta alla criminalità, che può offrire innovativi strumenti e mezzi per la ricerca delle prove, perseguendo altresì fini "preventivi".

I limiti costituzionali al potere coercitivo dello Stato, che può manifestarsi tramite gli strumenti processuali ed il conferimento di funzioni pubbliche ad organismi privati, quali gli *Internet Service Providers* (ISP), traspaiono da importanti decisioni di Corti costituzionali in Europa, il cui filo conduttore è costituito dal bilanciamento con i diritti fondamentali della persona.

Tali sentenze giungono in un delicato momento storico, in cui il ricorso alle "investigazioni tecnologiche" e all'accessibilità a dati ed informazioni trasmesse per via telematica devono confrontarsi con le esigenze di accertamento e di ricerca della prova ed il rispetto delle garanzie e dei diritti inviolabili dei cittadini [1].

In questo contesto le sentenze del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla

[1] 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.*, 2009, 3, p. 695 ss., nonché 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*, 2010, 11, 2, p. 359 ss. (con ampi riferimenti bibliografici). ID., *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constituțională*, in *Cass. pen.*, 2011, p. 1952 ss.

c.d. *Online Durchsuchung*[2] e del 2 marzo 2010 sul c.d. *Data retention*[3] costituiscono senza dubbio due decisioni epocali.

Con la prima pronuncia la Corte costituzionale tedesca ha dichiarato incostituzionali il § 5 comma 2, n. 11 della legge sulla protezione della Costituzione del North Rhein 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 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 modifica la direttiva 2002/58/CE) ed il § 100g StPO, comma 1, prima parte.

In questo caso si trattava di norme adottate anche per rispondere alle minacce del terrorismo internazionale che prevedevano la 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 tali reati.

La sentenza della *Curtea Constituțională* della Romania dell'8 ottobre 2009[4] ha affrontato alcune questioni simili a quelle oggetto della recente decisione del *Bundesverfassungsgericht*.

L'ordinamento romeno ha attuato la dir. 2006/24/CE in materia conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, che ha modificato la direttiva 2002/58/CE, con la legge n. 298 del 2008 ed ha adottato dei correttivi alla legge n. 506 del 2004 relativa al trattamento ed alla protezione dei dati personali nel settore delle comunicazioni elettroniche.

La legge n. 298 del 2008 prevede l'obbligo per i fornitori di servizi pubblici di comunicazioni elettroniche o i fornitori di reti pubbliche di comunicazione di archiviare i dati generati o trattati durante la loro attività per renderli disponibili alle autorità competenti nell'ambito di attività di indagine e nei procedimenti contro gravi reati. Ai sensi dell'art. 15 della stessa legge, infatti, il *provider* è obbligato a rendere accessibili tali informazioni alle autorità competenti, salvo in casi di "forza maggiore", sulla base di una loro richiesta a seguito della legittima autorizzazione motivata del giudice.

Le citate sentenze sono caratterizzate da una linea argomentativa comune basata sulla questione di legittimazione di metodologie tecniche di investigazione, di archiviazione dei dati e delle informazioni o di controllo ed intervento sull'operato dell'utente rispetto alla tutela dei diritti fondamentali dell'individuo e, più in particolare, della sfera esclusiva di estrinsecazione della sua personalità (*allgemeine Persönlichkeitsrecht*).

[2] *BVerfG* 370/07-595/07, 27 febbraio 2008, in *CR*, 2008, p. 306 ss. Per un primo commento si consenta il rinvio a R. FLOR, *Brevi riflessioni*, cit., p. 695 ss.

[3] 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., p. 359 ss.

[4] Cfr. *Decizia* 1258 dell'8 ottobre 2009, in *Monitorul Oficial*, n. 798, 23 novembre 2009. Per un primo commento vedi J. RINCEANU, *Das Urteil des rumänischen Verfassungsgerichtshofs zur Verfassungswidrigkeit der Vorratsdatenspeicherung*, in *Jahrbuch für Ostrecht*, 52/1, p. 49 ss.

2. La sentenza del *Bundesverfassungsgericht* sulla c.d. *Online Durchsuchung*

Il § 5, comma 2, n. 11 della legge sulla protezione della Costituzione del North Rhein Westfalia aveva autorizzato un organismo di *intelligence* a "protezione della Costituzione" (*Verfassungsschutzbehörde*)[5] ad effettuare due tipi di misure d'indagine: in primo luogo, il monitoraggio e la ricognizione segreti di Internet ("alternativa 1") e, in secondo luogo, l'accesso segreto a sistemi informatici ("alternativa 2")[6].

Questa norma, che costituisce la base giuridica per definire la c.d. *Online Durchsuchung* e, in particolare, l'ultima parte, è stata oggetto di un ampio dibattito[7].

Essa può essere eseguita con opzioni tecniche diverse, che possono comportare la violazione delle misure di sicurezza e, di conseguenza, concreti pericoli per la riservatezza, l'integrità e la sicurezza del sistema e dei dati[8].

In particolare tali rischi possono derivare da fattori: temporali (se si tratta di un monitoraggio a lungo termine); preselettivi (in quanto lo strumento investigativo potrebbe non permettere una selezione tecnica dei dati, in base alla loro natura, da trattare ed archiviare) ed invasivi (che potrebbero comportare la manipolazione delle informazioni o l'accesso non autorizzato da parte di terzi)[9].

Si tratta comunque di mezzi di ricerca della prova che, dovessimo proporre un paragone con il sistema processuale italiano, non trovano una loro contro figura definita, nemmeno dopo la legge n. 48 del 2008, di ratifica della Convenzione *Cybercrime*[10].

---

[5] Si tratta di un organismo [*intelligence Agency*] "a tutela della Costituzione" afferente al Ministero dell'Interno che ha il compito di raccogliere ed analizzare anche le informazioni personali, notizie e documentazione, fra gli altri, su fenomeni criminosi contro la libertà e l'ordine democratico, nonché la sicurezza della Federazione o di un *Land*, volti all'interferenza illecita degli organi costituzionali, della Federazione o di un *Land* o dei suoi membri; ovvero atti riferiti all'uso della forza o atti preparatori di fronte a un pericolo per gli affari esteri della Germania. Vedi §§ 2 e 3 *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*.

[6] Di fatto, i compiti della *Verfassungsschutzbehörde* riguarderebbero, come specificato dai Giudici costituzionali, il monitoraggio segreto o la ricognizione di Internet, come la partecipazione nelle *communication facilities*, e la ricerca, nonché l'accesso segreto alle informazioni contenute in sistemi informatici, che possono coinvolgere anche il dispiegamento di misure tecniche.

[7] La disposizione rappresenterebbe il primo caso di conferimento ad una autorità tedesca di un esplicito potere di impegnarsi in una *Online Durchsuchung*. Si veda quanto ripreso dalla stessa Corte costituzionale (su *Entscheidungen des Bundesgerichtshofes in Strafsachen – BGHSt* – 51, 211). Vedi *BVerfG 370/07*, p. 7. *Online Durchsuchung* può essere tradotta in inglese in *online search* o *online surveillance (supervision)*. In verità, quest'ultima locuzione identifica una "*clandestine long-time monitoring of the computer system*", ossia un monitoraggio prolungato di un sistema informatico (effettuato, per ipotesi, tramite *key-logger software*). *Online search*, invece, è una misura più riferibile alla *one-time copy* dei dati informatici che si trovano in un determinato momento in un sistema informatico. Questa nuova forma di "investigazione *online*" può essere realizzata quindi, sia "da vicino", ossia tramite l'installazione fisica di strumenti atti a monitorare le attività di un sistema informatico o ad avervi accesso, sia "da lontano", attraverso l'uso di *software* e sfruttando le potenzialità della rete e delle innumerevoli *utlities*, che consentono simili operazioni. Vedi, in merito, M. HANSEN-A. PFITZMANN, *Techniken der Online Durchsuchung*, cit., p. 131 ss.; A. WEISS, *Online Durchsuchungen im Strafverfahren*, Hamburg, 2009, in specie p. 15 ss.

[8] I *network sniffers*, in particolare, sono *software* che catturano i pacchetti di informazioni in una rete di *computer* e possono essere utilizzati per monitorare il funzionamento della rete e del sistema e/o scoprire nomi utenti e *passwords*. Su tali aspetti vedi, ancora, M. HANSEN-A. PFITZMANN, *Techniken der Online Durchsuchung*, cit., p. 131 ss.

[9] Si consenta di rinviare a quanto riportato da R. FLOR, *Brevi riflessioni*, cit.

[10] Per un approfondimento sulla distinzione rispetto alla perquisizione, all'ispezione informatica ed alle intercettazioni, comprese quelle informatiche e quelle preventive, vedi R. FLOR, *Brevi riflessioni*, cit. Sugli artt. 19, 20 e 21 CoC vedi L. LUPÁRIA, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 717 ss. Per alcuni spunti di riflessione sul piano del diritto penale sostanzia-

I giudici hanno rilevato che l'uso di sistemi di "sorveglianza" o di "monitoraggio" dell'attività degli *users* possono portare alla profilazione dell'utente. Per tale motivo emerge la necessità di proteggere i diritti fondamentali riconducibili all'art. 1, comma 1 *Grundgesetz* (*postea*: GG) – la dignità umana è inviolabile ed il suo rispetto e la sua protezione costituiscono un dovere da parte delle autorità statali – all'art. 2, comma 1, GG – ogni individuo ha diritto al libero sviluppo della sua personalità, nella misura in cui non viola i diritti degli altri e l'ordine costituzionale o la legge morale – e, quali manifestazioni del diritto generale della personalità (*allgemeine Persönlichkeitsrecht)*, all'art. 10 GG – segretezza della corrispondenza e delle [tele]comunicazioni (*Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich*) – ed all'art. 13 GG – inviolabilità del domicilio (*Die Wohnung ist unverletzlich*).

Vengono in rilievo, in particolare, due diritti fondamentali, espressione del diritto generale alla personalità.

Il primo è il "*diritto di autodeterminazione informativa"* (*Recht auf informationelle Selbstbestimmung*), che va oltre la tutela della *privacy* e non si limita ad informazioni sensibili per loro natura, ma conferisce alla persona, in linea di principio, il potere di determinare, in sé, la divulgazione e l'utilizzo dei suoi dati personali, anche se connotati da un contenuto informativo minimo, che amplia la tutela della libertà della vita privata in termini di diritti fondamentali [11].

Il secondo è il *diritto fondamentale alla garanzia della riservatezza e dell'integrità dei sistemi informatici*, in quanto i sistemi informatici oggetto di indagine possono contenere dati personali della persona in misura e diversità tali da facilitare la conoscenza di parti significative della sua vita o della sua personalità in ambiti sia privati che economico-professionali [12].

Il diritto generale della personalità, in queste sue particolari manifestazioni, offre una tutela contro l'accesso segreto.

La Corte costituzionale ammette, però, che il diritto fondamentale alla garanzia della riservatezza e l'integrità dei sistemi informatici *non è illimitato.*

Limitazioni a tale diritto possono essere giustificate sia per fini di prevenzione che per il perseguimento di reati, purché si basino su un fondamento costituzionale.

Inoltre, i Giudici hanno ritenuto le disposizioni impugnate non conformi ai *principi di chiarezza [precisione]* [13] *e determinatezza*, che trovano le basi negli artt. 20, 28, comma 1, GG [14], nonché al *principio di proporzionalità*, il quale richiede che la compressione dei diritti

le ma anche processuale vedi L. PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet*, 2008, 5, p. 437 ss.

[11] Sul *Recht auf informationelle Selbstbestimmung* vedi anche *BVerfGE 65*, *1 <43>*; *84*, *192 <194>*, richiamata dalla Corte.

[12] Per la traduzione di alcuni essenziali parti della decisione vedi R. FLOR, *Brevi riflessioni*, cit.

[13] Il "principio di chiarezza" può essere tradotto in "principio di precisione", quale espressione della riserva di legge comportante l'obbligo, per il legislatore, di disciplinare con precisione il reato e le sanzioni penali in modo da circoscrivere gli spazi di discrezionalità dell'autorità giudiziaria. Un diritto penale che "ignori il principio di precisione" lascia che i limiti ai diritti di libertà del cittadino "non derivino dal potere legislativo", bensì dalle "scelte politico criminali di questo o quel giudice". Così G. MARINUCCI-E. DOLCINI, *Corso di diritto penale*, I, III ed., Milano, 2001, pp. 119 e 120, a cui si rinvia anche per gli opportuni riferimenti agli orientamenti della Corte costituzionale italiana.

[14] I requisiti di *chiarezza [precisione]* e *determinatezza* assicurano che l'interessato possa comprendere la disciplina giuridica e regolare di conseguenza la sua condotta e le misure da adottare. Il legislatore, quindi, deve determinare casi, finalità e limiti delle restrizioni del diritto fondamentale, in modo che sia chiara e precisa, in termini di formulazione, la "zona" di intervento. Si veda il rinvio della Corte alla decisione: *BVerfG*, 13 giugno 2007 – 1 *BvR 1550/03 u.a.*, in *NJW*, 2007, p. 2464.

fondamentali dovrebbe perseguire uno scopo legittimo ed essere idonea, necessaria ed opportuna quale mezzo per il raggiungimento di questo scopo [15].

La sicurezza dello Stato, come potere di garantire la pace e l'ordine costituzionali, e la sicurezza della popolazione da pericoli per la vita, l'incolumità fisica e la libertà, sono valori di rango costituzionale, che devono essere valutati e considerati nel bilanciamento con altrettanto alti valori e contro-interessi [16].

In particolare, il § 5, comma 2, n. 11 ("alternativa 2") VSG non è conforme al principio di proporzionalità in senso stretto *(Verhältnismäßigkeit im engeren Sinne)* [17], che presuppone che la gravità della restrizione del diritto fondamentale, in una valutazione generale, non possa essere sproporzionata rispetto alla gravità dei motivi che la giustificano. In questo senso le misure previste dalla norma in esame incidono sui diritti fondamentali in modo intenso e sproporzionato rispetto al pubblico interesse alle indagini effettuate tramite l'accesso segreto, che può essere realizzato anche neutralizzando misure di sicurezza (quali la crittografia) adottate dallo stesso titolare per la sicurezza del sistema e dei dati.

La compressione dei diritti fondamentali è ulteriormente determinata dalla *segretezza* dell'accesso, e deve costituire un'eccezione in uno Stato di diritto, dovendo essere necessaria una specifica giustificazione [18].

Dalla motivazione della Corte appare evidente che la compressione dei diritti fondamentali nel contesto di *un obiettivo di prevenzione* soddisfa il requisito di adeguatezza solo se determinati fatti costituiscano un pericolo, nel singolo caso concreto, per un prevalente bene giuridico, benché possa non essere ancora accertato e non si possa quindi stabilire con sufficiente probabilità che il pericolo si concretizzerà in un prossimo futuro.

La possibilità di effettuare un accesso segreto, dunque, è costituzionalmente ammissibile solo se tale misura risulta essere necessaria per la protezione di *importanti e predominanti beni giuridici*, quali possono essere la vita, l'incolumità fisica e la libertà dei singoli, nonché quelli della collettività (*Güter der Allgemeinheit*), la cui minaccia tocca le fondamenta dello

[15] Vedi i riferimenti che la Corte cost. fa a: *BVerfG*, 13 giugno 2007 – *1 BvR 1550/03*, cit.

[16] In questo contesto è espresso il riferimento ad attività terroristiche. La Corte afferma, infatti, che lo Stato, con il suo mandato costituzionale, contrasta i pericoli del terrorismo [o di altre gravi attività criminali]. Una parte della dottrina italiana si è posta la questione, in particolare con riferimento ai reati di terrorismo, se i diritti fondamentali e la giurisdizione penale fossero da intendersi quali garanzie contro l'uso del "diritto come arma" o piuttosto come giustificazione per tale uso. Tale questione deve necessariamente essere ripresa, in particolare se si considera che lo stesso *Bundesverfassungsgericht* si è trovato, da un lato, a dover giudicare norme modificate dal recente "pacchetto sicurezza" tedesco contro il terrorismo, dall'altro lato e relativamente a misure investigative fortemente invasive della sfera riservata dell'individuo, a portare quale esempio di attività preventiva legittima, se rispondente a rigidi presupposti, proprio la lotta contro il terrorismo per la tutela di predominanti beni giuridici. Non è possibile negare, inoltre, che il diritto penale di "matrice europea" sia riconducibile, in taluni settori, al diritto penale "di lotta", non solo con riferimento al terrorismo, ma anche rispetto, ad esempio, alla pedopornografia, alla criminalità economica ed alla criminalità informatica. Si veda M. DONINI, *Lo status di terrorista: tra il nemico ed il criminale. I diritti fondamentali e la giurisdizione penale come garanzia contro, o come giustificazione per l'uso del diritto come arma*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona a prova dell'emergenza*, Napoli, 2009, p. 85 ss., con ampi riferimenti bibliografici.

[17] Sul principio di proporzionalità e sulla sua "gradazione" si rinvia, fra tutti, ad W. HASSEMER, *Erscheinungsformen des modernen Rechts*, Frankfurt am Main, 2007, in particolare p. 191 ss.; ID., *Strafrecht. Sein Selbstverständnis, seine Welt*, Berlin, 2008, in specie p. 198 ss.; p. 219 ss. e, con riferimento a *die Verheerungen der Prävention*, p. 241 ss. In generale e più di recente, anche sui nuovi beni giuridici e su *Schutz der Privatsphäre*, nonché con riferimento al bilanciamento fra *Freiheit* e *Sicherheit*, si rinvia a ID., *Warum Strafe sein muss: ein Plädoyer*, Berlin, 2009. Si consenta di rinviare, inoltre, ai richiami di R. FLOR, *Brevi riflessioni*, cit.

[18] Se i soggetti destinatari della misura sono informati prima della sua esecuzione possono difendere i loro interessi sin dall'inizio (ricorrendo ai mezzi di ricorso previsti, oppure mettendo a disposizione i dati). In questo senso vedi il rinvio della Corte anche a: *BVerfG*, 13 giugno 2007 – 1 *BvR* 1550/03, cit.

Stato o il suo mantenimento o la base dell'esistenza umana, fino a comprendere anche la possibilità di funzionamento delle parti essenziali dei servizi di pubblica utilità.

Un punto fondamentale della motivazione riguarda la riserva della decisione all'autorità giudiziaria. Le attività di indagine in esame, infatti, devono essere contro bilanciate da idonee precauzioni procedurali, riservando la misura ad un *ordine del giudice* che svolga un controllo preventivo, che dovrebbe avere la funzione di "compensazione di rappresentanza" (*kompensatorischen Repräsentation*) degli interessi della persona interessata al procedimento [19].

La Corte costituzionale ha però precisato che un'eccezione al controllo preventivo può essere ammessa nel caso di urgenza, per esempio in caso di pericolo imminente, se è garantito che l'organismo neutrale possa effettuare un esame successivo.

Con riferimento al "monitoraggio segreto della rete" la Corte ha rilevato, infine, che in linea di principio allo Stato non è negata la possibilità di ottenere informazioni accessibili al pubblico come, ad esempio, nel caso in cui raccolga i contenuti di comunicazioni disponibili in Internet ed afferenti ad un gruppo di persone, o in ipotesi in cui venga effettuato un collegamento con una pagina *Web* e l'iscrizione ad una *mailing list* o ad una *chat room* "aperta".

La declaratoria di incostituzionalità non riguarda, pertanto, i nuovi mezzi "di carattere tecnologico" in quanto tali ed in termini assoluti, ma i loro modi di utilizzo, i presupposti ed i limiti, anche temporali, per la loro adozione. In altre parole, il legislatore avrebbe dovuto determinare i casi, le finalità ed i confini della compressione del diritto fondamentale, in modo da rendere chiara e precisa, in termini di formulazione legislativa, la "zona" di intervento riferita a gravi reati a tutela di importanti beni giuridici, nel rispetto del principio di proporzionalità, nonché prevedere la riserva all'autorità giudiziaria sul controllo di tali requisiti.

3. La sentenza del *Bundesverfassungsgericht* sul c.d. *data retention*

La recente decisione della Corte costituzionale tedesca [20] in materia di conservazione dei dati di traffico telematico ha avuto ad oggetto la questione di costituzionalità dei §§ 113a e 113b del *Telekommunikationsgesetzes* (TKG) e sul § 100g StPO, comma 1, prima parte.

In sintesi, la Corte ha ritenuto i §§ 113a e 113b TKG – come modificati dall'art. 2 n. 6 della legge di riforma del settore delle telecomunicazioni e delle altre misure d'indagine sotto copertura (*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen*) e di attuazione della direttiva 2006/24/CE del 21 dicembre 2007 – incostituzionali in quanto in contrasto con l'art. 10, comma 1, GG.

Inoltre, il § 100g, comma 1, prima parte StPO – come modificato dall'art. 1, n. 11 della citata legge di riforma è stato ritenuto, in relazione all'acquisizione dei dati di traffico telematico *ex* art. 113a TKG, in contrasto con gli artt. 1 e 2 GG, nonché 10, comma 1, GG.

Pertanto, i dati archiviati sulla base di queste disposizioni devono essere cancellati e non possono essere trasmessi alle autorità richiedenti [21].

[19] Vedi: *BVerfGE 110*, pp. 33-67; nonché *SächsVerfGH*, 14 maggio 1996 – *Vf.44-II-94* –, in *JZ*, 1996, p. 957 ss.

[20] 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., p. 359 ss., nonché M. FOGLIA, *Valori comuni in materia di privacy e trattamento dei dati personali*, in *Dir. inf.*, 2010, p. 514 ss. Per ulteriori riferimenti vedi R. FLOR, *Data retention*, cit., p. 1954 ss.

[21] Precedentemente, infatti, sono state emesse l'ordinanza sospensiva dell'11 marzo 2008 nel procedimento 1 *BvR* 256/08 (*Bundesgesetzblatt Teil I Seite* 659), ripetuta ed estesa in data 28 ottobre 2008 (*Bundesgesetzblatt*

La complessità della sentenza e le molteplici questioni puntualmente affrontate dalla Corte non permettono in questa sede, per ovvi motivi, un'ampia e completa disanima critica [22]. Ai fini del presente lavoro è sufficiente riportare i soli passaggi relativi alla questione di costituzionalità sul c.d. *data retention*, pur facendo un breve cenno al rapporto fra ordinamento interno e diritto europeo.

Sotto questo ultimo aspetto, infatti, i Giudici costituzionali hanno evidenziato che la verifica di legittimità costituzionale riguarda non le disposizioni della direttiva europea, ma le soluzioni legislative adottate dal legislatore tedesco per raggiungere gli scopi prefissati dall'Unione.

La questione sul principio di prevalenza del diritto comunitario e la sua incidenza sui diritti fondamentali non è stata, dunque, in discussione o, almeno, non direttamente. La direttiva, infatti, conferisce agli Stati un'ampia discrezionalità e le sue previsioni sono limitate essenzialmente all'obbligo di conservazione dei dati, non prevedendo la disciplina sull'accesso e l'utilizzo degli stessi da parte delle autorità statali.

In questo contesto la direttiva può essere attuata dal legislatore tedesco senza comportare una forte compressione o limitazione dei diritti fondamentali.

Con riferimento all'oggetto della decisione, è utile premettere che il § 113a TKG prevede l'obbligo, per il fornitore di servizi pubblici di comunicazioni elettroniche, di conservazione dei dati di traffico telefonico (da rete fissa, mobile, fax, sms e mms), e-mail e servizi Internet, che è esteso a tutte le informazioni necessarie per ricostruire chi ha effettuato la comunicazione o ha tentato di effettuarla (fra cui quelle relative a quando, per quanto tempo, a chi e da dove, nonché identificativo telefonico ed *Ip address*). Il contenuto della comunicazione e di conseguenza i dettagli su quali pagine Internet sono state visitate dagli utenti non devono essere archiviati. Al termine di 6 mesi i dati devono essere cancellati entro un mese.

Lo scopo perseguito dal legislatore era quello di adeguare la norma, nella lotta al terrorismo ed alla criminalità organizzata, alle condizioni poste dalle moderne tecniche di comunicazione.

Il successivo § 113b ha previsto che l'obbligo di archiviazione avesse ad oggetto, ai sensi del § 113a, i dati necessari per perseguire i reati, per evitare gravi minacce alla sicurezza pubblica o per adempiere ai compiti istituzionali delle autorità a protezione della Costituzione della federazione o di un Land, dei servizi segreti federali e di *intelligence*. Oltre a disciplinare i presupposti per la conservazione dei dati, la seconda parte del medesimo comma 1 contiene l'autorizzazione all'utilizzazione indiretta dei dati nella forma di richiesta di informazioni al service provider per identificare l'Ip address. In altri termini, se l'autorità è a conoscenza di tale informazione può richiedere ulteriori dati relativi all'utente "titolare" dell'indirizzo Ip. Questo ultimo, dunque, non rientrerebbe nell'area di tutela del nucleo essenziale del diritto fondamentale alla riservatezza da preservare tramite la previsione di stringenti limiti al potere coercitivo dello Stato.

Il § 100g StPO, invece, contiene le norme applicabili in relazione all'obbligo da parte dei providers di rendere accessibili i dati necessari alle investigazioni in materia penale disponendo che, per la repressione di gravi reati (previsti dal precedente § 100a, comma 2, che definisce i "gravi reati" – "Schwere Straftaten im Sinne des Absatzes 1 n. 1 sind" […]) o per quelli commessi con mezzi di telecomunicazione, è consentita l'acquisizione dei dati di traffico, nel-

Teil I Seite 2239) e ripetuta in data 15 ottobre 2009 (*Bundesgesetzblatt Teil I Seite* 3704), relative alle richieste di accesso ai dati da parte delle autorità competenti ai *service providers.*

[22] Per un approfondimento, anche in relazione al concetto di "*Ip address*" ed alle sue "forme", si rinvia alle motivazioni della decisione, in *http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.*

la misura necessaria per l'indagine [23]. In realtà, la norma disciplina qualsiasi accesso ai dati di traffico telematico permettendo anche quello alle informazioni archiviate dai service providers per altre ragioni (per ipotesi relative, fra le altre, all'effettuazione di transazioni economiche).

Inoltre, il legislatore non ha distinto fra l'uso di dati archiviati ai fini del § 113a TKG ed altri dati di traffico, ma ha ritenuto opportuno permettere l'utilizzazione indipendentemente da una lista di reati significativi o per perseguire quelli commessi tramite sistemi di telecomunicazione.

Le citate norme, secondo i giudici costituzionali, incidono sull'area di tutela dell'art. 10, comma 1, GG, ossia sul diritto fondamentale alla riservatezza ed alla confidenzialità dei sistemi informativi, quali espressioni del generale diritto alla personalità (che include anche il c.d. diritto all'autodeterminazione informativa).

I fornitori di servizi pubblici di comunicazioni elettroniche pur essendo, nella maggior parte dei casi, soggetti privati, svolgono attività di rilevanza pubblica di collaborazione con le autorità statali e, attraverso gli atti legittimi di queste ultime, rappresentano una manifestazione del potere coercitivo dello Stato *in subiecta materia*.

Le disposizioni sulla memorizzazione delle informazioni per un periodo di 6 mesi non sono incompatibili con l'art. 10 GG in termini assoluti e non è preclusa *ab origine* l'archiviazione di tali dati da parte di *service providers*, se tali previsioni sono integrate in una struttura legislativa "appropriata", ossia capace di soddisfare il principio di proporzionalità. I rilievi di incostituzionalità hanno dunque riguardato anzitutto l'obbligo di memorizzazione, che prescinde da specifici presupposti (*anlasslos gespeicherten Daten*), riguarda tutti gli utenti ed è previsto per qualsiasi dato in modo indiscriminato.

Simili operazioni, anche se non coinvolgono il contenuto delle comunicazioni, afferiscono alla sfera intima dei soggetti, potendo attrarre, seppur potenzialmente, informazioni di natura sensibile (ad esempio di carattere politico o sulle inclinazioni e preferenze personali), e comportare il "tracciamento" e la "profilazione" degli utenti.

In altri termini, tale attività comporta il rischio, da un lato, di sottoporre uno o più soggetti ad indagini o ad ulteriori indagini senza che essi vi abbiano dato in alcun modo occasione, dall'altro lato di abusi da parte delle medesime autorità.

Di conseguenza, considerate le potenzialità dei sistemi di archiviazione e la natura dei dati ivi memorizzati, è indispensabile, a parere dei Giudici, non solo la previsione dei presupposti, ma anche l'adozione di misure di sicurezza proporzionate che assicurino uno standard elevato, la cui valutazione ed implementazione non può essere lasciata all'apprezzamento soggettivo del *provider* o a mere valutazioni economiche e prevedendo, eventualmente, un organismo ad hoc per la regolamentazione degli standard tecnici.

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 [24].

---

[23] A titolo di esempio, sono considerati "gravi reati" quelli contro la pace, la difesa nazionale, la libertà personale, di banda armata, contro l'identità sessuale.

[24] *De jure condito* è assente, secondo i giudici, una garanzia di uno standard elevato di sicurezza. La norma fa solo riferimento, infatti, al generale bisogno di sicurezza (§ 113a.10 TKG) non definendo quali debbano essere tali misure introducendo solo considerazioni generali sull'adeguatezza economica nei singoli casi (§ 109.2, 4 TKG). In altri termini viene lasciato al singolo ISP ogni apprezzamento, che deve offrire servizi in condizioni competitive ed è soggetto alle regole di mercato nonché alla pressione dei costi.

In questo contesto l'ISP non è né 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), né un livello comparabile di

La Corte, riprendendo la sentenza sulla c.d. *Online Durchsuchung*, ha affermato, inoltre, la necessaria presenza di un pericolo concreto per la vita o la libertà delle persone, oppure per la sicurezza della Federazione o di un Land, quali presupposti affinché la compromissione dei diritti fondamentali possa essere ritenuta legittima.

Con l'obbligo di conservazione dei dati il legislatore deve prevedere, dunque, nel rispetto del principio di tassatività, una lista esaustiva dei reati in relazione a determinati ed importanti beni da proteggere.

L'utilizzo e la trasmissione dei dati archiviati deve comunque essere soggetta al controllo dell'autorità giudiziaria anche se, nell'ambito della discrezionalità legislativa, l'atto normativo potrebbe richiedere che alcune informazioni possano essere fornite anche indipendentemente dai limiti previsti o imposti per specifici reati o da una lista di illeciti o beni giuridici, sulla base di autorizzazioni generali previste da specifiche disposizioni di legge.

Per quanto riguarda la soglia di interferenza, però, secondo i giudici si dovrebbe garantire che le informazioni non possano essere raccolte a "random", ma solo sulla base di un obiettivo sospetto o di un pericolo concreto sulla base dei fatti relativi al caso concreto.

Nelle indagini penali, inoltre, è possibile la previsione dell'uso dei dati in modo segreto solo se tale utilizzo risultasse indispensabile, previa comunque l'autorizzazione da parte dell'autorità giudiziaria. In simili situazioni il legislatore dovrebbe prevedere un obbligo di informazione susseguente.

De jure condito, il § 100g, comma 1, n. 1, StPO non assicura che l'archiviazione dei dati avvenga solo per perseguire gravi reati ed il n. 2 della stessa disposizione include ogni reato commesso mediante mezzi di comunicazione, indipendentemente dalla sua gravità, quale presupposto per il recupero dei dati, sulla base di una valutazione generale nel corso di un controllo di proporzionalità.

In sintesi, queste disposizioni rendono i dati memorizzati *ex* § 113 *bis* TKG utilizzabili praticamente per tutti i reati.

In tale contesto, considerando l'incremento di importanza dei mezzi di comunicazione nell'attuale società dell'informazione, l'utilizzo di tali dati perderebbe il carattere eccezionale che lo dovrebbe connotare [25].

Inoltre, la norma permette il recupero di dati non per casi individuali supportati da una decisione giudiziaria, ma quale regola generale anche senza la conoscenza da parte del soggetto interessato (§ 100g.1, StPO).

Sull'uso indiretto degli Ip address, invece, i giudici hanno specificato che per tali informazioni non è necessario prevedere standard stringenti e nemmeno il rigido requisito della richiesta all'autorità giudiziaria. In ogni caso, però, le persone interessate devono essere informate quando questi dati sono trattati/raccolti.

Nella *dissenting opinion* il giudice Schluckebier ha ritenuto che l'obbligo di conservazione dei dati per un periodo di 6 mesi non contrasti con il diritto fondamentale protetto dall'art. 10, comma 1, GG. I dati di traffico rimangono, infatti, nella sfera riservata dell'ISP sui suoi servers, per ragioni tecniche, e gli utenti possono fare affidamento, sulla base del rapporto contrattuale, che i dati siano trattati in stretta confidenza e protetti. Se è garantita l'adozione di misure di sicurezza corrispondenti allo stato dell'arte non ci sono obiettivamente le basi per sostenere che l'utente potrebbe subire delle limitazioni rilevanti al diritto fondamentale. Considerando peraltro che l'archiviazione non si estende al contenuto delle comunicazioni.

sicurezza è altrimenti garantita. Nemmeno vi è un sistema equilibrato di sanzioni che attribuisca rilevanza alle violazioni della sicurezza dei dati rispetto alle violazioni dei doveri di immagazzinamento.

[25] Questo passaggio della motivazione si rinviene anche nella sentenza della Corte cost. della Romania (vedi *infra*, par. 4).

In sostanza, le disposizioni impugnate non sarebbero inappropriate essendo ragionevoli e proporzionate, soprattutto considerando la materia delle intercettazioni, in cui vi è l'effettivo rischio di invasione nella sfera privata, che non sarebbe lesa in sé dalla mera archiviazione, ma eventualmente dal recupero dei dati e dal loro utilizzo nei singoli casi.

Dalla *dissenting opinion* si desume che spetta comunque al legislatore garantire un bilanciamento fra contrapposti interessi, considerando anche l'effettiva e costituzionale amministrazione della giustizia in vista dei cambiamenti portati dalle nuove tecnologie e dalle nuove forme di comunicazione.

4. La sentenza della *Curtea Constituțională* della Romania sul c.d. *data retention*

La decisione della Corte costituzionale della Romania, che precede quella del *Bundesverfassungsgericht* del 2 marzo 2010[26] ed è successiva a quella della Corte Suprema bulgara[27], ha riguardato la questione di incostituzionalità relativa alle disposizioni della legge n. 298 del 2008 e della legge n. 506 del 2004, che prevedono l'obbligo per i fornitori di servizi pubblici di comunicazioni elettroniche o i fornitori di reti pubbliche di comunicazione di archiviare i dati generati o trattati durante la loro attività per renderli disponibili alle autorità competenti nell'ambito di attività di indagine e nei procedimenti contro gravi reati. La Corte, in particolare, ha ritenuto convincenti le obiezioni relative alla compromissione dei diritti di libertà di movimento, di intimità e del rispetto della vita privata, nonché gli effetti sul diritto alla segretezza della corrispondenza ed alla libertà di espressione protetti dalla Costituzione romena.

I Giudici hanno richiamato il riconoscimento internazionale del diritto alla *privacy* ed alla vita famigliare, protetto dall'art. 26 della Costituzione romena, come risulta dall'art. 12 della Dichiarazione universale sui diritti dell'uomo, dall'art. 17 del Patto internazionale relativo ai diritti civili e politici, dall'art. 8 della Convenzione per la tutela dei diritti umani e delle libertà fondamentali.

Tali diritti, incluso quello alla libertà di espressione previsto dall'art. 30 della Costituzione e dall'art. 10 della citata Convenzione, non sono però assoluti.

In questo contesto, né la Convenzione per la tutela dei diritti umani e delle libertà fondamentali né la Costituzione nazionale vietano soluzioni legislative limitative dei diritti fondamentali. Tali limiti, però, sono legittimi se rispettano specifici requisiti, espressamente richiesti dall'art. 8 della Convenzione e dall'art. 53 Cost., e 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. Esso, 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[28].

[26] Per una sintesi della decisione in lingua inglese e per un breve commento vedi B. MANOLEA, *Romania: Implementation of EU Data Retention Directive Uncostitutional*, in *Cri*, 2010, 2, p. 49 ss. Più dettagliatamente cfr. J. RINCEANU, *Das Urteil des rumänischen Verfassungsgerichtshofs*, cit. Si consenta di rinviare a R. FLOR, *Data retention*, cit., che richiama altresì la sentenza della Corte costituzionale della Repubblica ceca, del 31 marzo 2011, che ha dichiarato incostituzionali le norme interne sul *data retention*. Su quest'ultima decisione vedi ampiamente R. FLOR, *Perspectives of new types of "technological investigations" and protection of fundamental rights in the Era of Internet. The cyberterrorism as a prime example, between problems of definition and the fight against terrorism ad cyber-crime*, in II International Conference of young penalist/II Congreso International de Jóvenes Investigadores en ciencias Penales, Salamanca, 2011 (in corso di pubblicazione).

[27] Si veda la sentenza della Corte Suprema Amministrativa della Bulgaria (SAC) dell'11 dicembre 2008.

[28] La Corte costituzionale richiama la propria giurisprudenza in materia di intercettazioni di comunicazioni telefoniche e elettroniche, che ha confermato la costituzionalità dell'art. 911 c.p.p. (vedi in particolare *Decizia*

La Corte ha evidenziato, inoltre, che l'attuazione delle direttive europee comporta degli obblighi per quanto concerne gli scopi, ma non le modalità per raggiungerli, lasciando dunque agli Stati membri un certo margine di discrezionalità.

La legge n. 298 del 2008, regolando l'obbligo imposto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare i dati per un periodo di 6 mesi esprime l'intenzione del legislatore di limitare l'esercizio di questi diritti fondamentali.

La norma, però, deve ritenersi incostituzionale.

In primis la Corte ha rilevato il mancato rispetto del principio di precisione nel determinare la sfera dei dati necessari per identificare gli utenti, che apre la possibilità ad abusi nell'attività di conservazione, trattamento ed utilizzo delle informazioni archiviate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

Le limitazioni ai diritti fondamentali della riservatezza, della segretezza della corrispondenza e della libertà di espressione devono, infatti, essere previste in modo chiaro e non ambiguo, per evitare valutazioni arbitrarie da parte delle autorità. I soggetti su cui incide la normativa sono membri della società civile e devono essere messi nella condizione di comprendere le leggi applicabili, in modo da adattare le loro condotte e rappresentarsi le conseguenze di queste ultime.

In secondo luogo, secondo i Giudici il legislatore non ha individuato il significato della locuzione "per la prevenzione ed il contrasto di minacce alla sicurezza nazionale le istituzioni statali […] possono avere accesso, secondo le condizioni stabilite dagli atti normativi che regolano l'attività di sicurezza nazionale, ai dati conservati presso i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione" [29].

In terzo luogo, la Corte ha rilevato che la legge n. 298 del 2008 stabilisce, in generale, la regola della conservazione dei dati per un periodo di 6 mesi e l'obbligo del *provider* è di carattere intrinsicamente continuo.

La direttiva 2002/58/CE, la legge n. 677 del 2001 sulla protezione dei dati personali e, successivamente, la legge n. 506 del 2004 consentono dei limiti eccezionali al diritto alla riservatezza sulla base delle condizioni espressamente previste dalla Costituzioni e dalla normativa internazionale applicabile *in subiecta materia*.

Ma, mentre nel caso, ad esempio, delle intercettazioni e delle registrazioni audio-video l'art. 91 c.p.p. rispetta il carattere eccezionale della limitazione, ammettendola sulla base di stringenti circostanze dal momento dell'autorizzazione motivata dell'autorità giudiziaria e per un periodo limitato di tempo non superiore a 120 giorni in totale, per la stessa persona e per lo stesso fatto, la legge n. 298 ha "trasformato" l'eccezione in "regola" obbligando l'archiviazione dei dati per un periodo di 6 mesi, i quali possono essere utilizzati con l'autorizzazione motivata del giudice "per il passato e non per il futuro" [30]. Perciò la previsione di un obbligo

962 del 25 giugno 2009, in *Monitorul Oficial* n. 563 del 13 agosto 2009), nonché le decisioni della Corte europea dei diritti dell'uomo sui casi *Klass e altri vs. Germania*, del 1978 e *Dumitru Popescu vs. Romania*, del 2009, caratterizzate dall'affermazione dei limiti dell'intervento dello Stato nell'esercizio dei diritti, da parte dei cittadini, della libertà di espressione ed alla vita privata e familiare.

[29] La norma non definendo, in particolare, le "minacce alla sicurezza nazionale" difetta di precisione e contribuisce ad accrescere il rischio che azioni di *routine* possano essere attuate sulla base di criteri arbitrari ed in modo abusivo. Alla stessa conclusione si può giungere considerando la locuzione "*possono avere*", che induce a ritenere che i dati non siano conservati per l'utilizzo esclusivo da parte delle istituzioni dello Stato con attribuzioni specifiche per la tutela della sicurezza nazionale e ordine pubblico ma, viceversa, che possano essere accessibili anche per altre autorità.

[30] Si consideri che 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 repres-

positivo relativo alla limitazione continuativa dei diritti fondamentali alla riservatezza ed alla segretezza della corrispondenza comporta un'intrusione non proporzionata nella sfera esclusiva di pertinenza della persona [31].

La legge n. 298 del 2008, invece, non considera la necessità della cessazione della limitazione e, a parere dei Giudici costituzionali, l'intrusione nel libero esercizio dei diritti fondamentali coinvolti avviene in modo "continuativo ed indipendente dal verificarsi di un fatto che la giustifichi, di una causa determinante e solo per la prevenzione e la scoperta, dopo la perpretazione, di gravi reati".

Inoltre, le disposizioni oggetto del giudizio di costituzionalità sono generalmente applicabili e coinvolgono anche coloro che utilizzano i servizi di comunicazione elettronica o reti pubbliche di comunicazione che abbiano o meno commesso dei reati o che siano o meno soggetti ad indagine, "rovesciando in tal modo la presunzione di innocenza".

Infine, anche se la norma non si applica al contenuto delle comunicazioni o delle informazioni, secondo i Giudici la quantità e la qualità dei dati sono determinanti, potendo essi determinare tipo, ora e durata della comunicazione, il tipo di dispositivo utilizzato e la sua localizzazione, la provenienza e la destinazione, nonché i soggetti coinvolti nella comunicazione e i c.d. "dati connessi" (ossia qualsiasi dato) utili all'identificazione dell'utente.

In questo contesto, gli strumenti legali di tutela rispetto al concreto utilizzo dei dati conservati dai *providers*, per i quali l'inosservanza dell'obbligo comporta l'applicazione di una sanzione pecuniaria (ammenda) *ex* art. 18 della medesima legge, non sono stati ritenuti dalla Corte sufficienti ed appropriati affinché la compromissione dei diritti fondamentali coinvolti possa ritenersi legittima.

I Giudici hanno precisato che non si rigetta il proposito perseguito dal legislatore con l'adozione della legge n. 298 del 2008, ma vi è un urgente bisogno di assicurare un'adeguata ed efficiente tutela compatibile con il continuo processo di modernizzazione e di aggiornamento tecnologico dei mezzi di comunicazione, che consideri quale oggetto di protezione i diritti della persona, i quali possono essere legittimamente limitati, o costituire "oggetto di restrizioni", in relazione alla protezione di diritti collettivi ed interessi pubblici inerenti alla sicurezza nazionale, all'ordine pubblico o alla prevenzione dei reati, nell'ottica di un bilanciamento fra questi ultimi interessi ed i diritti individuali fondamentali da una parte, ed i diritti e gli interessi dell'ordine sociale dall'altra parte [32].

In conclusione, le norme previste dagli artt. 1 e 15 legge n. 298 del 2008, così come le modifiche alla legge n. 506 del 2004, sono state dichiarate incostituzionali.

Tale decisione non ha eliminato l'obbligo per la Romania di recepire le direttive europee. Nel frattempo, però, l'applicazione delle leggi coinvolte è stata sospesa.

---

sione 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. Il comma 3 della disposizione prevede che entro il termine di cui al comma 1, 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., ferme restando le condizioni di cui art. 8, comma 2, lett. f), per il traffico entrante.

[31] Anche in questo caso i Giudici hanno richiamato l'art. 91 c.p.p., considerato compatibile con il principio di proporzione sia con riferimento alla durata della limitazione, che per quanto attiene l'immediata cessazione della misura non appena siano scomparse le circostanze che l'hanno determinata.

[32] La Corte richiama la decisione della Corte europea dei diritti dell'uomo nel caso *Klass e altri vs. Germania*, 1978, in cui i giudici hanno affermato che le misure di sorveglianza adottate senza sufficienti garanzie possono "distruggere la democrazia".

5. Gli elementi argomentativi comuni dei Giudici delle Leggi

Le importanti decisioni del *Bundesverfassungsgericht* (2008 e 2010) e della *Curtea Constituțională* (2009) si inseriscono nel contesto attuale della società dell'informazione, in cui le nuove tecnologie costituiscono sia un mezzo per la preparazione e la commissione di reati, che un'efficace strumento investigativo, di contrasto e/o preventivo.

In tutte le decisioni riportate 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 [33].

Dalle motivazioni delle sentenze è possibile ricavare alcuni elementi argomentativi comuni.

In primo luogo è innegabile il riconoscimento, esplicito o implicito, del ruolo essenziale dei *service providers*, che possono svolgere attività anche di rilevanza pubblica [34]. 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 finalità 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 [35].

In terzo luogo, le Corti hanno affrontato la questione della legittimazione dei mezzi di in-

[33] 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., che rinvia a M. KRANZBERG, *The Information Age: Evolution or Revolution?*, in B.R. GUILE (ed.), *Information Technologies and Social Transformation*, Washington, D.C., 1985, p. 50. Per alcuni riferimenti derivanti dall'analisi della sentenza della Corte costituzionale tedesca sulla c.d. *Online Durchsuchung* basti il rinvio a: G. HORNUNG, *Ein neues Grundrecht. Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme*, in *CR*, 2008, pp. 299, 302; M. KUTSCHA, *Mehr Schutz von Computerdaten durch ein neues Grundrecht?*, in *NJW*, 2008, p. 1042; M. GERCKE, *Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden*, in *MMR*, 2008, pp. 291-298; T. HOEREN, *Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme?*, in *MMR* 2008, 365-366; S. BEUKELMANN, *Die Online-Durchsuchung*, StraFo, 2008, p. 1 ss.; A. WEISS, *Online Durchsuchungen im Strafverfahren*, cit., p. 89 ss.

[34] 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). Su ruolo e rilevanza degli ISP nella società dell'informazione e sul bilanciamento fra le esigenze di tutela del *copyright* con quelle di protezione dei dati personali si consenta il rinvio a R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010, in specie p. 418 ss.

[35] 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. Èutile ricordare, inoltre, che la sentenza della Corte costituzionale tedesca sul c.d. *data retention* ha avuto ad oggetto proprio alcune delle norme introdotte dal "pacchetto anti-terrorismo" e volte ad adeguare le misure di contrasto al mutato contesto comunicativo globaleSi 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, pp. 353-364; U. SIEBER, P. BRUNST, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions*, Council of Europe Publishing, 2007, pp. 9-105. Sulla necessità di rivedere la disciplina europea del *data retention*, assicurando la tutela dei diritti fondamentali anche nella lotta alla criminalità grave ed al terrorismo, vedi il report della Commissione UE al Consiglio ed al Parlamento europeo del 18 aprile 2011 (COM-2011/225 final), nonché R. FLOR, *Perspectives*, cit.

dagine, di archiviazione e di controllo dei dati di traffico telematico rispetto alla tutela dei diritti fondamentali della persona, giungendo alla conclusione che non sussiste un divieto assoluto di adottare soluzioni legislative limitative di tali diritti [36].

La qualificazione degli interventi pubblici nella sfera dei diritti individuali, inoltre, 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 [37].

[36] 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, né 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 comma 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". Non vi è dubbio che la locuzione "ingerenza prevista dalla legge" sia da intendersi alla stregua di "riserva di legge", pur nella concezione "flessibile" della Corte europea dei diritti dell'uomo. Con riferimento alle sentenze della Corte costituzionale italiana n. 348, n. 349 del 2007 e n. 39 del 2008, e sul rango della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali nell'ordinamento italiano, vedi R. CONTI, *La corte costituzionale viaggia verso i diritti CEDU: prima fermata verso Strasburgo*, in *Corriere giur.*, 2008, p. 205 ss.; L. CAPPUCCIO, *La corte costituzionale interviene sui rapporti tra convenzione europea dei diritti dell'uomo e costituzione*, in *Foro it.*, 2008, I, c. 47 ss. Sulla "riserva di legge" vedi Corte europea, sez. II, 20 gennaio 2009, ric. n. 75909/01.

[37] Tale principio è ricavabile anche da un'altra sentenza di una Corte costituzionale europea e, precisamente, del *Conseil Constitutionnel* (vedi *Conseil Constitutionnel*, 10 giugno 2009, n. 2009-580). Per la traduzione in italiano si rinvia a *Dir. inf.*, 2009, p. 524 ss., con nota di G. VOTANO, *Internet fra diritto d'autore e libertà di comunicazione: il modello francese*, che richiama il parere della *Commission Nationale de l'Informatique et des Libertés*.Il *Conseil Constitutionnel*. Il legislatore francese, con la legge "*favorisant la diffusion et la protection de la création sur internet*" o c.d. legge "Olivennes" (o *loi Hadopi* o *loi Création et Internet*) presentata nel maggio 2009 dopo un iter legislativo travagliato e censurata, il 10 giugno 2009, dal *Conseil Constitutionnel*, aveva adottato specifiche disposizioni per contrastare la diffusione abusiva in Internet di opere dell'ingegno protette dal diritto d'autore. A seguito della declaratoria di incostituzionalità, il 12 giugno 2009 è stata adottata la *loi* n. 2009-669 (c.d. "*Hadopi 2*"). La legge, infatti, è passata in *Sénat 1ère lecture – Assemblée nationale 1ère lecture – Sénat 2e lecture – Commission Mixte Paritaire – Lecture texte CMP – Assemblée nationale Nouvelle lecture – Sénat Nouvelle lecture – Conseil Constitutionnel* (quest'ultimo, *Décision n. 2009-580 DC* del 10 giugno 2009, *ex* art. 61.2 Costituzione). Questa norma ha istituito un'autorità indipendente (*Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* – Alta autorità per la diffusione delle opere e la tutela dei diritti in Internet), ossia un'organismo-commissione amministrativa per la vigilanza ed il controllo della diffusione in rete di materiale protetto dal diritto d'autore, ed ha previsto meccanismi di segnalazione ai titolari dell'accesso ad Internet, predisponendo una graduale applicazione delle sanzioni in "tre fasi", tramite misure preventive e repressive, che comprendevano la sospensione temporanea della connettività e l'introduzione di *softwares* per l'"accesso sicuro". I Giudici dichiarando che le libertà di comunicazione e di accesso ad Internet non possono essere limitate tramite strumenti sanzionatori amministrativi, non intendevano sostenere che il bilanciamento con il diritto d'autore doveva essere riservato al legislatore penale. Più ragionevolmente pare abbiano voluto evidenziare la delicatezza del contemperamento fra contrapposti interessi di rilevanza costituzionale, che deve essere non solo oggetto di un'ampia riflessione parlamentare, ma deve anche tradursi nella regolazione di strumenti di

Interventi legislativi che possono comprimere i diritti fondamentali dovrebbero considerarsi legittimi, però, solo se diretti alla tutela di importanti e predominanti beni giuridici nel rispetto del principio di proporzionalità.

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 determini 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).

6. Conclusioni: il contenuto essenziale del diritto fondamentale come rapporto fra libertà e limite nella Carta dei diritti dell'Unione Europea

La previsione di metodologie di investigazione adattabili al mutato contesto tecnologico ed alla diffusione di Internet si è tradotta nella disciplina di attività preventive che coinvolgono misure preprocessuali di contrasto, di ricerca della prova e di accertamento dei reati. Non poteva non assumere un ruolo centrale la questione relativa al rispetto dei diritti fondamentali.

La stessa Corte costituzionale italiana [38], con riferimento alla questione di legittimità costituzionale degli artt. 189 e 266-271 c.p.p. e, in particolare, dell'art. 266, comma 2, c.p.p., nella parte in cui non estendono la disciplina delle intercettazioni delle comunicazioni tra presenti nei luoghi indicati dall'art. 614 c.p. alle riprese visive o videoregistrazioni effettuate nei medesimi luoghi, aveva evidenziato che nel sistema delle libertà fondamentali, la libertà domiciliare si presenta "strettamente collegata alla libertà personale, come emerge dalla stessa contiguità dei precetti costituzionali che sanciscono l'una e l'altra (artt. 13 e 14 Cost.) [39].

In sintesi, i Giudici hanno sostenuto che la captazione di immagini in luoghi di privata dimora può configurarsi, in concreto, come una forma di intercettazione di comunicazioni fra presenti, "che si differenzia da quella operata tramite gli apparati di captazione sonora solo in rapporto allo strumento tecnico di intervento, come nell'ipotesi di riprese visive di messaggi gestuali: fattispecie nella quale già ora è applicabile, in via interpretativa, la disciplina legislativa della intercettazione ambientale in luoghi di privata dimora". Il problema di costituzionalità si configura, però, solo ove si "fuoriesca dall'ipotesi della videoregistrazione di comportamenti di tipo comunicativo, venendo allora in considerazione soltanto l'intrusione nel domicilio in quanto tale". In questo caso sussisterebbe una sostanziale eterogeneità delle situazioni

tutela che possano garantire i diritti fondamentali, compresi quelli della difesa, ed una necessaria circolazione del sapere, essenziale per lo sviluppo culturale ed economico della società. Vedi in merito R. FLOR, *Tutela penale*, cit., p. 350 ss.

[38] Vedi Corte cost., sent. n. 135 del 2002, in *Giur. cost*., 2002, p. 1067 ss., con nota di F. SAVERIO MARINI, *La costituzionalità delle riprese visive nel domicilio: ispezione o libertà «sotto-ordinata»?*, *ivi*, p. 1076 ss.; A. PACE, *Le videoregistrazioni «ambientali» tra gli artt. 14 e 15 Cost.*, *ivi*, p. 1070 ss.

[39] Inoltre, le garanzie previste nel secondo comma dell'art. 14 Cost., in rapporto alle limitazioni dell'inviolabilità del domicilio, riproducono espressamente quelle stabilite per la tutela della libertà personale. Nel panorama delle libertà fondamentali il domicilio viene dunque in rilievo quale proiezione spaziale della persona, "nella prospettiva di preservare da interferenze esterne comportamenti tenuti in un determinato ambiente: prospettiva che vale, per altro verso, ad accomunare la libertà in parola a quella di comunicazione (art. 15 Cost.), quali espressioni salienti di un più ampio diritto alla riservatezza della persona". Appare dunque rilevante come la Corte italiana, che ha opposto all'ordinamento europeo il controlimite del rispetto dei livelli costituzionali di protezione dei diritti fondamentali, nella decisione richiamata abbia utilizzato il riferimento alla Carta per limitare l'espansione di una libertà costituzionale.

poste a confronto: "la limitazione della libertà e segretezza delle comunicazioni, da un lato; l'invasione della sfera della libertà domiciliare in quanto tale, dall'altro".

Pertanto, anche se la libertà di domicilio e la libertà di comunicazione rientrano entrambe in una comune e più ampia prospettiva di tutela della "vita privata", restano differenziate sul piano dei contenuti [40].

I Giudici avevano precisato: "giova soggiungere che l'ipotizzata restrizione della tipologia delle interferenze della pubblica autorità nella libertà domiciliare non troverebbe riscontro né nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (art. 8), né nel Patto internazionale sui diritti civili e politici (art. 17); né, infine, nella Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza nel dicembre 2000 (artt. 7 e 52), qui richiamata – ancorché priva di efficacia giuridica – per il suo carattere espressivo di principi comuni agli ordinamenti europei" [41].

È pur vero che la Corte costituzionale ha utilizzato la Carta come strumento interpretativo in quanto espressiva dei principi comuni negli ordinamenti europei [42].

Salvi i noti rilievi sul suo "valore giuridico" è opportuno evidenziare che il Trattato di Lisbona, entrato in vigore il 1° dicembre 2009, all'art. 6 del Trattato sull'Unione dispone che la Carta "ha lo stesso valore giuridico dei trattati" [43].

L'art. 52 della stessa Carta, adattata il 12 dicembre 2007 a Strasburgo, prevede che eventuali limitazioni all'esercizio dei diritti e delle libertà in essa riconosciuti devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. "Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

Il comma 3 del medesimo articolo dispone che laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti del-

[40] La Corte ha dunque precisato che la "libertà di domicilio ha una valenza essenzialmente negativa, concretandosi nel diritto di preservare da interferenze esterne, pubbliche o private, determinati luoghi in cui si svolge la vita intima di ciascun individuo. La libertà di comunicazione, per converso – pur presentando anch'essa un fondamentale profilo negativo, di esclusione dei soggetti non legittimati alla percezione del messaggio informativo – ha un contenuto qualificante positivo, quale momento di contatto fra due o più persone finalizzato alla trasmissione di dati significanti". I Giudici non hanno esitato a concludere che l'ipotesi della videoregistrazione che non abbia carattere di intercettazione di comunicazioni potrebbe essere disciplinata soltanto dal legislatore, nel rispetto delle garanzie costituzionali dell'art. 14 Cost., "ferma restando, per l'importanza e la delicatezza degli interessi coinvolti, l'opportunità di un riesame complessivo della materia da parte del legislatore stesso".

[41] Così Corte cost., sent. n. 135 del 2002, cit., p. 1067 ss., con nota di F. SAVERIO MARINI, *La costituzionalità*, cit., p. 1076 ss.; A. PACE, *Le videoregistrazioni*, cit., p. 1070 ss.

[42] Vedi in merito Corte Giust., sent. n. 445 del 2002, in *Giur. cost*., 2002, p. 3634 ss., con nota di G. BRUNELLI, *L'illegittimità derivata di norme analoghe come tecnica di tutela dei diritti fondamentali*.

[43] Per alcuni spunti critici si veda G. GRASSO, *La protezione dei diritti fondamentali nella Costituzione per l'Europa e il diritto penale: spunti di riflessione critica*, in G. GRASSO-R. SICURELLA (cur.), *Lezioni di diritto penale europeo*, Milano, 2007, p. 633 ss. Più di recente vedi H. SATZGER, *Internationales und Europäisches Strafrecht*, 3. Auf., Baden Baden, 2009, in specie p. 186 ss. (*Die Europäische Menschenrechtskonvention*). Si consideri inoltre che, dal 1° dicembre 2009, per espressa previsione dei commi 2 e 3 dell'art. 6 TUE, l'Unione aderisce alla CEDU e i diritti fondamentali da essa garantiti e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali. Il Consiglio di Stato italiano, nella sentenza n. 1220/2010, depositata il 2 marzo 2010, ha affermato che gli artt. 6 e 13 della Convenzione europea dei diritti dell'uomo sono divenuti direttamente applicabili nel sistema nazionale, a seguito della modifica dell'art. 6 TUE, disposta dal Trattato di Lisbona. In verità i giudici non affrontano compiutamente la questione, limitandosi ad una sintetica affermazione.

l'Uomo e delle Libertà fondamentali, "il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione", non precludendo che il diritto dell'Unione conceda una protezione più estesa.

In altri termini, sono ammesse le restrizioni al diritto fondamentale, ma queste non possono far venir meno le condizioni effettive del suo esercizio o, utilizzando le parole della Corte costituzionale italiana, l'esercizio di ogni diritto, anche quello costituzionalmente garantito, può essere dalla legge regolato e così sottoposto a limite, sempre che questo sia compatibile con la funzione [di tale] diritto […] e non si traduca comunque nella esclusione dell'effettiva possibilità dell'esercizio in parola"[44].

La Carta, dunque, non determina previamente il contenuto essenziale, ma richiede il contemperamento fra l'esercizio di un diritto ed i suoi limiti rapportato al caso concreto[45].

È altrettanto vero, però, che anche se l'elaborazione dei diritti fondamentali europei attinge a tradizioni costituzionali comuni, sussistono dislivelli contenutistici che portano gli Stati ad una visione autonomistica dell'area di inviolabilità, in taluni casi avente effetti che potrebbero incidere sul principio di supremazia dell'ordinamento europeo.

In effetti, le Corti costituzionali tedesca e romena, nelle decisioni sul c.d. *data retention*, *in primis* hanno ammesso che la verifica di legittimità costituzionale riguarda non le disposizioni della direttiva europea, ma le soluzioni legislative adottate dallo Stato per raggiungere gli scopi prefissati dall'Unione; in secondo luogo, hanno evidenziato che le modalità di attuazione dovrebbero essere adottate in modo da non contrastare o compromettere i diritti fondamentali.

Se la rilevanza degli interessi da proteggere è tale da giustificare la compressione di tali 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.

Di conseguenza si pone la questione del limite entro il quale può operare il legislatore nazionale e quello europeo nella compromissione dei diritti contenuti nella Carta, considerando quanto previsto dall'art. 52, comma 1, a garanzia del "contenuto essenziale" di detti diritti e libertà, che dovrebbe segnare il confine invalicabile delle limitazioni ai diritti fondamentali.

In altri termini esso costituirebbe il "limite dei limiti"[46] o, meglio, il contenuto di garanzia minimo inderogabile e essenzialmente costitutivo di una libertà[47].

Pur considerando la rilevanza delle teorie relativa, assoluta e dell'essenzialità del limite[48],

[44] Vedi Corte cost., n. 203 del 1985, in *Giur. cost*., 1985, p. 1575. Si veda anche R. BIN, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992, p. 94 ss.

[45] L'"interesse generale", dovendo essere riconosciuto dall'Unione, "include certamente se non principalmente quelle ipotesi in cui esso possa essere perseguito soltanto attraverso gli strumenti normativi europei, ove siano coinvolte competenze di pertinenza dell'Unione". In questo senso già L. PIROZZI, *Separazione dei poteri e garanzia dei diritti nel progetto di costituzione europea*, in A. D'ATENA-P.F. GROSSI, *Tutela dei diritti fondamentali e costituzionalismo multilivello. Tra Europa e Stati nazionali*, Milano, 2004, p. 85 ss. Si veda anche R. TONIATTI, *Verso la definizione dei "valori superiori" dell'ordinamento comunitario: il contributo della Carta dei diritti fondamentali dell'Unione Europea*, in R. TONIATTI (a cura di), *Diritto, diritti, giurisdizione. La Carta dei diritti fondamentali dell'Unione Europea*, Padova, 2002, p. 7 ss.; cfr., inoltre, F. PALERMO, *La Carta dei diritti fondamentali dell'Unione Europea tra diritto positivo e positività del diritto*, *ivi*, p. 195 ss.

[46] I. MASSA PINTO, *Contenuto minimo essenziale dei diritti costituzionali e concezione espansiva della Costituzione*, in *Dir. pubbl*., 2001, p. 1095 ss., in specie p. 1097.

[47] T. GROPPI, *Art. 52*, in R. BIFULCO-M. CARTABIA-A. CELOTTO, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Bologna, 2001, p. 351 ss., in particolare p. 355.

[48] Si rinvia a E. DENNINGER, *Zum Begriff des Wesensgehaltes in der Rechtsprechung (art. 19, comma 1, GG*), in *Die öffentliche Verwaltung*, 13, 1960, p. 812 ss. Vedi anche V. EPPING, *Grundrechte*, Heidelberg, 2005, p. 55 ss. Per una sintesi vedi recentemente P. RIDOLA, *Introduzione*, in P. HÄBERLE, *Le libertà fondamentali nel-*

che non possono, per evidenti ragioni, essere compiutamente analizzate in questa sede, preme evidenziare che, sul piano della struttura, ogni libertà costituisce un elemento costitutivo dell'ordinamento costituzionale e ciascun diritto fondamentale subisce dei limiti rispetto alla tutela di altri diritti, di pari rilevanza, che a loro volta costituiscono l'ordinamento. Di conseguenza, il nucleo essenziale inviolabile dovrebbe essere individuato da questa relazione fra diritti e libertà fondamentali, ossia nella limitazione di queste ultime che consentono la realizzazione di altri valori costituzionali.

In conclusione l'art. 52 della Carta considera tale bilanciamento fra diritti identificando nel principio di proporzione il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte politico normative del legislatore, delimitandone l'area di discrezionalità.

In questo contesto le sentenze sin qui esaminate, avendo individuato alcuni *standards* normativi ed applicativi, possono già costituire un primo punto di riferimento per il legislatore, anche europeo, che può trovare in esse delle importanti linee guida nel bilanciamento fra contrapposti interessi e in prospettiva di tutela di un nucleo essenziale minimo dei diritti fondamentali. Tale valutazione deve però considerare l'attuale assetto della società dell'informazione e di Internet. Non è possibile pensare di poter affrontare le sfide poste dalle nuove tecnologie, quando sono utilizzate per la commissione di reati, esclusivamente con i tradizionali mezzi investigativi.

Le stesse declaratorie di incostituzionalità non hanno avuto ad oggetto le metodologie di indagine "di carattere tecnologico" in quanto tali, ma i loro modi di utilizzo, nonché i presupposti ed i limiti, anche temporali, per la loro adozione e per la tutela di importanti e predominanti beni giuridici.

La compromissione delle libertà fondamentali in materia penale, in specie nella lotta a gravi forme di criminalità e nell'ambito del settore delle indagini ad alto contenuto tecnologico o della conservazione dei dati di traffico telematico, dunque, non può essere preclusa *ab origine*, pur dovendo in ogni caso essere di carattere eccezionale e comportare interferenze minime.

lo Stato costituzionale, Roma, 1993, p. 12 ss.; D. BUTTURINI, *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, Napoli, 2009, p. 174 ss.

CAPITOLO 3

La responsabilità dei fornitori di servizi di informazione in Internet

di *Domenico De Natale*

SOMMARIO: 1. Premessa. – 2. La responsabilità dei fornitori dei servizi di informazione per le immissioni *on line* da parte di terzi di contenuti lesivi dell'altrui reputazione. – 3. La pretesa responsabilità del *blogger*. – 3.1. *Segue*. L'inutilizzabilità dei riferimenti normativi della legge sulla stampa e della legge sui sistemi radio-televisivi. – 3.2. *Segue*. I servizi offerti in internet e la loro presunta natura editoriale. Riserve sugli effetti a cascata sul versante della responsabilità penale. – 3.3. *Segue*. L'inapplicabilità dei dettami imposti dal c.d. Decreto Pisanu per il contrasto del terrorismo internazionale. – 4. I nuovi scenari in materia desumibili dal caso Google. – 5. L'esito processuale del caso Google. – 6. Conclusioni. Soluzioni alternative all'ipotesi di irresponsabilità degli ISP. – 6.1. *Segue*. Conclusioni in tema di elemento psicologico.

1. Premessa

Il profilo della responsabilità penale dei fornitori di informazioni in internet [1] rappresenta oggi un tema di interesse non solo teorico ma anche pratico se si considera che le possibilità di ognuno di propagare le proprie idee sono state notevolmente ampliate grazie alla capacità multimediale ed alla interoperatività dei nuovi sistemi di comunicazione nell'epoca del c.d. *web* 2.0.

L'incremento esponenziale dei nuovi sistemi operativi in internet, la crescente creazione di siti e *blog* che hanno dato vita a nuovi *attori della conoscenza* e che hanno messo in luce un complesso meccanismo caratterizzato da fluidità, evanescenza, cattiva gestione, profitto quale regola prioritaria, criminalità impalpabile anche a causa del ricorso, reale o supposto, all'anonimato, ha generato non indifferenti problemi nell'individuazione dei centri di responsabilità penale e nell'individuazione del modello secondo il quale ascriverle. Gli interpreti si

[1] In argomento si veda L. PICOTTI, *Fondamento e limiti della responsabilità penale dei service-providers in* internet, in *Dir. pen. proc.*, 1999, p. 379 ss.; ID., *La responsabilità penale dei service-providers in Italia*, in *Dir. pen. proc.*, 1999, p. 501 ss.; ID., *Profili penali delle comunicazioni illecite via internet*, in *Dir. inf.*, 1999, p. 283 ss.; volendo D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet per i casi di diffamazione on line***,** in *Riv. trim. dir. pen. econ.*, 2009, p. 509 ss. In giurisprudenza, con riferimento al reato di diffamazione, Trib. Oristano, sent. 25 maggio 2000, Giud. Tuveri, imp. Z e altra, con nota di C. RUSSO, *Internet, libertà di espressione e regole penali: spunti di riflessione a margine di una pronuncia in tema di diffamazione*, in *Foro it.*, II, 2000, c. 663 ss.; sulla responsabilità del *blogger*, Trib. Aosta, sent. 26 maggio-1 giugno 2006, n. 553, in *Giur. merito*, 2007, p. 1065 ss., con nota critica di I. SALVADORI, *I presupposti della responsabilità penale del blogger per gli scritti offensivi pubblicati su un blog da lui gestito* e in *Dir. Internet*, 2006, p. 486 ss. con nota di P. GALDIERI, *Giornalismo, diffamazione e blogging*. Con riferimento alla posizione dei titolari di siti *web* per i casi di diffusione di materiale pedopornografico ad opera di terzi si veda Trib. Milano, sent. 18 marzo 2004, in *Giur. merito*, 2004, p. 1713 ss., con nota di F. RESTA, *La responsabilità penale del provider: tra laissez-faire e obblighi di controllo*.

interrogano, con riferimento al settore della tutela dell'altrui reputazione disciplinata dall'art. 595 c. p., sulla possibile responsabilità degli *internet service provider* (ISP)[2], nel tentativo di individuarne la disciplina che contemperi il diritto di libertà di impresa, il diritto della libertà di informare e di essere informati, il diritto della persona a non subire deformazioni nella dimensione sociale.

2. La responsabilità dei fornitori dei servizi di informazione per le immissioni *on line* da parte di terzi di contenuti lesivi dell'altrui reputazione

Preliminarmente, in via generale ed astratta, appare opportuno rilevare che "*quando una notizia risulti immessa sui cc.dd. media, vale a dire nei mezzi di comunicazione di massa (cartacei, radiofonici, televisivi, telematici ecc.), la diffusione della stessa, secondo un criterio che la nozione stessa di 'pubblicazione' impone, deve presumersi, fino a prova del contrario*"[3]. Pertanto, l'analisi si snoderà attraverso la valutazione di alcuni casi giurisprudenziali che, sintomatici delle peculiarità dei vari servizi fruibili *on line*, hanno avuto ad oggetto l'attività di *blog*, l'attività di un sito *web* cui era collegato un servizio di *forum* e l'attività offerta con il servizio Google Video gestito dalla Google srl. La giurisprudenza[4] e la dottrina[5] hanno sostanzialmente raggiunto un orientamento, consolidato nei suoi tratti essenziali, secondo il quale internet, intesa in senso lato, rappresenta un sistema di divulgazione delle informazioni veicolate che consente l'applicabilità della disposizione di cui all'art. 595, comma 3, c.p. (in virtù dell'espressione ivi inserita secondo la quale la diffamazione è aggravata se compiuta con "*qualsiasi altro mezzo di pubblicità*")[6] se la condotta dell'autore inequivocabilmente individuato è offensiva dell'altrui reputazione ed esplica i suoi effetti mediante strumenti di comunicazione c.d. aperti, ossia accessibili a chiunque, senza particolare formalità.

Sulla scorta di tale interpretazione e facendo corretta applicazione delle disposizioni penalistiche presenti nella parte speciale del codice è stato condannato per diffamazione aggravata *ex* art. 595, comma 3, c.p. colui che, personalmente, attraverso procedure dirette, aveva creato un sito *web* in cui, autonomamente, aveva inserito messaggi lesivi della reputazione altrui, decontestualizzando l'immagine della persona dileggiata in un luogo che, per quanto virtuale, era da chiunque visitabile[7].

---

[2] La definizione di *internet service provider* si rinviene all'art. 1, lett. c) della Convenzione Cybercrime di Budapest del 2001, leggibile al sito *www.coe.int.*

[3] Testualmente Cass. pen., sez. V., 25 luglio 2006, n. 25875, Pres. Foscarini, in *Dir. Internet*, 2007, p. 166, con nota di A. MACRILLÒ, *Presunzione iuris tantum di pubblicazione e prova del delitto di diffamazione con il mezzo della rete telematica*.

[4] Per le differenti sfumature si vedano Cass. pen., sez. V, 17 novembre-27 dicembre 2000, n. 4741, in *Crit. dir.*, 2000, p. 504 ss., con nota di C. LONGOBARDO, *Il ruolo dell'evento nella diffamazione* "*a mezzo internet*", in cui si afferma, con riferimento alla tecnologia di acquisizione e di trasmissione dei dati mediante internet, che "*le informazioni e le immagini immesse in rete, relative a qualsiasi persona sono fruibili (potenzialmente) in qualsiasi parte del mondo*", Trib. Trani, sez. Molfetta, ud. 18 febbraio 2003 (dep. 16 maggio 2003), imputato XY, con nota di F.G. CATULLO, *Diffamazione telematica attraverso la decontestualizzazione dell'identità*, in *Cass. pen.*, 2003, p. 3956 ss., Trib. Oristano, 25 maggio 2000, cit.

[5] L. PICOTTI, *Profili penali delle comunicazioni illecite*, cit., p. 288 ss., nonché V. SPAGNOLETTI, *Profili problematici del reato di diffamazione a mezzo internet*, in *Giur. merito*, 2003, p. 1622, *sub* nota 15; e seppure con diverse sfumature M. NISTICÒ, *Sui reati contro l'onore per via telematica*, in *Dir. pen. proc.*, 2002, p. 57 ss.

[6] Cfr. Cass. pen., 17 novembre-27 dicembre 2000, n. 4741, cit.

[7] Trib. Trani, sez. Molfetta, udienza 18 febbraio 2003 (dep. 16 maggio 2003), est. Oliveri del Castello, cit., p. 3956. L'imputato, dopo aver creato un sito internet, aveva sviluppato dei messaggi di posta elettronica con i

Più complesso e problematico, invece risulta ancora oggi, l'accertamento del ruolo e la eventuale responsabilità penale di coloro che gestiscono servizi interattivi tramite cui i terzi possano immettere e rendere accessibili al pubblico informazioni, sotto forma di testi, disegni o immagini, aventi contenuto illecito.

È noto che in materia la disputa verte sulla possibilità o meno di configurare una responsabilità commissiva mediante omissione degli ISP secondo il modello che deriva dalla combinazione dell'art. 110 c.p. con l'art. 40 cpv. c.p. [8].

È pacifico che il riconoscimento di una eventuale posizione di garanzia, cui è subordinata l'operatività della clausola di equivalenza prevista dall'art. 40 cpv. c.p., in capo all'ISP richiede a monte di individuare l'esistenza *de jure condito* di un obbligo giuridico di impedire determinati eventi tipici (*rectius* reati) perpetrati in internet o di eliminare specifici contenuti offensivi di altrettanti determinati beni giuridici.

Nel tentativo di individuare la sussistenza di norme cogenti valevoli per la tutela dell'altrui reputazione lesa da soggetti terzi *on line* mediante gli strumenti di comunicazione offerti dagli ISP l'attenzione è stata rivolta alle norme predisposte per la regolamentazione dell'attività di giornalismo [9], valutando la possibilità di equiparare internet alla stampa e il gestore/titolare di un servizio a contenuto informativo al direttore di un giornale o al suo editore.

3. La pretesa responsabilità del *blogger*

Con specifico riferimento all'attività di gestione di un *blog* [10], la giurisprudenza di merito ha osservato che, pur non utilizzandosi la medesima forma semantica per il gestore e proprietario del sito internet su cui altri possono inserire i propri commenti: "… *colui che gestisce il blog altro non è che il direttore responsabile dello stesso*" [11].

La vicenda processuale ha avuto origine dalla denuncia presentata da alcune persone che ritenevano che la loro reputazione fosse stata lesa da alcuni post denigratori veicolati tramite il *blog* "*il bolscevicostanco.com*". Le indagini consentivano di accertare che alcuni messaggi fossero riconducibili alla digitazione del gestore/titolare del *blog* in quanto dallo stesso sottoscritti attraverso uno pseudonimo con il quale era solito firmarsi, mentre per altri, parimenti

quali si invitavano gli utenti a contattare la persona presa di mira, di cui erano stati forniti nome, cognome e numero di telefono cellulare, per ottenere prestazioni sessuali, anche per telefono.

[8] In tema si veda G. GRASSO, *Il reato omissivo improprio*, Milano, 1983, *passim*.

[9] In tale direzione, un obbligo di controllo del materiale veicolato, seppure in ambito civilistico, veniva riconosciuto dal Trib. Napoli, ord. 8 agosto 1996, Est. Schisano, M. Cirino Pomicino s.p.a. c. Geredil s.a.s. ed altri, in *Dir. inf.*, 1997, p. 970 ss.; Trib. Teramo, ord. 11 dicembre 1997, in *Dir. inf.*, 1998, p. 370 ss.; Trib. Cuneo, ord. 23 giugno 1997, in *Giur. piem.*, 1997, p. 493; Trib. Macerata, 22 dicembre 1997, in *Riv. dir. ind.*, 1998, p. 35 ss.. *Contra*, Trib. Roma, 4 luglio 1998, in *Dir. inf.*, 1998, p. 807 ss., con nota di P. COSTANZO, *I newsgroup al vaglio dell'autorità giudiziaria (ancora a proposito della responsabilità degli attori in* internet*)*. Tale ultimo provvedimento escludeva la responsabilità del *provider* per i contenuti diffamatori presenti sul *newsgroup*, in quanto non moderato e, dunque, non soggetto a controllo preventivo. In ambito penale per le attività di *blogging* favorevole all'estensione, Trib. Aosta, cit., p. 1066 e s. la cui pronuncia è stata riformata in parte dalla Corte di Appello di Torino in data 26 aprile 2010, Pres. Witzel che correttamente ha negato i profili di responsabilità ascritti dal primo giudice al blogger con riferimento all'omesso impedimento del reato di diffamazione effettuata, tramite il suo blog, da terzi rimasti anonimi.

[10] Il termine *weblog* "traccia su rete" è stato creato da Jorn Barger nel dicembre del 1997. La versione tronca *blog* è stata creata da Peter Merholz che nel 1999 ha usato la frase "*we blog*" nel suo sito, dando origine al verbo "*to blog*" (ovvero: *bloggare*, scrivere un *blog)*. Così su *http://it.wikipedia.org.*

[11] Testualmente Trib. Aosta, 25 maggio 2006, cit., p. 1066.

lesivi della reputazione dei soggetti presi di mira, postati in modo anonimo, l'autore non veniva individuato. Il *blogger*, titolare e gestore del diario telematico, tratto a giudizio per rispondere del reato di diffamazione aggravata, per fatto proprio e per non aver impedito che terzi offendessero la reputazione altrui, è stato condannato ai sensi dell'art. 596 *bis* c.p., perché riconosciuto responsabile per aver omesso il dovuto controllo sui post da terzi veicolati tramite il servizio dallo stesso offerto e gestito.

Il giudizio di colpevolezza è stato formulato evidenziando asseritamente la sussistenza di un potere di filtraggio dei post inseriti da terzi nell'attività espletata dal gestore di servizi interattivi di *blogging*, in forza dell'astratto totale controllo del materiale postato, e di un conseguente potere di cancellare i messaggi dal contenuto illecito.

Da tali premesse si è fatto derivare in capo al proprietario-gestore l'obbligo di adottare le medesime cautele che sono proprie dell'attività di controllo, esplicitamente riconosciuta dagli artt. 57 e ss. c.p., del direttore, del vice-direttore (nel caso di reati commessi col mezzo della stampa periodica), dell'editore (nel caso di stampa non periodica e nel caso in cui sia ignoto, o non imputabile l'autore dell'esternazione), o dello stampatore (nel caso in cui l'editore non sia indicato, o non sia imputabile).

Internet e i suoi innumerevoli servizi sono stati automaticamente accomunati agli altri mezzi di comunicazione, espressamente indicati dalle norme di settore, contrariamente all'opinione da tempo dominante in dottrina e ai precedenti giurisprudenziali più attenti alle evoluzioni dei mezzi di comunicazione di massa [12].

L'indagine giuridica così impostata, finalizzata all'individuazione degli indici normativi cui riferire la responsabilità dei fornitori di servizi in internet per le attività illecite altrui, e le relative conclusioni si sono rilevate errate e di ciò ne ha preso atto la Corte di Appello di Torino che, investita del gravame proposto dall'imputato, ha riformato la sentenza di primo grado, assolvendolo dalle accuse di non aver impedito che terzi non individuati, sfruttando il suo servizio, offendessero la reputazione di terzi e tenendo ferma la condanna a titolo di diffamazione aggravata del blogger per i post riconducibili alla sua digitazione [13].

La Corte, dopo aver precisato che il blogger fosse in grado di cancellare i commenti, ha richiamato la tesi dell'impossibilità tecnica di vagliare preventivamente il contenuto del materiale postato da terzi. In proposito è stato affermato che la quantità dei messaggi veicolati in rete, ovviamente da vagliare caso per caso, non consente monitoraggi costanti che abbiano efficacia impeditiva dimostrata anche a causa della possibilità di essere costantemente modificati e/o aggiornati dall'autore. Il preteso comportamento, in grado di impedire la perpetrazione di reati in internet, sarebbe in sostanza inesigibile [14].

I giudici hanno, inoltre, fornito esaustive motivazioni in ordine alla tesi dell'inapplicabilità ai fatti commessi *on line* delle norme in cui il concetto di stampa o i suoi derivati, ad es. stampati, concorrono a descrivere il fatto tipico.

L'attività svolta da coloro che offrono e gestiscono servizi di *chat*, *mailing list*, *forums*, *news groups*, *blogs* presenta differenze strutturali rispetto a quella svolta dal direttore di un giornale al punto da non consentire l'estensione ai primi del precetto di cui all'art. 57 c.p. [15].

---

[12] Fra gli altri si veda V. ZENO-ZENCOVICH, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Dir. inf.*, 1998, p. 15 s. In giurisprudenza Trib. Oristano, 25 maggio 2000, cit., c. 670, più di recente Trib. Milano, 18 marzo 2004, cit., p. 1713 s.

[13] App. Torino, 23 aprile-22 luglio 2010, Pres. Est. Witzel, Imp. M., inedita.

[14] In merito si veda G. FORNASARI, *Il ruolo dell'esigibilità nella definizione della responsabilità penale del Provider*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, p. 423 ss.

[15] Ai sensi degli artt. 2, 3 e 5 della legge n. 47 del 1948, "*il direttore è la persona che assume di fronte alla legge penale la responsabilità della pubblicazione e, come tale, viene indicato sul periodico. La norma prevede*

La disposizione codicistica, ora citata, sancisce una responsabilità per fatto proprio omissivo del direttore o vice-direttore responsabile del giornale o di altro periodico per i reati commessi col mezzo della stampa [16]. La norma riflette la sua operatività esclusivamente su soggetti qualificati che assumono il ruolo indicato a seguito di specifica nomina ai sensi degli artt. 3 e 5 della legge 8 febbraio 1948, n. 47 (che prevede norme in tema di stampa). In forza di tale funzione essi assumono la qualifica di garanti della correttezza dell'informazione. Ne consegue che la responsabilità del direttore responsabile o del vice-direttore di stampa periodica [17], nelle ipotesi omissive, si fonda sui precetti di cui agli artt. 57 e ss. c.p. che presuppongono notoriamente obblighi di vigilanza e di sindacato sul materiale che deve essere stampato e da cui deriva l'obbligo di impedire che con il mezzo della pubblicazione siano commessi reati [18] e che può essere efficacemente espletato mediante una penetrante e capillare verifica sul contenuto della informazione, verifica che l'attività professionale svolta impone in ossequio ai dettami del codice deontologico di categoria (ovviamente tenendo conto della dimensione dell'impresa editoriale e della possibilità di delegare le funzioni ai collaboratori in caso di grosse dimensioni).

I servizi offerti in internet, per converso, sono il più delle volte strutturati in modo diverso da un giornale tradizionalmente inteso e dunque non completamente assimilabili ad esso quantomeno sotto il profilo dei risvolti penalistici in caso di omesso controllo da parte dei gestori/titolari del materiale in esso transitante e/o attraverso esso veicolato.

Si è affermato, condivisibilmente, in forza del principio di legalità di cui all'art. 25, comma 2, Cost. [19] e del divieto di analogia in *malam partem* [20], che internet così come l'attività di chi gestisce siti *web* e *blog* non sottostanno alla regolamentazione prevista dalla legge 8 febbraio 1948, n. 47 [21] perché non comportano una riproduzione tipografica o ottenuta con mezzi meccanici o fisico-chimici [22], trattandosi di strumenti e servizi che si caratterizzano per una modalità di trasmissione/ricezione di messaggi in forma elettronica, operata da un soggetto e diretta ad uno o più individui determinati o indeterminati con l'ausilio di una rete di telecomunicazioni.

Se, dunque, le forme di comunicazione telematica e fra esse internet e i servizi che essa offre avvengono con modalità distinte rispetto alle modalità di diffusione della stampa, le norme predisposte per altri settori non sono sovrapponibili ed ampliabili indistintamente ad ogni forma, anche elettronica, di informazione, stante il concepimento originario per modalità

esplicitamente una posizione di garanzia ex art. 40 cpv. c.p.…". Testualmente I. SALVADORI, *I presupposti della responsabilità penale del blogger*, cit., p. 1071.

[16] Secondo M. ROMANO, *sub art. 57*, in M. ROMANO-G. GRASSO, *Commentario sistematico del codice penale*, Milano, 2004, vol. I, p. 616, l'art. 57 prevede un'ipotesi speciale di agevolazione colposa geneticamente dipendente dalla condotta dell'autore dell'articolo a contenuto illecito.

[17] Afferma M. ROMANO, *sub art. 57*, cit., p. 617 che la fattispecie sia di natura complessa e che gli elementi costitutivi siano un fatto colposo del direttore e un evento dato dal reato commesso dall'autore della pubblicazione, che rappresenta sin dall'origine ciò che si vuole evitare con l'imposizione del controllo della pubblicazione.

[18] Fra le altre cfr. Cass. pen., sez. V, 7 luglio 1981, in *Giust. pen.*, 1982, II, c. 699.

[19] Cfr. I. SALVADORI, *I presupposti della responsabilità penale del blogger*, cit., p. 1071, nonché P. GALDIERI, *Giornalismo, diffamazione e blogging*, cit., p. 490.

[20] Cfr. sul punto S. TABARELLI DE FATIS, *La controversa disciplina penale della diffamazione tramite Internet,* in *Dir. inf.*, 2001, p. 314 e 317 e, in giurisprudenza, Trib. Oristano, 25 maggio 2000, cit., c. 670.

[21] L'art. 1 della legge, rubricato con il titolo *Definizione di stampa o stampato* testualmente recita: «*Sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione*».

[22] Cfr. V. ZENO-ZENCOVICH, *La pretesa estensione alla telematica*, cit., p. 16.

diverse di diffusione di notizie, caratterizzate da "*unitarietà fisica e temporale*" [23].

La difficoltà di delimitare un'area di responsabilità penale dei gestori di siti internet ed in particolare per i gestori dei *blog* per gli illeciti commessi da terzi si è mostrata, infine, allorquando è stato analizzato l'art. 596 *bis* c.p. Siffatto richiamo normativo, effettuato dal primo giudice, non è stato condiviso dalla Corte.

L'art. 596 *bis* c.p. si colloca in un contesto specifico (diffamazione a mezzo stampa) che non consente estensioni alle attività similari (internet e servizi telematici) e che non ha funzione incriminatrice, limitandosi a richiamare l'esclusione della prova liberatoria agli imputati di cui agli artt. 57 e ss. c.p. Pertanto, anche se inopinatamente e ripetiamo inammissibilmente, dovesse equipararsi ad esempio il *blogger*-gestore di un diario telematico al direttore di un giornale, eventualmente dall'opzione dovrebbe discendere quale conseguenza giuridica l'applicazione del disposto dell'art. 57 c.p. [24], ma così non può avvenire per le motivazioni sopra esposte.

3.1. *Segue.* L'inutilizzabilità dei riferimenti normativi della legge sulla stampa e della legge sui sistemi radio-televisivi

Inapplicabili appaiono ai fatti commessi *on line* le fattispecie legalmente tipizzate negli artt. 1 e 13 della legge n. 47 del 1948 e nell'art. 30 della legge n. 223 del 1990 per la rilevata impossibilità di procedere ad un'equiparazione dei diversi mezzi di comunicazione di massa, ivi espressamente indicati, obiettivamente diversi rispetto all'internet.

La giurisprudenza di merito si è premurata di sostenere, in forza della diversità delle modalità di una trasmissione effettuata con internet rispetto a quella con i mezzi di diffusione televisiva e radiofonica, che la regolamentazione emanata "*in un periodo storico in cui la stessa creazione della rete di comunicazione Internet non era nemmeno ipotizzabile dal legislatore*" [25] non poteva e non può essere applicata ad altri contesti, diversi dalle trasmissioni radiofoniche o televisive, in cui tuttavia si sviluppano suoni ed immagini, oltre che scritti, il più delle volte con modalità d'interazione.

In linea con tale orientamento ai casi di diffamazione *on line* non può applicarsi il regime di cui all'art. 13 legge n. 47 del 1948, il quale prevede un aggravamento di pena per il caso di attribuzione di un fatto determinato unitamente all'uso del mezzo della stampa [26]. Il richiamo espresso al concetto di stampa e dunque al concetto espresso dall'art. 1 della medesima legge impedisce che si operi un'estensione della disciplina anche ai fatti in internet, sebbene abbiano natura editoriale.

Parimenti inapplicabile si deve considerare la disposizione di cui all'art. 30, comma 4, legge n. 223 del 1990, norma che estende il regime sanzionatorio dell'art. 13, legge n. 47 del 1948 ai concessionari pubblici o privati e ai loro delegati per le ipotesi di diffamazione commesse mediante "*trasmissioni*".

---

[23] Testualmente V. ZENO-ZENCOVICH, *I "prodotti editoriali" elettronici nella l. 7 marzo 2001 n. 62 e il preteso obbligo di registrazione*, in *Dir. inf.*, 2001, p. 158; conforme P. GALDIERI, *Giornalismo, diffamazione e blogging*, cit., p. 490.

[24] La medesima osservazione effettuano I. SALVADORI, *I presupposti della responsabilità penale del blogger*, cit., p. 1070 e P. GALDIERI, *Giornalismo, diffamazione e blogging*, cit., p. 491, il quale sostiene che non tutti i *blog* funzionano allo stesso modo e che pertanto è necessario procedere ala loro previa analisi tecnica.

[25] Testualmente Trib. Oristano, 25 maggio 2000, cit., c. 671.

[26] In merito si veda S. TABARELLI DE FATIS, *La controversa disciplina*, cit., p. 310 per la quale l'art. 13 rappresenta, conformemente alla unanime dottrina e giurisprudenza, un'aggravante complessa ad effetto speciale che comporta un sensibile aumento di pena ed anche l'applicazione congiunta di pena detentiva e pecuniaria.

Infatti, essendo ben individuati i soggetti cui la disciplina si riferisce ed essendo ben chiaro che le norme regolamentano il sistema radio-televisivo, sarebbe contrario al principio di legalità estenderne la portata ai casi in cui fosse l'utente a selezionare il materiale da visionare e le modalità con cui effettuare tale opzione [27].

3.2. *Segue.* I servizi offerti in internet e la loro presunta natura editoriale. Riserve sugli effetti a cascata sul versante della responsabilità penale

Una risposta, altrettanto negativa, deve essere data riguardo alla pretesa equiparazione di internet agli altri mezzi di comunicazione in virtù della legge n. 62 del 2001 [28] con la quale è stato precisato il concetto di "*prodotto editoriale*", in particolare per l'impossibilità di estendere gli obblighi previsti dall'art. 2 della legge sulla stampa [29], non essendo possibile per i siti, o per le banche dati in essi contenuti, o per le singole notizie in essi leggibili, laddove la legge si voglia riferire anche ad essi, indicare luogo e anno di una "*inesistente pubblicazione* – intesa in senso tradizionale – *e il nome e il domicilio di un altrettanto inesistente stampatore*" [30].

Sotto questo versante merita di essere appuntato il contrario orientamento espresso dal Tribunale di Firenze che ha condannato il titolare di un sito *web* a titolo di diffamazione aggravata per aver omesso il controllo del contenuto dei messaggi veicolati tramite un *forum* ad esso collegato [31].

Il giudice, dopo aver dato atto dell'obiettiva valenza diffamatoria dei messaggi inviati da alcuni utenti sul *forum*, della inapplicabilità dell'esimente del diritto di critica, della non veridicità del fatto determinato attribuito alla persona offesa, ha sostenuto che il direttore di una testata telematica soggetta a registrazione qual era quella diretta dall'imputato avesse violato l'obbligo di controllo e verifica delle informazioni rese fruibili dal servizio offerto senza particolari formalità, obbligo scaturente dalla registrazione cui sarebbero sottoposti coloro che, operando nel *web*, agiscono con funzioni editoriali.

Rilevato, inoltre, che nel caso di specie non potesse ravvisarsi un concorso *ex* art. 110 c.p. con l'autore dell'esternazione diffamatoria, il profilo di responsabilità del direttore è stato impostato dal giudice sul modello dell'art. 57 c.p. così motivando: "[i]*l sito internet, inteso qua-*

---

[27] Cfr. V. SPAGNOLETTI, *Profili problematici*, cit., p. 1625.

[28] Sull'argomento si veda V. ZENO-ZENCOVICH, *I "prodotti editoriali" elettronici nella l. 7 marzo 2001 n. 62*, cit., p. 153 ss.. La normativa intitolata "*Definizione e disciplina del prodotto editoriale*" all'art. 1 recita: "*Per 'prodotto editoriale', ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografico*"; il comma 3 che ai nostri fini interessa dispone: "*Al prodotto editoriale si applicano le disposizioni di cui all'art. 2 della legge 8 febbraio 1948, n. 47. Il prodotto editoriale diffuso al pubblico con periodicità regolare e contraddistinto da una testata, costituente elemento identificativo del prodotto, è sottoposto, altresì, agli obblighi previsti dall'art. 5 della medesima legge n. 47 del 1948*".

[29] L'art. 2 della legge n. 47 del 1948 recita: "*Ogni stampato deve indicare il luogo e l'anno della pubblicazione, nonché il nome ed il domicilio dello stampatore e, se esiste, dell'editore. I giornali, le pubblicazioni delle agenzie di informazione e i periodici di qualsiasi altro genere devono recare la indicazione: del luogo e della data della pubblicazione; del nome e del domicilio dello stampatore; del nome del proprietario e del direttore o vice direttore responsabile. All'identità delle indicazioni, obbligatorie e non obbligatorie, che contrassegnano gli stampati, deve corrispondere identità di contenuto di tutti gli esemplari*".

[30] Testualmente V. ZENO-ZENCOVICH, *I "prodotti editoriali" elettronici nella l. 7 marzo 2001 n. 62*, cit., p. 159.

[31] Trib. Firenze, 13 febbraio 2009, consultabile al sito *www.penale.it*.

le insieme di hardware e di software attraverso cui si genera il prodotto telematico sotto forma di trasmissione di flussi di dati, in quanto prodotto editoriale, ai sensi della l. n. 62/2001, si deve ritenere sottoposto anche ai fini penali alla disciplina sulla stampa"[32].

Traendo spunto da questo orientamento giurisprudenziale si rendono necessarie alcune precisazioni. L'interpretazione ristretta attribuibile al concetto di "*prodotto editoriale*", secondo cui per prodotto si deve intendere ciò che rappresenta il "*risultato di un'attività imprenditoriale o, comunque, svolta professionalmente ed a fine di profitto*"[33], consentirebbe un'equiparazione della informazione in rete alla stampa solo in forza del ricorso all'attività di giornalisti professionisti, di cui le testate telematiche dovrebbero dotarsi, al fine di rendere effettivamente attuati gli *standards* professionali, sempre più richiesti in un settore ad alta competitività.

Pur condividendosi tale premessa, costituisce un salto logico, a nostro sommesso avviso, l'affermazione del Tribunale di Firenze secondo la quale in "*caso di diffamazione commessa con il mezzo di un giornale telematico, non possono non richiamarsi le norme del codice penale in materia di stampa, ossia l'art. 595 co. 3 c.p. e l'art. 57 c.p.*" dato che i periodici *on line* appartengono "*al* genus *della stampa*", che sono soggetti "*alle indicazioni obbligatorie in tema di editoria previste per gli stampati e alla registrazione obbligatoria della testata (art. 1 co. 3)*", che sono curati da ‹‹*un direttore responsabile*" e che hanno "*un editore*" i cui nominativi "*devono essere riportati sul sito web*". Non può, infatti, non rilevarsi come simili rilievi denotino una chiara ipotesi di procedimento analogico in *malam partem*, essendo stata operata nel caso di specie una estensione di quelle norme che, proprio perché dotate di caratteri peculiari, primi fra tutti il richiamo al concetto di stampa e stampato, dovrebbero essere espressamente previste anche per internet attraverso un'azione svolta esclusivamente dal legislatore.

La registrazione richiesta dalla legge, che secondo l'opinione del Tribunale fiorentino costituirebbe la fonte da cui origina il conseguente obbligo di monitoraggio delle informazioni veicolate in rete, rappresenta un semplice onere e non un obbligo, da assolvere nel momento in cui una persona decide di trasformare il semplice "*titolo*" identificativo di un sito in "*testata*"[34], ciò solo con la finalità di ottenere le provvidenze in materia di editoria, così come desumibile sin dalle prime battute della legge secondo cui "[p]*er* 'prodotto editoriale', *ai fini della presente legge*, *si intende* ...".

La normativa n. 62 del 2001, pertanto, non costituisce fonte di obblighi la cui violazione possa avere rilievo penale a titolo di omissione, in virtù del fatto che i fini in essa previsti ed esplicitati in ben 19 dei 21 articoli che la compongono riguardano erogazioni di provvidenze e concessioni di agevolazioni a favore di taluni soggetti.

Da tanto deriva che nel caso in cui la notizia sia apparsa solo in rete, mediante una testata

[32] Così Trib. Firenze, 13 febbraio 2009, cit. Circa l'impossibilità di equiparare agli stampati le manifestazioni del pensiero attuate attraverso la rete Internet, e con riferimento alla possibilità di sequestro del sito si veda Cass. pen., 11 dicembre 2008, Ric. Aduc, in *Foro it.*, 2010, II, c. 95, con nota di CHIAROLLA, *Riflessioni intorno al concetto di prodotto editoriale digitale*, e più recentemente Trib. Cassino, Ufficio del giudice delle indagini preliminari, Giudice Tudino, sent. 26 giugno 2009, consultabile al sito *www.dirittoegiustizia*, arretrato del 3 ottobre 2009.

[33] Così S. TABARELLI DE FATIS, *La proposta di riforma della disciplina sulla diffamazione a mezzo Internet. Osservazioni critiche*, in *Dir. Internet*, 2006, p. 195.

[34] Per V. ZENO-ZENCOVICH, *I "prodotti editoriali" elettronici nella l. 7 marzo 2001 n. 62*, cit., p. 1163 s., il termine testata è rappresentativo non di un fatto, bensì di una qualificazione giuridica. Vi è testata solo se vi è iscrizione nel registro della stampa e se ciò ha un senso questo significa che disporre che, ai sensi dell'art. 1, comma 3, legge n. 62 del 2001, devono essere iscritte le testate rappresenta un'inversione logica di un processo che notoriamente prima prevede solo un titolo e solo a seguito di registrazione una testata che in tal modo diventa elemento identificativo di un prodotto.

telematica registrata, come accaduto nel caso in commento, il direttore responsabile potrà rispondere solo ai sensi dell'art. 595, comma 3, c.p. e in forma monosoggettiva se risulterà allo stesso attribuibile la paternità dell'informazione illecita veicolata nei confronti di un numero indeterminato di utenti, stante il carattere potenzialmente diffusivo dello strumento utilizzato. Potrà rispondere a titolo di concorso materiale o morale nel medesimo reato qualora l'informazione dal contenuto illecito sia stata materialmente creata da un terzo e dell'attività di partecipazione al reato sussistano in capo al direttore responsabile tutti gli elementi oggettivi e soggettivi richiesti.

Per converso, allo stato, se il direttore abbia solo colposamente permesso a terzi di "pubblicare" *on line* contenuti lesivi dell'altrui reputazione dovrà evidenziarsi, per le ragioni sopra dette, l'impossibilità di applicare la disciplina sulla stampa *ex* art. 57 c.p., vigendo nel nostro ordinamento il principio di legalità e il divieto di analogia.

3.3. *Segue.* L'inapplicabilità dei dettami imposti dal c.d. Decreto Pisanu per il contrasto del terrorismo internazionale

La difficoltà di individuare *de iure condito* una norma cogente che sancisce l'obbligo giuridico di impedimento del reato di diffamazione trova conferma in un altro caso che ha visto coinvolto il gestore di un *internet point* accusato di aver consentito che, tramite il proprio punto commerciale, un utente inviasse ad una casella di posta elettronica, consultabile da parte di più soggetti, messaggi lesivi dell'altrui reputazione.

Contestata nel caso di specie la diffamazione, proprio per l'indirizzamento *ad incertam personam* del messaggio, prima i giudici di merito e poi la Suprema corte di cassazione [35] hanno affermato il principio secondo cui il gestore dell'*internet point* non è legittimato ad esercitare un potere di interferenza sull'operato altrui, non avendo il diritto di conoscere e controllare il contenuto dei messaggi veicolati tramite l'attività commerciale messa a disposizione degli avventori, essendo ciò vietato nel nostro diritto, in forza dell'art. 617 *quater* c.p. e, aggiungiamo, dell'art. 616, ult. comma, c.p., non rivestendo il ruolo tipico proprio dei pubblici ufficiali ai quali, solo nei casi e nei modi stabiliti, è concesso un potere di intervento nella sfera privata degli utenti, limitando diritti costituzionalmente garantiti.

Sul punto si osserva che le comunicazioni postate per *e-mail* rientrano certamente nell'ambito di tutela di cui all'art. 15 Cost. che sancisce l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione [36].

In tale direzione si è preferito privilegiare la tutela della riservatezza della corrispondenza telematica e, conseguentemente, proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali [37].

Sotto tale profilo merita condivisione la soluzione adottata dalla Suprema Corte di cassazione.

L'accusa, nel formulare il capo d'imputazione aveva rilevato che l'omessa preventiva identificazione di colui che aveva utilizzato il terminale per l'invio di posta elettronica, desumibile da una delibera del Consiglio dell'Autorità per le Garanzie nelle comunicazioni n. 467 del 2000 (delibera integralmente trasfusa nel c.d. Decreto Pisanu adottato il 16 agosto 2005,

[35] Cass. pen., sez. V, sent. 11 novembre 2008-11 febbraio 2009, n. 6046, in *CED*, n. 242960.

[36] Analogamente V. SPAGNOLETTI, *La responsabilità del provider*, cit., p. 1932.

[37] Cfr. *Le linee guida del Garante per posta elettronica e Internet-Provvedimento a carattere generale-Delibera 1 marzo 2007, n. 13*, in *Dir. Internet*, 2007, p. 314.

recante misure urgenti per il contrasto del terrorismo internazionale e ad oggi prorogato)[38], costituisse violazione di un obbligo giuridico gravante sul titolare/gestore dell'esercizio commerciale in grado di far ascrivere il reato di diffamazione *ex* art. 40 cpv. c.p.

La Suprema Corte, nel dichiarare inammissibile il ricorso della parte civile avverso le sentenze di assoluzione, correttamente ha motivato che allo stato non sussiste alcun obbligo per i gestori di *internet point* finalizzato ad impedire reati commessi da terzi tramite le loro strutture e che l'obbligo di annotare nell'apposito registro i dati anagrafici dell'utente (*ex* art. 1, comma 1, lett. *b* del decreto Pisanu), anche laddove assolto non avrebbe impedito il reato.

Tale ultimo decreto è finalizzato a contrastare essenzialmente il terrorismo e gli obblighi ivi sanciti costituiscono il presupposto che fornisce la prova dell'utilizzazione del terminale da parte dell'utente. Essi, data la loro funzione, non possono costituire il riferimento normativo da cui desumere un obbligo di impedimento di tutti i reati astrattamente realizzabili *on line*, erigendo i gestori degli *internet point* a guardiani di un'internet sana. Se poi si riflette che, ai sensi dell'art. 2 del medesimo decreto, è vietata la memorizzazione dei contenuti delle comunicazioni non si scorge nel preteso obbligo la necessaria funzione preventiva di impedire l'uso criminoso della comunicazione informatica. A tutto concedere, laddove tramite un *internet point* un fatto costituente reato dovesse realizzarsi, il gestore o il titolare dell'esercizio pubblico (che ha messo a disposizione un terminale per le comunicazioni telematiche) potrà essere ritenuto responsabile a titolo di concorso attivo con l'autore primario se si dimostrasse che al fatto di reato commesso dal terzo egli abbia apportato un contributo causale (avendo determinato l'inoltro della comunicazione) e sussista la piena conoscenza della delittuosità della comunicazione.

4. I nuovi scenari in materia desumibili dal caso Google

Gli insormontabili limiti giuridici, in particolare nel momento in cui oggetto di analisi è la pretesa attività di intermediazione passiva[39], sono stati oggetto di disputa nel noto caso Google[40] scaturito dalla pubblicazione su *You Tube* di un video nel quale alcuni ragazzi, vessando e percuotendo un compagno diversamente abile, offendevano la sua reputazione e quella di un'associazione tutoria mediante espressioni denigratorie[41].

La Procura di Milano si è occupata della posizione dei vertici amministrativi di Google Italy srl., fornitore e gestore del servizio Google Video.it, contestando oltre al reato di illecito trattamento di dati sensibili riguardanti il minore ignobilmente ripreso per essere deriso *ex* art. 167 d.lgs. n. 196 del 2003, anche il reato di diffamazione (artt. 595, comma 1 e 3 c.p.) *ex* art. 110 c.p., 40 cpv. c.p. perché in concorso fra loro e mediante omissione consentivano che i giovani utenti del servizio (giudicati separatamente e condannati dal Trib. dei minorenni di

[38] Il decreto è pubblicato in *Guida dir.*, 5 novembre 2005, 43, p. 47 ss.

[39] Così viene anche definita l'attività di *hosting* disciplinata dall'art. 16 del d.lgs. n. 70 del 2003 relativo al c.d. commercio elettronico.

[40] Le motivazioni della sentenza del Tribunale di Milano, n. 1972 del 2010 del 24 febbraio 2010, depositate il 12 aprile 2010, sono leggibili nel blog *www.Roberto_flor.blogspot.com.*

[41] Il caso è stato oggetto di aspro dibattito fin dalle sue prime battute. In proposito si vedano G.M. RICCIO, *Solo la neutralità degli internet provider può salvare la rete da un ‹‹effetto gelo››*, in *Guida dir.*, 2008, 48, p. 107; G. CORRIAS LUCENTE, *La pretesa responsabilità penale degli intermediari di contenuti su Internet*, in *Dir. inf.*, 2009, p. 91 ss.; L. BONESCHI, *La procura della repubblica di Milano, un errore della rivista e una discussione necessaria*, nota del direttore responsabile a seguito di richiesta di rettifica *ex* art. 8 legge 8 febbraio 1948, n. 47, in *Dir. inf.*, 2009, p. 735 ss.; F. SGUBBI, *Parere pro veritate*, in *Dir. inf.*, 2009, p. 745 ss., formulato su richiesta del difensore della parte civile Associazione Vivi Down.

Torino a 10 mesi di messa alla prova da svolgersi con attività di volontariato presso la medesima associazione offesa) effettuassero l'*upload* e di seguito diffondessero per il tramite del medesimo servizio offerto da Google il filmato girato.

L'obbligo giuridico formale non rispettato da ciascuno degli amministratori nella rispettiva qualità è stato individuato nel contesto della disciplina relativa al trattamento dei dati personali *ex* d.lgs. n. 196 del 2003, per non avere proceduto nel lanciare il servizio Google Video.it in conformità del disposto di cui all'art. 13 in tema di informativa sulla privacy, per non avere acquisito il preventivo consenso del titolare dei dati sensibili trattati secondo quanto sancito dall'art. 23, comma 3, per i casi di comunicazione o diffusione degli stessi, per non aver rispettato l'art. 26, essendo i dati veicolati e comunque trattati mediante quel servizio idonei a rivelare lo stato di salute della persona ripresa con un videofonino e per non avere rispettato l'art. 17 che prescrive l'interpello presso l'Autorità Garante, nonostante i rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato, insiti nel tipo di trattamento omesso.

La dottrina[42] già nel 1999 aveva individuato il modello in grado di identificare obblighi giuridici posti a fondamento di una responsabilità concorsuale *ex* art. 110 c.p. per contributo omissivo di partecipazione richiamando il sistema delineato dalla legge sulla tutela dei dati personali *ex* legge n. 675 del 1996, in virtù dell'ampia definizione del concetto di ‹‹*trattamento*›› [43] e dell'ampia definizione della locuzione "*dati personali*" [44]. Autorevolmente si era sostenuto che potesse sussistere responsabilità a titolo di omissione per l'offesa all'altrui reputazione realizzata tramite la diffusione di dati sensibili se i dati fossero stati trattati e conseguentemente resi accessibili ai terzi in violazione delle prescrizioni imposte dalla normativa (previo consenso del titolare dei dati, notifica o autorizzazione delle autorità competenti), se la condotta oltre a ledere la riservatezza ledesse anche l'onore e la dignità della persona offesa[45].

La vicenda Google ha chiaramente attinto da questo esempio riproponendolo in chiave aggiornata alla normativa attuale di cui al d.lgs. n. 196 del 2003. Il fulcro della ritenuta attività di trattamento illecito di dati è stato individuato nel sistema di raccolta pubblicitaria denominato AdWords[46].

Si è sostenuto che il dato relativo al minore diffuso tramite il servizio offerto rappresentasse un dato sensibile, in quanto idoneo a rivelare lo stato di salute dello stesso a nulla rilevando l'uso improprio di termini tecnici, effettuato dagli autori del video, in grado di identificare correttamente lo *status* reale di diversamente abile. Si è, altresì, sostenuto che l'attività di Google Video fosse stata ideata e messa in atto senza curare il rispetto della normativa italiana

[42] L. PICOTTI, *La responsabilità penale dei service-providers*, cit., p. 505.

[43] Si veda l'art. 4, comma 1, lett. a), d.lgs. n. 196 del 2003 secondo cui per trattamento si intende "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione,la cancellazione e la distruzione di dati, anche se non registrati in una banca dati*". Pertanto, l'art. 23 del medesimo decreto richiamato nel capo di imputazione si riferisce non solo al trattamento in senso proprio dei dati ma anche alla loro comunicazione o diffusione, vietando le stesse senza il consenso dell'interessato.

[44] Si veda l'art. 4, comma 1, lett. d), d.lgs. n. 196 del 2003 secondo cui per dati sensibili si intendono, fra l'altro, quelli idonei a rivelare "*lo stato di salute e la vita sessuale*" dell'interessato.

[45] L. PICOTTI, *La responsabilità penale dei service-providers*, cit., p. 505.

[46] Si tratta di un sistema che tramite alcune parole chiave, digitate da un qualunque utente al momento della richiesta/ricerca, permette di far apparire sullo schermo dell'utente del servizio un messaggio pubblicitario ad esse collegato, consente alla società che gestisce il servizio Google Video la monetizzazione dell'inserzione. Cfr. Trib. di Milano, sent. n. 1972 del 2010, cit., p. 17 s., *sub* nota 30 e p. 63 ss.; memorie di replica dei p.m. *ex* art. 121 c.p.p. dell'8 febbraio 2010, p. 11 s. e, più diffusamente, memoria dei p.m. al Tribunale, pp. 97-108.

ed europea in tema di trattamento di dati, con particolare riferimento all'obbligo di informativa che il titolare del trattamento deve rispettare nei confronti dell'interessato affinché quest'ultimo, in relazione ai dati che lo riguardano, possa esprimere un consapevole consenso al trattamento ovvero esercitare i propri poteri di autodeterminazione [47].

Si è, infine, sostenuto che il regime di irresponsabilità per gli *internet provider* non potesse essere desunto da norme pattizie (nella specie l'informativa offerta dal gestore agli utenti del servizio in tema di privacy) di difficile comprensione e sottoposte ad un discutibile regime di accettazione, così derogando alle norme imperative di cui al d.lgs. n. 196 del 2003; che non potesse essere richiamato il regime di irresponsabilità predisposto, al fine di garantire la libera circolazione di beni e servizi [48], dall'art. 17 del d.lgs. n. 70 del 2003 [49] per le seguenti ragioni: l'indubitabile prevalenza del bene oggetto di tutela del codice relativo ai dati personali (diritti fondamentali della persona riconducibili all'art. 2 Cost.) [50] rispetto all'art. 41 Cost.; le limitazioni del decreto sul commercio elettronico che, ai sensi dell'art. 2, comma 1, lett. *b*), non regolamenta le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali; il ruolo di Google Video che non può nel caso di specie considerarsi mero intermediario passivo, ai sensi dall'art. 16 d.lgs. n. 70 del 2003, bensì *hoster* attivo in quanto "*non si limita, per così dire, a fare il suo mestiere*" [51], come accade normalmente per qualsiasi motore di ricerca che agisce a richiesta del destinatario del servizio, ma appronta le pagine *web*, le organizza, le modifica inserendovi *link* pubblicitari, le indicizza, dispone del diritto di escludere dalla diffusione ad un pubblico indeterminato il materiale ritenuto inopportuno o non idoneo.

5. L'esito processuale del caso Google

Il modello di responsabilità ricostruito nella forma della compartecipazione omissiva non ha sortito gli effetti sperati, ossia porre un freno all'indiscriminato sfruttamento di dati altrui per finalità di lucro, senza il previo consenso dell'interessato e comunque in spregio degli obblighi imposti in materia di tutela dei dati personali, considerato dall'accusa il presupposto del reato di diffamazione.

Il Tribunale di Milano, nell'assolvere dal reato di diffamazione così come ascritto, pur condividendo l'analisi tecnica sviluppata dall'accusa in ordine alla predisposizione ed al funzionamento del servizio Google Video, ha disatteso sotto il profilo giuridico ed in relazione al reato di diffamazione i profili di responsabilità concorsuale omissiva ascritti ai vertici della società.

---

[47] Cfr. art. 13, comma 4, d.lgs. n. 196 del 2003 e artt. 10 e 11 Direttiva 46/1997/CE, nonché memorie di replica dei p.m., cit., p. 27 s. e dottrina *ivi* citata *sub* nota 158.

[48] Cfr. art. 1 d.lgs. n. 70 del 2003, attuativo della direttiva 2000/31/CE.

[49] Su punto sia consentito rinviare a D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet*, cit., p. 559 ss.

[50] Cfr. memorie di replica dei p.m., cit., p. 29.

[51] Così P. COSTANZO, *Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutela dei diritti?*, in *Dir. Internet*, 2006, p. 648. Sulla finalità della prestazione di *hosting* si veda di recente I.P. CIMINO, *I contratti degli Internet Providers e per i data services on line*, in G. CASSANO-I.P. CIMINO (a cura di), *Diritto dell'internet e delle tecnologie telematiche*, Padova, 2009, p. 20. Con riferimento al servizio aste fornito da eBay si vedano in ambito comparato *United States District Court-Northern District of California* – M. Hall Patel (Judge), 4 marzo 2008 – M. Mazur – eBay – Hot Jewelry Auctions.com e *Tribunal de Commerce de Paris*, 30 giugno 2008 – Pres. Geronimi – S.A. Christian Dior Couture – eBay, con nota di E. FALLETTI, *I vestiti nuovi di eBay: operatore neutrale o intermediario attivo nelle aste su Internet?*, in *Dir. Internet*, 2008, p. 567 ss.

Sotto il profilo tecnico è apparsa condivisibile la ricostruzione del ruolo svolto nel caso di specie dal servizio Google Video.

Il Tribunale ha, infatti, affermato che con tale servizio l'ISP non assolve la funzione di mero intermediario di informazioni da altri create e veicolate *on line* in quanto provvede, anche attraverso la campagna pubblicitaria denominata AdWords, a raccogliere dati, ad organizzarli e a diffonderli, integrando gli estremi di una attività di trattamento che deve svolgersi in conformità ai dettami del d.lgs. n. 196 del 2003 [52].

In casi del genere l'ISP, di cui va evidenziata la "*polifunzionalità*" [53] e l'"*ambivalenza*" delle condotte concretamente poste in essere [54], garantendo un nuovo sistema di informazione "*partecipata*" o "*collaborativa*" attraverso cui si fornisce all'utente-lettore di interagire con i contenuti del servizio, va considerato alla stregua di un fornitore di contenuti o secondo equivalente definizione un *hoster* attivo.

La posizione concretamente rivestita da Google, che nel servizio offerto organizza le pagine *web*, ne cura l'aggiornamento quantomeno sotto il profilo pubblicitario, impedisce di farla rientrare nel contesto delle garanzie e del regime di irresponsabilità di cui all'art. 17 del d.lgs. n. 70 del 2003 secondo il quale gli *hosting provider* sono esenti da obblighi generali di sorveglianza "*sulle informazioni che trasmette o memorizza*" e da obblighi generali di ricerca attiva di "*fatti o circostanze che indichino la presenza di attività illecite*", avendo solo un dovere di informare se a conoscenza di presunte attività illecite altrui le autorità competenti (le sole in grado di intervenire con poteri di inibizione) o di collaborazione mediante la fornitura di informazioni che consentano l'identificazione del destinatario dei suoi servizi a richiesta delle autorità competenti, peraltro non sanzionato nelle forme dell'omissione propria.

Ne consegue che l'ISP, oltre a fungere da fornitore di contenuti, rispondendo in casi illeciti per fatto proprio, può, rendendo concretamente accessibili ad un pubblico indeterminato informazioni e dati pur provenienti da terzi, assumere il rischio di rispondere penalmente anche a titolo di responsabilità concorsuale [55], se le comunicazioni rivolte *ad incertam personam* sono penalmente rilevanti.

Sotto il profilo giuridico il giudice milanese ha, inoltre, osservato che i "*comportamenti complessivi che vengono effettuati ai danni del ragazzo disabile (e non solo le parole citate) […] evidenziano un atteggiamento dei responsabili del fatto che non può essere ridotto ad un 'gioco'", si tratta "di atti di persecuzione nei confronti di una persona solo perché 'diversa'*" in cui "*le parole diffamatorie sono solo una piccola parte della violenza complessiva*" e che l'aver considerato l'associazione Vivi Down responsabile del fatto in questione rappresenta una condotta evidentemente volta a denigrare sia l'universo down sia quella parte che di quel mondo mostra di avere interesse [56].

Il fatto descritto nel capo di imputazione si presenterebbe sotto questo profilo tipico, ai sensi dell'art. 595, comma 3, c.p., antigiuridico per non essere scriminato da una causa di giustificazione, come ad esempio il diritto di cronaca [57].

---

[52] Cfr. Trib. di Milano, sent. n. 1972 del 2010, cit., p. 74 ss.

[53] Per ulteriori approfondimenti sia consentito il rinvio a D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet*, cit., p. 509 ss. e alla dottrina *ivi* citata.

[54] Si veda D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004, p. 124.

[55] Cfr. F. RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'internet provider*, in *Giur. merito*, 2001, p. 593.

[56] Cfr. sentenza Trib. Milano, n. 1972 del 2010, cit., p. 100.

[57] In proposito dubbi esprime G. CORRIAS LUCENTE, *La pretesa responsabilità penale degli intermediari*, cit., p. 98.

Tuttavia, puntualizza il Giudice, l'ipotesi dell'accusa, ingegnosamente costruita in forma di compartecipazione omissiva, non può trovare conferma allo stato attuale in quanto non esiste "*un obbligo di legge codificato che imponga agli ISP un controllo preventivo della innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web, e non appare possibile ricavarlo* aliunde *superando d'un balzo il divieto di analogia in malam partem*" [58].

Con tali rilievi il giudice registra *de iure condito* che la violazione della legge relativa al corretto trattamento dei dati personali, e per la quale sono stati condannati, non possa fungere da ulteriore copertura di comportamenti diversi e che indirettamente incidano sulla reputazione di un individuo, aggiungendo, altresì, che ad oggi non esiste una legge che equipari l'attività degli ISP alla attività giornalistica espletata su carta stampata o al servizio espletato dalle reti televisive.

Osserva, in aggiunta, che il preventivo controllo, sotto il profilo del necessario consenso dell'interessato, di tutti i dati personali circolanti in rete, meglio in quella porzione di rete, di fatto oltre a causare l'immediata impossibilità di funzionamento del servizio [59] imporrebbe ad un terzo la preventiva conoscenza di tutti i dati personali e particolari di tutte le persone che ogni momento "*transitano*" sul *web*, ossia l'assolvimento di un obbligo irrealizzabile [60].

Tralasciando l'esame di quest'ultimo profilo, sembrerebbe che il Tribunale abbia seguito l'orientamento che nega la sovrapposizione dei beni giuridici oggetto di tutela delle disposizioni previste dal codice di tutela dei dati personali e del reato di diffamazione per giungere alla conclusione che non possono venire in considerazione tutele riflesse di beni che non rientrano nell'area di tutela diretta e specifica delle posizioni di garanzia [61].

Considerando i beni oggetto di tutela della disciplina del d.lgs. n. 196 del 2003 si scorge, in effetti, che l'art. 2, rubricato "*Finalità*", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali che, pertanto, assurge ad autonoma categoria, così come emerge ai sensi dell'art. 1 del codice.

L'identità personale [62], evocata quale bene oggetto di tutela specifico, presenta tratti suoi propri che la distinguono dalla riservatezza [63], dall'onore [64] e dalla reputazione [65] in quanto attiene al diritto di ciascuno ad essere se medesimo nel rapporto di relazione con la comunità in cui l'individuo afferma la propria personalità, a non vedersi disconosciuta la paternità delle proprie azioni, nel più ampio significato e, soprattutto, a non sentirsi attribuire la paternità di azioni non proprie, a non vedersi travisare la propria personalità individuale, ovverosia, il diritto ad essere se stesso, come partecipe della vita associata, con le acqui-

[58] Testualmente, sentenza Trib. Milano, n. 1972 del 2010, cit., p. 103.

[59] Cfr. sentenza Trib. Milano, n. 1972 del 2010, cit., p. 104.

[60] Cfr. sentenza Trib. Milano, n. 1972 del 2010, cit., p. 96.

[61] Cfr. G. GRASSO, S*ub* art. *110*, in M. ROMANO-G. GRASSO, *Commentario sistematico del codice penale*, vol. II, Milano, 2005, p. 177.

[62] In merito si veda A. MANNA, *Beni della personalità e limiti della protezione penale*, Padova, 1989, p. 233 ss.

[63] Sull'argomento si veda S. FIORE, *Riservatezza* (diritto alla): IV diritto penale (voce), in *Enc. giur. Treccani*, *App. agg*., VII, Roma, 1999, p. 1 ss. e dottrina *ivi* citata.

[64] A. MANNA, *Beni della personalità*, cit., p. 177 ss.

[65] Sul bene reputazione, quale riflesso oggettivo dell'onore, si veda A. MANNA, *Privacy on line: quali spazi per la tutela penale?*, in *Dir. Internet*, 2005, p. 266.

sizioni ideologiche, religiose, morali e sociali che differenziano e tratteggiano l'individuo [66].

Il bene oggetto di tutela specifica del d.lgs. n. 196 del 2003 può essere inteso allora in una duplice valenza, positiva e negativa, quale libertà di escludere l'indiscriminato accesso di terzi ai dati personali e quale libertà di garantire all'interessato il controllo della correttezza e non eccedenza del trattamento al fine di salvaguardare l'identità personale [67].

A tal proposito si è osservato che i due beni riservatezza e onore/reputazione, nonostante siano certamente confinanti presentano una linea di demarcazione il cui solco si è ulteriormente accentuato già a far data dal 1996 con la legge n. 675 fino a segnare una netta linea di demarcazione con l'introduzione del Codice per la protezione dei dati personali del 2003 che ha reso il diritto alla riservatezza alla stregua di un bene superindividuale per una pluralità di ordine di ragioni: burocratizzazione degli strumenti di tutela, affidamento al Garante di importanti compiti con funzioni di disciplina, prevenzione e sanzione, presenza di disposizioni di rilevanza penale la cui violazione è perseguibile d'ufficio [68].

Proprio tale condizione di procedibilità è stata considerata la riprova dello iato che sussiste fra i due reati (illecito trattamento di dati e diffamazione, reato procedibile a querela) e la conferma della indisponibilità del bene giuridico oggetto di tutela del codice relativo ai dati personali che per ciò stesso assume una dimensione collettiva e non più individuale, proprio perché non rimesso alla disponibilità del titolare dei dati sensibili trattati e divulgati senza il suo consenso [69], come confermano le funzioni affidate in materia all'Autorità garante (si pensi ai poteri di dirigismo previsti dall'art. 154 del Codice) le cui prerogative sono tutelate attraverso reati di natura funzionale.

Inoltre, il Tribunale ha sostenuto che possono verificarsi casi in cui dalla lesione della riservatezza non derivi una lesione della reputazione perché l'onore, quale bene giuridico diverso ed ulteriore, rimane comunque integro come sembra evincersi dall'esempio citato dal giudice che definisce colpevole ai sensi dell'art. 167 il fatto di mostrare un video che riprenda una particolare preferenza sessuale di un soggetto senza dare all'atteggiamento tenuto dal protagonista alcuna connotazione negativa o derisoria [70]. In questi casi sussistendone i presupposti oggettivi e soggettivi la condotta corrisponde al fatto tipico di rivelare dati personali idonei a rivelare la vita sessuale, ma non raggiunge gli estremi della diffamazione.

---

[66] A. MANNA, *Il diritto di cronaca, di critica, di denuncia e la diffamazione: "gli arresti giurisprudenziali"*, in *Cass. pen*., 2003, p. 3613. L'identità personale, pertanto, si distingue dalla riservatezza perché la tutela dell'identità non è volta ad escludere una certa sfera della propria vita privata dalla curiosità esterna, ma al contrario riguarda attribuzioni pubbliche della persona. Essa attiene solo "*al momento gnoseologico del rapporto di un soggetto con gli altri (potendosi risolvere indifferentemente in conseguenze positive, negative o neutre)*". Così F.G. CATULLO, *Diffamazione telematica*, cit., p. 3965 che aggiunge come nei casi di diffamazione attraverso la decontestualizzazione dell'identità ciò che viene compromessa è la "verità".

[67] Cfr. Cass. pen., sez. III, sent. 28 maggio 2004-9 luglio 2004, n. 30134, in *CED*, n. 229472 e in *Dir. pen. proc.*, 2005, p. 338 ss. con nota di E. ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale*.

[68] G. CORRIAS LUCENTE, *Le recenti prescrizioni del Garante sulla pubblicazione di atti di procedimenti penali e la cronaca giudiziaria. Rigide interferenze tra privacy e libertà d'informazione*, in *Dir. inf.*, 2007, p. 593 s., nonché P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica*, cit., p. 189, laddove si osserva, seppure in relazione all'art. 35 legge n. 675 del 1996, che tale fattispecie pur avendo un più diretto aggancio alla tutela della riservatezza risulta funzionale in realtà a scopi ulteriori rispetto a prerogative individuali, per come si evince dal regime di procedibilità d'ufficio e dalla limitata valenza del consenso in funzione scriminante.

[69] Si veda, seppure con riferimento alla precedente disciplina di cui alla legge n. 675 del 1996, S. CAGLI, *La rilevanza del consenso nella disciplina del trattamento dei dati personali*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica*, cit., p. 298.

[70] Cfr. sentenza Trib. Milano, n. 1972 del 2010, cit., p. 90.

6. Conclusioni. Soluzioni alternative all'ipotesi di irresponsabilità degli ISP

Da quanto finora osservato sembrerebbe attestarsi un preteso regime di irresponsabilità per gli ISP che, pur essendo qualificabili come *hoster* attivi, non impediscano nonostante la violazione delle norme del codice di tutela dei dati personali anche la lesione dell'altrui reputazione. A nostro sommesso avviso una soluzione oggi praticabile sussiste e consiste nel contestare il reato di diffamazione aggravata a titolo di concorso attivo.

Una conferma a tale orientamento, almeno in linea astratta, proviene proprio dalla giurisprudenza citata come caso emblematico dall'accusa che, seppure relativa al contesto della violazione dei diritti di autore [71], supporta la tesi secondo la quale l'ISP che non sia un mero intermediario passivo ma un *hoster* attivo può a ragione rispondere in concorso con i terzi anche anonimi ai sensi del solo 110 c.p. [72].

Invero, un corretto inquadramento della responsabilità dei *provider* potrebbe individuarsi procedendo alla determinazione delle condotte attive di predisposizione di servizi aggiunti, il cui esempio emblematico è costituito dall'attività di *blogging* che consente a terzi di immettere i propri contributi e di renderli fruibili agli utenti del servizio ed oggi da Google Italy che "[a]*ttraverso il sistema AD Words ed il riconoscimento di parole chiave* [… ha] *sicuramente la possibilità di collegare, attraverso la creazione di link pubblicitari, le informazioni riguardanti i clienti paganti alle schermate riguardanti Google Video, e quindi, in qualche modo, gestire, indicizzare, organizzare anche i dati contenuti in quest'ultimo sito*" [73].

L'attività di fornitura dell'accesso e di strutture di supporto tecnico e logistico, propedeutica alla veicolazione dei dati, assolutamente "*incolore*" quando l'ISP si avvale esclusivamente di procedure automatizzate senza acquisire e gestire l'*hardware* e le infrastrutture di telecomunicazione occorrenti per la divulgazione in rete, lo rendono un semplice "*common carrier*" che permette a terzi, autoresponsabili, la trasmissione autonoma delle informazioni [74].

L'esegesi della responsabilità muta, invece, già sul piano oggettivo quando un *provider* permette a terzi di inserire *post* o video a contenuto diffamatorio, assicurando con la sua attività la ulteriore memorizzazione e diffusione dei contenuti**,** assumendo un ruolo che, non più agnostico, è idoneo a far assumere alla condotta del *provider* un "*quid pluris*" rispetto alla sua solita attività, causalmente rilevante per l'attività costituente reato [75].

Il contributo rilevante del *provider* rileverebbe se, inserendosi nell'iter esecutivo, almeno parzialmente, proseguisse quello messo in atto dall'autore primario o originario [76], emergendo quale indispensabile anello nella catena causale della diffusione del contenuto illecito. Proprio sotto il profilo causale, quindi, il fatto di reato sarebbe addebitabile a tutti i concorrenti (*provider* compreso) laddove, eliminata mentalmente la funzione di apporto del *service provider* al fatto di reato, esso non si sarebbe realizzato concretamente con quelle modalità [77], essendo irrilevanti "*i processi causali ipotetici che avrebbero eventualmente operato al posto di quello*

[71] Cfr. Cass. Pen. sez. III, 29 settembre 2009-23 dicembre 2009, n. 49437, in *Foro it.*, 2010, II, c. 136 ss.; Cass. pen., sez. III, 4 luglio 2006-10 ottobre 2006, n. 33945, con nota di R. FLOR, *La rilevanza penale dell'immissione abusiva in un sistema di reti telematiche di un'opera dell'ingegno protetta:* bene iudicat qui bene distinguit?, in *Dir. inf.* 2007, p. 557 s.; Trib. Milano, 18 marzo 2004, cit., p. 1714 s.

[72] A sostegno del concorso commissivo L. PICOTTI, *Fondamento e limiti della responsabilità*, cit., p. 380.

[73] Cfr. sentenza Trib. Milano, n. 1972 del 2010, cit., p. 96.

[74] Trib. Cuneo, 19 ottobre 1999, in *Aida*, 2000, p. 705.

[75] Si veda Cass. pen., sez. III, sent. n. 49437 del 2009, cit., c. 139.

[76] G. GRASSO, *sub art. 110*, in *Commentario*, cit., p. 167.

[77] Sul punto G. GRASSO, *sub art. 110*, in *Commentario*, cit., p. 166.

reale"[78], bensì emergendo le modalità di propagazione[79] così come verificatesi e accertate *hic et nunc*.

6.1. *Segue.* Conclusioni in tema di elemento psicologico

Sotto il profilo psicologico, seppure il Tribunale di Milano si sia espresso richiedendo la "*consapevolezza del fatto delittuoso, al di là della esistenza di posizioni di garanzia non mutuabili da altri settori dell'ordinamento*", e che tale prova, è stato aggiunto, non è stata pienamente conseguita per l'estrema difficoltà dell'effettuazione delle indagini e per la difficoltà di ricostruzione del profilo soggettivo che deve sorreggere la condotta del soggetto agente in vicende di questo tipo, si osserva come invece sia sufficiente anche in tema di diffamazione il semplice dolo eventuale[80] da intendersi come minima consapevole accettazione del rischio[81]. Ciò non significa che sia sufficiente dimostrare la semplice supposizione del fatto illecito altrui che può rappresentare solo un neutro segnale di allarme[82], essendo necessaria la prova dell'effettiva rappresentazione della diffamazione in capo al gestore del servizio fondata, ad esempio, sui seguenti elementi: evidenza del contenuto diffamatorio, perché le espressioni utilizzate nel post o per veicolare il video o quest'ultimo di per sé sono manifestamente offensivi e lesivi della reputazione dei soggetti cui si riferiscono; il tempo di "*affissione*" (*rectius* permanenza) del post o del video nel sistema (una maggiore permanenza del post o del video anche in presenza di comprovate segnalazioni con il sistema di *flag in* sulla sua inopportunità, come avvenuto concretamente nel caso del minore denigrato nel servizio Google Video, può essere sintomatica, se non dell'adesione al contenuto, quantomeno della sua conoscenza, con conseguente accettazione del rischio che il fatto determini un reato); la valutazione di eventuali penetranti controlli sulla operatività del sistema (si pensi ai controlli attraverso il sistema di *mosaic tool* o per controllare la funzionalità del sistema pubblicitario denominato AdWords); l'attività di aggiornamento dei contenuti da cui dedurre logicamente che il fatto incriminato non è passato inosservato e che le conseguenze penali sono state accettate.

[78] Così G. GRASSO, *sub art. 110*, in *Commentario*, cit., p. 166.

[79] Cfr. per tutti L. PICOTTI, *La responsabilità penale dei service-providers*, cit., p. 502.

[80] Sul tema si vedano F. BRICOLA, *Dolus in re ipsa*, Milano, 1960; L. EUSEBI, *In tema di accertamento del dolo: confusioni tra dolo e colpa*, in *Riv. it. dir. proc. pen.*, 1987, p. 1060 ss.; L. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993.

[81] Con riferimento alla responsabilità dei *service providers* L. PICOTTI, *La responsabilità penale dei service-providers*, cit., p. 502 s. Con riferimento al servizio di *blog* sia consentito rinviare a D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet*, cit., p. 574 ss. Con riferimento al servizio Google Video si veda F. SGUBBI, *Parere pro veritate*, cit., p. 747. In tema di diffamazione a titolo di dolo eventuale, cfr. Cass. pen., sez. V, 5 novembre 1998, n. 1794, in *Cass. pen.*, 2000, p. 372.

[82] Sui segnali di allarme si veda D. PULITANÒ, *Amministratori non operativi e omesso impedimento di delitti commessi da altri amministratori*, in *Le società*, 2008, p. 902 ss., particolarmente p. 905 ss. il quale osserva che essi devono essere univoci.

CAPITOLO 4

Intercettazioni e Spazio di Libertà, Sicurezza e Giustizia [*]

di *Michele Panzavolta*

SOMMARIO: 1. Intercettazioni. – 2. Intercettazioni e spazio. – 3. Alcune prassi giurisprudenziali in tema di cooperazione giudiziaria. – 4. La richiesta di intercettazioni nel quadro dell'assistenza rogatoriale convenzionale. – 5. Dentro l'Unione: 1) il perfezionamento dei meccanismi di mutua assistenza giudiziaria (la Convenzione di assistenza giudiziaria di Bruxelles del 2000). – 6. *Segue*: 2) il superamento dei meccanismi di assistenza giudiziaria. – 7. *Segue*: 3) mutuo riconoscimento probatorio e intercettazioni. – 8. Scenari.

1. Intercettazioni

Per indagare il tema "intercettazioni e spazio di libertà, sicurezza e giustizia", ossia della disciplina dell'Unione europea in tema di intercettazioni, si deve procedere per gradi e affrontare prima il rapporto fra "intercettazioni e spazio". Per vero, sarebbe anzitutto necessario soffermarsi sullo stesso concetto di "intercettazioni", un punto che qui sarà velocemente toccato solo per delimitare i confini del presente intervento. Resteranno infatti esclusi dalla presente analisi:

a) le intercettazioni ambientali (fra presenti), le quali, presupponendo un collegamento fisico col bersaglio da intercettare, pongono problemi di azione transfrontaliera diversi da quelli delle intercettazioni telefoniche e più simili a quelli delle tradizionali misure d'investigazione. Il caso problematico in questo ambito pare essenzialmente quello della microspia collocata nel veicolo che oltrepassa la frontiera, questione risolta dalla Corte di cassazione italiana ammettendo la legittimità di tale pratica anche oltre i confini nazionali [1];

b) i tabulati, ossia i dati esteriori delle comunicazioni, la cui disciplina a livello europeo è tendenzialmente distinta da quella delle intercettazioni. Lo conferma la decisione quadro del 18 dicembre 2008 sul mandato europeo di ricerca della prova (2008/978/JHA), la quale, nell'escludere dal proprio ambito di applicazione tanto le intercettazioni quanto la raccolta dei tabulati, tiene le due ipotesi rigorosamente distinte (v. art. 4 decisione quadro sul mandato di ricerca della prova). Anche in questo caso i profili di cooperazione giudiziaria che rilevano assumono fisionomia parzialmente diversa rispetto all'intercettazione di dialoghi, nel senso che non si tratta di operazione di acquisizione di dati in tempo reale. La richiesta e la trasmissione di tabulati esteri può al massimo essere assimilata al caso in cui si richiedano ad uno

[*] Testo corredato di note dell'intervento pronunciato al Convegno "Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali" tenutosi presso l'Università dell'Insubria il 21 e 22 maggio 2010.

[1] Cass., sez. IV, 6 novembre 2007, Assisi, in *CED*, rv. 238951.

Stato estero le registrazioni (o trascrizioni) di conversazioni già oggetto di autonoma intercettazione da parte dell'autorità straniera[2]. Ma anche sotto questo aspetto non può comunque ignorarsi la profonda differenza di natura che sussiste fra tabulati e intercettazioni *strictu sensu*, data dal fatto che i primi non contengono informazioni sul contenuto delle conversazioni, con una consequenziale diversa intensità di lesione della libertà di comunicare riservatamente[3]. Va comunque sin d'ora osservato che, al di là delle regole generali contenute nella direttiva n. 24/2006 (c.d. *data retention directive*), le quali valgono a stabilire un regime uniforme a livello europeo di conservazione dei dati esteriori delle comunicazioni, la richiesta di acquisizione di tabulati all'estero è in linea di massima equiparabile, stando alle norme vigenti, ad una normale richiesta documentale[4].

c) Il discorso nemmeno si focalizzerà sulle intercettazioni telematiche, le cui specificità tecniche non sono qui espressamente tenute in considerazione. Con l'avanzamento tecnologico le intercettazioni di flussi telematici acquisiscono un peso sempre maggiore nell'economia delle indagini. Fra l'altro lo sviluppo di forme di telefonia che sfruttano le linee telematiche (si pensi in particolare ai protocolli Voip, *Voice over internet protocols*) sembra prefigurare uno scenario futuro in cui le intercettazioni telematiche costituiranno la regola, quelle telefoniche l'eccezione. Per quanto vi siano molti punti di contatto fra l'esecuzione di un'intercettazione telefonica e quella di un'intercettazione telematica, le peculiarità di quest'ultima suggeriscono di dedicarle un approfondimento specifico che qui non sarà compiuto. Quanto si verrà dicendo vale dunque per le forme di intrusione telematica solo in linea generale[5], salve le divergenze dovute alle peculiarità tecniche di questo mezzo di prova. Per alcune specifiche regole di cooperazione giudiziaria internazionale in materia di investigazioni digitali, si possono vedere, ad es., la Raccomandazione del Comitato dei Ministri del Consiglio d'Europa R (95) 13 del 15 settembre 1995 e, soprattutto, la Convenzione di Budapest sul cybercrime del 23 novembre 2001 (artt. 27 e 35)[6].

d) Infine, l'intervento si concentrerà sulle c.d. "intercettazioni giudiziarie", ossia quelle effettuate per fini repressivi, di indagine e persecuzione dei reati, ad esclusione quindi delle intercettazioni c.d. preventive, di sicurezza o di *intelligence* (in Italia disciplinate dall'art. 226 disp. att. c.p.p.). Settore quest'ultimo particolarmente insidioso, anche in forza dell'operare a livello europeo del cd. principio di disponibilità delle informazioni di *intelligence*[7].

---

[2] V. *infra*, § 7. Diversa, invece, la richiesta di ottenere i tabulati in tempo reale, la quale pare in effetti corrispondere ad una diversa operazione probatoria, al confine fra tracciamento e *instant monitoring*.

[3] Nel senso che "i due strumenti hanno una capacità lesiva molti diversa", A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 30. Nell'ordinamento italiano, la differenza fra tabulati e intercettazioni è stata sottolineata dalla stessa Corte costituzionale (Corte cost., 11 marzo 1993, n. 81), la quale, pur ritenendo che i dati esteriori delle comunicazioni rientrino nel cono di tutela dell'art. 15 Cost., ha tuttavia escluso che la loro acquisizione al procedimento penale richieda il rafforzato corredo di garanzie previsto per le intercettazioni di comunicazioni.

[4] Una volta, cioè, che l'autorità dello Stato abbia emesso un provvedimento di acquisizione dei tabulati nel rispetto dei presupposti del diritto interno, la richiesta all'autorità estera di acquisizione dei tabulati segue tendenzialmente le norme convenzionali che valgono per le domande di acquisizione di documenti (art. 3 della Convenzione di assistenza giudiziaria del 1959, di seguito anche Conv. 1959).

[5] In proposito, v. specialmente *infra*, § 5.

[6] Cui l'Italia ha recentemente dato attuazione con la legge 18 marzo 2008, n. 48. Sul punto v. L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009.

[7] Sul principio di disponibilità v. G. VERMULEN-T. VANDER BEKEN-L. VAN PUYENBROECK-S. VAN MALDEREN, *Availability of law enforcement information in the European Union*, Maklu, Antwerp, 2005.

2. Intercettazioni e spazio

È complicato sondare il rapporto fra intercettazioni e spazio, poiché la collocazione spaziale dell'atto investigativo è tutt'altro che intuitiva. Eppure è un tema necessariamente preliminare, perché le potestà penali sono (ancora) nazionalmente limitate. Ed il primo punto da chiarire è fin quando l'azione investigativa venga compiuta in uno Stato e quando invece ne travalichi i confini, esigendo perciò che si attivino i meccanismi di cooperazione giudiziale.

Le intercettazioni telefoniche (il discorso è, come detto, in buona parte diverso per quelle ambientali) costituiscono un mezzo di ricerca della prova che, almeno da un punto di vista tecnico, presenta un più labile collegamento territoriale degli altri atti d'indagine. I dialoghi si muovono lungo reti che, con l'evoluzione tecnologica (reti digitali GSM e reti satellitari), sono sempre più refrattarie ai confini statali tradizionali: parole che corrono in spazi la cui fisicità evapora. Ma non solo i dialoghi sono mobili: anche gli utenti possono muoversi e la tecnologia consente loro di continuare a conversare nello spostamento.

Insomma le intercettazioni sono un mezzo due volte subdolo: non solo nel senso tradizionale che restringono una libertà all'insaputa di almeno uno dei dialoganti [8]; ma anche perché altrettanto silenziosamente sono pronte ad evadere dai confini nazionali, a sconfinare ed incunearsi nello spazio di sovranità di altri Stati.

Questo labile collegamento territoriale potrebbe anche portare a concludere che il problema delle intercettazioni nello spazio di sicurezza e giustizia europeo "è un non-problema"; o, comunque, un problema minore, di "piccolo cabotaggio". Le nuove tecnologie consentono in diversi casi di carpire anche dialoghi che si svolgono fuori dal proprio territorio; dunque, si potrebbe dire, ciascuno degli Stati effettui pure l'intercettazione fin dove le potenzialità della tecnica gli consentono di spingersi, senza richiedere l'aiuto di un altro paese. Così inquadrato, il tema delle intercettazioni in Europa si ridurrebbe ai soli casi in cui uno Stato intenda carpire dialoghi rispetto a cui non possiede le capacità tecniche di intercettazione.

È questa una posizione plausibile? Evidentemente no, poiché ci si rassegna ad uno scenario da "*far west* tecnologico", in cui il diritto soccombe alla tecnologia. Ma soprattutto perché, come si dirà a breve, ne uscirebbe stravolto il sistema, tuttora nazionalmente ancorato, di tutela della libertà.

Il problema, allora, rimane e consiste anzitutto nel capire quando l'attività di indagine sia compiuta nel territorio di uno Stato e quando fuori da esso. In proposito, due sono le alternative possibili per localizzare l'intercettazione: o guardare al potere investigativo o concentrarsi sulla libertà ristretta.

1) Si può anzitutto fare riferimento al criterio della sovranità sull'atto investigativo. Questo parametro si appunta sul potere dell'inquirente nazionale di ordinare a soggetti sottoposti alla sua sfera di comando il compimento di intercettazioni. L'intercettazione si svolge in un determinato Stato fintantoché l'autorità inquirente di quel Paese ha la possibilità di ordinarla.

2) In alternativa, si può prendere come riferimento il criterio della libertà violata, valutando il luogo nel quale si verifica la restrizione della libertà di segretezza delle comunicazioni delle persone.

Quale criterio è il più adeguato? Si direbbe il secondo, perché il punto di partenza nella valutazione dei poteri investigativi deve sempre essere quello della libertà. In una concezione liberale del rito penale, il potere investigativo è sagomato come eccezione alla regola della libertà: "sono i diritti fondamentali della persona a definire i limiti dell'interesse statuale alla

[8] Sul carattere "subdolo" ed "insidioso" dell'intercettazione v. A. CAMON, *Le intercettazioni*, cit., p. 1.

attività *lato sensu* istruttoria, di accertamento processuale. All'autorità giudiziaria è vietato qualsiasi atto che incida sui diritti della persona, tranne ciò che è esplicitamente permesso"[9]. E le libertà trovano un radicamento statale, nel senso che esse sono garantite nei confini di ciascuno Stato secondo i principi di quell'ordinamento nazionale – e ad un livello comunque non inferiore allo standard minimo fissato dalla Convenzione europea dei diritti dell'uomo (CEDU)[10].

Di contro, il criterio della sovranità dell'atto investigativo finisce di fatto per legittimare quello scenario da "*far west*" cui poc'anzi si accennava e che genera non poche incongruenze. La più evidente è che la medesima libertà (quella di comunicare segretamente, per usare l'espressione di marca italiana, o di veder rispettata la propria vita privata, per esprimersi nei termini della CEDU) potrebbe essere aggredita nello stesso Stato secondo parametri diversi a seconda della nazionalità dell'organo intercettante.

È per questo che si deve preferire, come criterio di collocamento spaziale dell'intercettazione, quello del luogo in cui la libertà viene ristretta. Ovviamente è un criterio che non risolve tutti i problemi, poiché nel corso di un colloquio riservato telefonico è tutelata la libertà di entrambi i dialoganti, i quali potrebbero anche trovarsi in Stati diversi. Sarebbe però incongruo ritenere che, se un'utenza legittimamente intercettata all'interno di un territorio statale effettua o riceve una chiamata dall'estero, la captazione sia illegittima, poiché incide sulla libertà di comunicazione di persone che si trovano in un altro territorio e sono perciò soggette alle regole di libertà della *lex loci*. D'altronde, nemmeno sarebbe concretamente possibile, né ragionevole, attivare meccanismi di cooperazione giudiziaria in quest'ipotesi. Qui il punto va affrontato partendo dalla struttura del provvedimento intercettivo, il quale si concentra su un bersaglio (che potremmo definire primario od originario), ossia su un'utenza, carpendo poi tutte le parole che vi fluiscono. Nella rete captativa resta così impigliata anche la libertà di comunicazione di terze persone, che invece non costituiscono l'obiettivo primario dell'orecchio investigativo: sono i c.d. terzi intercettati indirettamente. Se si tengono presenti queste osservazioni diviene possibile rispondere alla domanda su quale sia il luogo in cui viene ristretta la libertà quando a conversare sono persone che si trovano in paesi diversi: nell'alternativa si deve guardare al luogo dell'utenza bersaglio[11].

La soluzione corretta, dunque, dovrebbe essere quella di ancorare la "nazionalità" dell'intercettazione al luogo d'uso dell'apparecchio telefonico che costituisce il *target* primario dell'azione investigativa.

Sulla base di questo assunto alcuni casi, apparentemente non problematici, andrebbero rimeditati in una prospettiva di maggiore complessità. Così, per esempio, la posizione secondo cui sarebbe possibile intercettare un'utenza telefonica mobile nazionale anche quando si trovi all'estero. In questi casi, per la Corte di cassazione italiana[12], "non rileva, al fine della individuazione della giurisdizione competente, il luogo dove sia in uso il relativo apparecchio, bensì

[9] F. RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 65, riprendendo le riflessioni svolte da M. NOBILI, *Divieti probatori e sanzioni*, in *Giust. pen.*, 1991, III, c. 641 ss.

[10] Sul livello di tutela previsto dalla Cedu in materia di intercettazioni, v. A. BALSAMO-A. TAMIETTI, *Le intercettazioni tra garanzie formali e sostanziali*, in A. BALSAMO-R. KOSTORIS, *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 426 ss.

[11] Sembra muoversi in questa direzione, A. CIAMPI, *L'assunzione di prove penali all'estero*, Padova, 2003, p. 329.

[12] Peraltro in sintonia con la dottrina; v. F. RUGGIERI, *Le intercettazioni "per instradamento" sul canale internazionale: un mezzo di ricerca della prova illegittimo*, in *Cass. pen.*, 2000, p. 1064; E. APRILE, *Nuovi strumenti e tecniche investigative nell'ambito dell'U.E.: intercettazioni all'estero, operazioni di polizia oltre frontiera, attività sotto copertura e videoconferenze con l'estero*, in *Cass. pen.*, 2009, p. 443.

esclusivamente la nazionalità dell'utenza, essendo tali apparecchi soggetti alla regolamentazione tecnica e giuridica dello Stato cui appartiene l'ente gestore del servizio. Ne consegue che non è necessario esperire una rogatoria internazionale, se le operazioni di intercettazione di un'utenza mobile nazionale in uso all'estero possono essere svolte interamente nel territorio dello Stato" [13].

È vero che per intercettare un'utenza mobile all'estero non vi è bisogno, dal punto di vista tecnico, di richiedere cooperazione ad un altro Stato. Nemmeno si può del tutto ignorare che, in questi casi, lo sconfinamento dell'intercettazione potrebbe avvenire in modo inconsapevole da parte dei soggetti che vi procedono; né che esigere dagli organi intercettanti di attivare una procedura rogatoriale minerebbe profondamento l'efficienza e l'efficacia dell'atto investigativo. L'intercettazione però è tecnicamente possibile solo in forza dei contratti in essere fra gestori di telefonia di diversi paesi. Il ragionamento della Corte, poi, evoca una sorta di principio di personalità nella legge di esecuzione delle intercettazioni, che segue la nazionalità del soggetto o dell'utenza (anzi, del gestore telefonico), su cui è lecito nutrire qualche dubbio.

Già questo è un profilo che dimostra quanto sia essenziale un'opera di chiarimento legislativo a livello sovranazionale.

3. Alcune prassi giurisprudenziali in tema di cooperazione giudiziaria

La tendenza giurisprudenziale – non solo italiana – sembra proprio quella di valorizzare il criterio che riduce al minimo la richiesta di assistenza giudiziaria. Anche per questo gli Stati tendono a privilegiare il primo approccio – quello legato alla sovranità dell'atto investigativo – che porta ad una sostanziale contrazione, al limite dell'elusione, delle forme di cooperazione.

Emblematico in questo senso l'esempio italiano dell'intercettazione per instradamento delle comunicazioni. In cosa consiste l'instradamento? È l'operazione cui ricorrono gli organi inquirenti per intercettare conversazioni effettuate dall'Italia verso l'estero quando si sia a conoscenza del numero straniero. In pratica "è la tecnica che consente, conoscendo il numero di una determinata utenza straniera, di effettuare la intercettazione di un fascio di telefonate partenti dal territorio nazionale, intestate ad utenti ignoti ed individuate nel corso delle operazioni acquisitive per il fatto che esse contattano numeri aventi le prime cifre identiche" [14]. Con questo sistema si intercettano "tutte le comunicazioni che partono dall'Italia e sono dirette verso un'utenza estera determinata, o a un fascio di utenze appartenenti a un determinato distretto geografico, e viceversa. L'istradamento sfrutta, dunque, un accorgimento tecnico che permette di identificare *ex post* il numero identificativo dell'utenza o delle utenze italiane la cui conversazioni telefoniche vengono registrate: gli inquirenti, cioè, conoscono un numero di una utenza straniera, e l'attività d'intercettazione viene autorizzata con riferimento a tutte le comunicazioni e conversazioni in partenza da utenze italiane, ancora indeterminate, e dirette verso quell'utenza straniera, ovvero provenienti da tale ultima e in arrivo verso qualsiasi, ancora non identificata, utenza italiana" [15].

Se si parte dal criterio sopra illustrato, secondo cui l'intercettazione che abbia come ber-

[13] Cass., sez. IV, 7 giugno 2005, Mercado Vasquez, in *CED,* rv. 232080; Cass., sez. I, 16 ottobre 2002, P.G. in proc. Strangio e altri, in *CED*, rv. 222406.

[14] A. DIDDI, *Il regime delle intercettazioni telefoniche per "instradamento"*, in *Giust. pen.*, 2001, III, c. 120 ss.

[15] E. APRILE, *Intercettazioni di comunicazioni*, in A. SCALFATI (a cura di), *Prove e misure cautelari*, in *Trattato di procedura penale* (diretto da G. Spangher), vol. II, tomo II, Torino, 2008, p. 528.

saglio principale un'utenza situata all'estero è un atto che fuoriesce dai confini nazionali ed esorbita quindi dalla potestà giurisdizionale (in questo caso, investigativa) dello Stato, l'instradamento dovrebbe essere bandito e sostituito da un'ordinaria procedura di (richiesta e concessione di) assistenza giudiziaria.

La posizione della giurisprudenza sull' ammissibilità di questa tecnica è però ormai consolidata nel senso opposto: poiché l'attività di intercettazione si svolge materialmente e legittimanente sul territorio italiano è irrilevante che il bersaglio della captazione sia costituito da un'utenza straniera [16]. Le uniche posizioni contrarie alla legittimità dell'istradamento si rinvengono in due pronunce di merito, ormai risalenti rispetto alle reiterate successive prese di posizione della Corte di cassazione [17].

A poco sono valse le obiezioni della dottrina, fondate non solo sull'elusione delle regole rogatoriali, ma anche sulla violazione delle norme interne in punto di presupposti per l'adozione della misura. In effetti, l'instradamento non configura soltanto un atto espletato in carenza di potere investigativo (nel caso di specie, addirittura in carenza di giurisdizione) [18], ma, per giunta, in quanto comporta la restrizione di un fascio di telefonate dirette all'utenza straniera lede la regola prevista dal codice di rito all'art. 267 c.p.p. in punto di indispensabilità dell'operazione di intercettazione ai fini della prosecuzione delle indagini [19]. Il requisito dell'indispensabilità va infatti correttamente riferito non solo al ricorso al mezzo di ricerca della prova, ma anche in relazione all'obiettivo prescelto: a dover essere indispensabile non è solo l'intercettazione in sé, ma più specificamente la sorveglianza di una determinata utenza [20]. In questa cornice, poiché l'instradamento capta un fascio indistinto di telefonate che solo *ex post* vengono identificate e selezionate, l'operazione non è diretta a colpire un preciso bersaglio e si risolve in una forma indiscriminata di intercettazione.

[16] Da ultimo, Cass., sez. I, 4 marzo 2009, Barbaro e altri, in *CED*, rv. 243138: "In tema d'intercettazioni telefoniche, il ricorso alla procedura dell'istradamento, è cioè il convogliamento delle chiamate in partenza dall'estero in un nodo situato in Italia (e a maggior ragione di quelle in partenza dall'Italia verso l'estero, delle quali è certo che vengono convogliate a mezzo di gestore sito nel territorio nazionale) non comporta la violazione delle norme sulle rogatorie internazionali, in quanto in tal modo tutta l'attività d'intercettazione, ricezione e registrazione delle telefonate viene interamente compiuta nel territorio italiano, mentre è necessario il ricorso all'assistenza giudiziaria all'estero unicamente per gli interventi da compiersi all'estero per l'intercettazione di conversazioni captate solo da un gestore straniero". Egualmente, Cass., sez. IV, 28 febbraio 2008, Volante, in *CED*, rv. 239288: "In tema di intercettazione di comunicazioni o conversazioni, è pienamente legittima l'utilizzazione della tecnica del cosiddetto "istradamento", che comporta il convogliamento attraverso un gestore nazionale delle telefonate provenienti dall'estero e dirette ad una utenza italiana, ovvero in partenza da quest'ultima e diretto verso utenze estere, senza che sia necessario promuovere una apposita rogatoria internazionale, posto che l'intera attività di captazione e registrazione si svolge sul territorio dello Stato". Cass., sez. VI, 3 dicembre 2007, Ortiz e a., 239459: "In tema di intercettazioni telefoniche, è legittimo il ricorso alla tecnica del cosiddetto istradamento, che comporta la destinazione ad uno specifico "nodo" telefonico delle telefonate estere provenienti da una determinata zona, senza che venga promossa un'apposita rogatoria internazionale, in quanto l'intera attività di captazione e registrazione si svolge sul territorio dello Stato". Nello stesso senso, in precedenza, v. Cass., sez. IV, 29 maggio 2002, Vercani, in *Cass. pen.*, 2004, p. 957, con nota di M. TIBERI, *L'instradamento delle telefonate straniere: una prassi discutibile*. Nella giurisprudenza di merito, v. Corte App. Bari, 29 marzo 2004, D'A. e altri, in *Dir. pen. proc.*, 2005, p. 223 ss., con nota di N. VENTURA, *Regole tecniche di intercettazione di comunicazioni telefoniche con utenti esteri*.

[17] Trib. Bologna, 23 giugno 1998, Bossert, in *Cass. pen.*, 2000, p. 1068; G.u.p. Roma, 20 ottobre 2000, Barbaro e a., in *Giust. pen.*, 2001, III, c. 120.

[18] F. RUGGIERI, *Le intercettazioni "per instradamento"*, cit., p. 1065 ss.

[19] M. TIBERI, *L'instradamento delle telefonate straniere*, cit., p. 961.

[20] In questo senso, v. Cass., sez. VI, 12 febbraio 2009, p.m. in c. Lombardi Stronati e a., in *CED*, rv. 243241, nonché in *Cass. pen.*, 2009, p. 3341 con nota di V. GREVI, *Un necessario collegamento tra "utenze telefoniche" e "indagini in corso" nel decreto autorizzativo delle intercettazioni*.

La tendenza a rifuggire dalla cooperazione giudiziaria ogni volta in cui la tecnica consenta di gestire l'intercettazione ad un livello esclusivamente nazionale non è solo italiana. Un orientamento giurisprudenziale analogo si rinviene pure in Francia. Anche lì vi sono pronunce della Corte di cassazione che ripetono pedissequamente il ragionamento italiano: se l'attività captativa è attuata nel territorio dello Stato allora l'intercettazione è legittimamente compiuta, a prescindere dal fatto che essa avesse come bersaglio principale un'utenza estera[21]. Conta, per la Corte suprema francese, che le operazioni siano state compiute – legittimamente – sul solo territorio francese e, in particolare, che concernessero telefonate partite dalla Francia[22].

E se in Inghilterra non si rinvengono espressamente pronunce concernenti la legittimità di intercettazioni su utenze situate all'estero, purtuttavia uno sguardo alla legislazione inglese lascia l'impressione che anche in quel sistema sia consentita la sorveglianza telefonica di conversazioni fra utenze britanniche ed utenze estere, a prescindere da quale sia il bersaglio principale della comunicazione (se quello estero o quello britannico). Questa, almeno, la conclusione che sembra potersi indurre dalla definizione di intercettazione contenuta nel *Regulation of investigatory powers Act* (RIPA) 2000, la quale si preoccupa anche di precisare il luogo in cui l'operazione debba ritenersi compiuta. Nel farlo, la previsione inglese mette anzitutto l'accento sul fatto che l'attività di intercettazione sia materialmente compiuta nel Regno Unito ("*if, and only if, the modification, interference or monitoring or, in the case of a postal item, the interception is effected by conduct within the United Kingdom*"), ma vi affianca poi due criteri alternativi: è ulteriormente necessario che a) la comunicazione transiti su un sistema pubblico britannico di telecomunicazioni, oppure che b) pur transitando all'interno di un sistema privato di telecomunicazioni sia effettuata o ricevuta da un utente nel Regno Unito[23]. Sembra dunque che, ai fini della legittimità dell'operazione captativa possa bastare una qualche forma di collegamento con il territorio britannico (che la chiamata circoli sul sistema pubblico di telecomunicazioni o che uno dei due interlocutori sia britannico), potendo anche essere di per sé irrilevante che l'utenza oggetto di sorveglianza sia estera.

Mentre si instradano le conversazioni e si legittimano intercettazioni di utenze oltreconfine, tendono a "deragliare" le libertà di segretezza delle comunicazioni vigenti negli altri Stati e le correlate regole rogatoriali. La violazione dell'altrui sovranità comporta infatti che la libertà di corrispondenza protetta da uno Stato estero venga ristretta secondo le logiche normative (spesso difformi) di un altro Stato. E volendo guardare le cose da un punto di vista italiano – dove le garanzie a protezione della riservatezza delle comunicazioni riservate sono fra le più alte europee – la libertà di segretezza delle comunicazioni delle persone in Italia può soffrire aggressioni, ancor più subdole in quanto non visibili, legate alle regole di restrizione vigenti in altri paesi (sempre supponendo, ovviamente, intercettazioni che siano disposte nel rispetto delle regole dello Stato dalle cui autorità sono effettuate).

[21] Ad esempio, Cour de cassation, chambre criminelle, Audience publique du 14 juin 2000, Bull. Crim. 2000, n. 224 (n° de pourvoi: 00-81.386), in relazione ad un caso di intercettazione di utenza telefonica satellitare "attribuée à un abonné qui demeure hors de son ressort territorial".

[22] Ancor più nititdamente Cour de cassation, chambre criminelle, 26 Mars 2008, Bull. Crim. 2008, n. 74 (n. de pourvoi: 07-88.281), a proposito della legittimità dell'intercettazione di una linea telefonica spagnola "dès lors que les interceptions, réalisée à pàrtir de centres internationaux de transit situés en France, portent sur les appels emis depuis le territoire francais".

[23] La sezione 2(4) del *Regulation of investigatory powers Act* (RIPA) 2000 recita: "*An interception takes place in the United Kingdom if, and only if, the modifcation, interference or monitoring or, in the case of a postal item, the interception is effected by conduct within the United Kingdom and the communication is either: a) intercepted in the course of its transmission by means of a public telecommunication system; or b) intercepted in the course of its transmission by means of a private telecommunication in a case in which the sender or intended recipient of the communication is in the United Kingdom".*

4. La richiesta di intercettazioni nel quadro dell'assistenza rogatoriale convenzionale

Un punto è vero, anche se non può essere un alibi per forme di lassismo giurisprudenziale: i tradizionali meccanismi di cooperazione fondati sull'istituto della rogatoria sono insoddisfacenti, anche perché sono legati ai mezzi di prova e di ricerca della prova tradizionali e non tengono invece conto delle peculiarità (e dell'insidiosità) dei più moderni e tecnologici strumenti probatori, prime fra tutti le intercettazioni.

Il testo normativo fondamentale nell'assistenza giudiziaria europea è ancora la Convenzione di mutua assistenza giudiziaria del 1959 (d'ora in avanti, Conv. 1959), anche detta "convenzione madre".

La Conv. 1959 (in vigore nel nostro paese in forza della legge n. 23 febbraio 1961, n. 215) non disciplina espressamente le intercettazioni, che però vengono generalmente fatte rientrare nell'art. 3 Conv. 1959, stante l'atipicità delle forme di cooperazione contemplata in quell'articolo. Seppur consentita, la richiesta di intercettazioni all'estero manca così nella "convenzione-madre" di una disciplina *ad hoc* [24].

Per accedere alle forme di cooperazione ci si deve dunque basare sui presupposti generali della Conv. 1959. E se è vero che non è più necessario che le domande vengano trasmesse al ministro della giustizia [25], potendo ormai procedersi alla trasmissione diretta fra autorità giudiziarie [26], rimane pur sempre l'inadeguatezza di una disciplina non calibrata sulla peculiarità dell'intercettazione, soprattutto in relazione ai motivi di rifiuto.

Della genericità dell'oggetto della cooperazione nella Conv. 1959 aveva preso atto già nel 1985 il Consiglio d'Europa. Per colmare almeno parzialmente il vuoto sul punto, fu varata la raccomandazione del consiglio d'Europa R(85)10. Essa fornisce alcune direttive per le rogatorie all'estero che abbiano ad oggetto le intercettazioni. Secondo quell'atto – non vincolante, trattandosi di *soft law* – le richieste dovrebbero contenere alcune indicazioni minime: una descrizione quanto più precisa possibile "*of the telecommunication to be intercepted*"; la spiegazione dell'assenza di altri mezzi d'indagine disponibili per raggiungere l'obiettivo investigativo; l'indicazione che l'intercettazione è stata autorizzata dall'autorità competente; l'informazione sulla durata delle intercettazioni.

L'esecuzione della rogatoria potrebbe poi essere rifiutata se: i) secondo la legge dello Stato richiesto non sarebbe possibile effettuare intercettazioni per i reati per cui si chiede l'intercettazione (dovendo quindi preliminarmente sussistere la condizione della doppia incriminazione); ii) se alla luce delle circostanze del caso, l'intercettazione non sarebbe stata giustificata secondo il diritto interno dello Stato richiesto.

La Raccomandazione contiene altresì la possibilità di subordinare l'esecuzione della richiesta ad alcune condizioni, quali la garanzia della distruzione delle intercettazioni irrilevanti

[24] Per considerazioni simili, v. D. FLORE, *Droit pénal européen. Les enjeux d'une justice pénale européenne*, Bruxelles, 2009, p. 355.

[25] Vedi l'art. 53 della Convenzione di applicazione dell'accordo di Schengen del 1990 (superato dall'art. 7 della stessa Conv. EU 2000), che ha sostituito l'art. 15 Conv. 1959 (in cui la trasmissione diretta era confinata ai soli casi di urgenza); v., in argomento, B. PIATTOLI, voce *Rogatorie e cooperazione internazionale nel processo penale*, in *Dig. pen.*, Agg. III, Torino, 2005, p. 1475 ss., ove anche l'osservazione che, nell'ordinamento italiano, il principio di giudiziarietà avrebbe ricevuto "un'applicazione temperata", poiché per le rogatorie passive è comunque previsto che l'autorità giudiziaria italiana ricevente trasmetta una copia della richiesta al Ministro della giustizia; in questo senso dispone l'art. 204-*bis* disp. att. c.p.p., il quale non implica però minimamente una reviviscenza di un controllo politico.

[26] V., sul punto, le precisazioni di E. APRILE, *Nuovi strumenti e tecniche investigative nell'ambito dell'U.E.*, cit., p. 443.

ai fini dell'indagine penale in corso, l'impegno ad informare la persona intercettata al termine dell'operazione, l'assicurazione che i risultati delle intercettazioni non saranno utilizzati ad altri fini (v. punto 4, lett. *a-d*).

Pur preziose, queste indicazioni integrative, in quanto non vincolanti, non riescono a porre rimedio alla lacunosità della disciplina. Resta poi intatto il problema di fondo: per attivare i meccanismi di cooperazione giudiziale è anzitutto necessario che siano definiti normativamente i confini territoriali dell'intercettazione. Emerge così la necessità a livello – almeno – continentale di una disciplina più specifica per le richieste di cooperazione giudiziaria aventi ad oggetto le intercettazioni.

5. Dentro l'Unione: 1) il perfezionamento dei meccanismi di mutua assistenza giudiziaria (la Convenzione di assistenza giudiziaria di Bruxelles del 2000)

Cosa ha fatto l'Unione europea (UE) in questo settore? Si sente spesso ripetere che l'Unione è più concentrata sull'efficienza investigativa che sulle garanzie, che lo spazio di libertà sicurezza e giustizia sarebbe sbilanciato più sulla sicurezza che sulla libertà. L'UE sarebbe animata prevalentemente dalla preoccupazione di perseguire i crimini, mentre il fronte garantista delle istituzioni continentali sarebbe rappresentato dal Consiglio d'Europa (nella cui orbita si inscrive la CEDU).

Un simile giudizio non ricalca però perfettamente le iniziative intraprese in tema di intercettazioni. Lo strumento fondamentale in materia è la Convenzione di mutua assistenza giudiziaria di Bruxelles del 29 maggio 2000 (2000/C 197/01, d'ora innanzi Conv. EU 2000)[27].

Come si legge nell'art. 1, la Conv. EU 2000 è "volta a completare" il quadro normativo esistente in materia di assistenza giudiziaria, integrando quindi la disciplina già offerta dalla Conv. 1959 e dal suo protocollo aggiuntivo del 1978, nonché dalla Convenzione di applicazione dell'accordo di Schengen 1990[28]. Essa fissa, fra l'altro, regole specifiche per la cooperazione giudiziaria riferite alle intercettazioni di telecomunicazioni, concetto che la convenzione non definisce, ma che – secondo la relazione esplicativa[29] – va "inteso nella sua accezione più ampia", sino ad includere le intercettazioni di comunicazioni tramite *internet*[30] e, secondo alcuni, persino gli stessi tabulati[31].

In materia di intercettazioni, la Convezione punta sostanzialmente a tre obiettivi fondamentali: 1) chiarire la dislocazione territoriale delle operazioni di intercettazione; 2) provvedere a superare gli ostacoli tecnici per l'intercettazione di conversazioni di utenti che si trova-

[27] La Convenzione è entrata in vigore il 23 agosto 2005 all'atto della ratifica da parte di otto Stati membri.

[28] In generale, sulla Conv. EU 2000, v. L. SALAZAR, *La nuova convenzione sull'assistenza giudiziaria in materia penale*, in *Dir. pen. proc.*, 2000, pp. 1534 ss. e 1664 ss.; E. CALVANESE-G. DE AMICIS, *Appunti sulla nuova convenzione di assistenza giudiziaria penale tra gli stati membri dell'Unione europea*, in *Giur. merito*, 2000, IV, p. 1052 ss.; E. SELVAGGI, *Una ratifica in tempi rapidi per assicurare l'operatività dello strumento*, in *Guida dir.*, 2000, p. 120 ss.; E. APRILE, *Diritto processuale penale europeo e internazionale*, Cedam, Padova, 2007, p. 48 ss.; E. DENZA, *The 2000 Convention on Mutual Assistance in Criminal Matters*, in 40 *Common Market Law Review* (2003), p. 1047 ss.

[29] Il testo della *Relazione esplicativa sulla convenzione del 29 maggio relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'unione europea* (approvato dal Consiglio dell'Unione europea il 30 novembre 2000) si può leggere nella Gazzetta ufficiale delle Comunità europee del 29 dicembre 2000, C 379, p. 7 ss.

[30] Questa posizione, già espressa nella relazione esplicativa alla convenzione, è condivisa da B. PIATTOLI, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, 2002, p. 181.

[31] Così L. SALAZAR, *La nuova convenzione sull'assistenza giudiziaria in materia penale (II)*, cit., p. 1667.

no sul proprio territorio; 3) definire regole per l'intercettazione oltreconfine[32].

Conviene partire da quest'ultimo punto, che concerne lo scenario tradizionale di uno Stato che voglia intercettare una persona che si trovi sul territorio di un altro Stato, senza averne le capacità tecniche. La strada obbligata per quest'ipotesi è quella di avanzare una tradizionale richiesta di cooperazione giudiziaria, con cui uno Stato chiede ad un altro di procedere ad intercettare l'utenza che si trova nel territorio di quest'ultimo.

La Convenzione si preoccupa di regolamentare questa ipotesi classica, per la quale, si è detto, mancavano prima regole *ad hoc* vincolanti (art. 18, § 2 *b*).

L'autorità giudiziaria (o un'"autorità competente equivalente")[33] dello Stato richiedente dovrà inoltrare una richiesta che indichi: a) l'autorità da cui proviene la domanda; b) la conferma che si tratta di un ordine legittimo emesso nell'ambito di un procedimento penale; c) le informazioni necessarie per l'identificazione della persona da intercettare; d) l'indicazione della condotta criminale sottoposta ad indagine; e) la durata dell'intercettazione; f) la comunicazione, se possibile, di una quantità di dati tecnici sufficienti per soddisfare materialmente la domanda (art. 18, § 3, destinato a sostituire l'art. 14 Conv. 1959 per quanto concerne le richieste di intercettazioni).

Lo Stato richiesto può poi anche esigere una sintesi dei fatti[34], nonché le ulteriori informazioni che gli permettano di valutare se l'intercettazione sarebbe possibile in un caso analogo a livello nazionale (art. 18, § 4)[35]. Nell'ambito di una tale verifica, che ove si concluda negativamente potrebbe condurre ad un rifiuto da parte dello Stato richiesto di prestare cooperazione, dovrebbero rientrare sia il controllo del requisito della doppia incriminazione, sia la sussistenza dei requisiti di ammissibilità dell'intercettazione previsti dal diritto interno.

Questa disciplina configura un regime "aggravato" di cooperazione[36], con regole più rigide di quelle generalmente previste per la richiesta di assistenza giudiziaria oltreconfine.

La Conv. EU 2000 stabilisce poi che la regola sia quella dell'immediata trasmissione del flusso comunicativo allo Stato membro richiedente (art. 18, § 1, lett. *a*), che potrebbe dirsi, mutuando un'espressione di marca italiana, "remotizzazione"[37]. L'eventualità in cui lo Stato

[32] Per una ricostruzione della disciplina della Conv. EU 2000 in materia di intercettazioni di comunicazioni v. A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, in 8 *European Journal of Law Reform* (2006), p. 285 ss.

[33] La Conv. EU 2000 tiene in considerazione il fatto che in alcuni Stati membri le misure d'intercettazione sono disposte da autorità non giudiziarie (organi di polizia, servizi doganali, ecc.), Ai sensi degli artt. 17 e 24, § 1, lett. *e*), Conv. EU 2000, gli Stati membri possono così indicare, al momento della notifica al segretario generale del Consiglio dell'Unione europea, che le richieste di cooperazione giudiziaria concernenti le intercettazioni possono essere avanzate da un'autorità non giudiziaria, "se le autorità giudiziarie non hanno competenza nel settore". Su questo punto, anche per un catalogo di massima delle diverse autorità competenti, v. D. FLORE, *Droit pénal européen*, cit., p. 357.

[34] La *Relazione esplicativa*, cit., p. 22, precisa che "per interpretare questi termini occorre riferirsi all'art. 12, paragrafo 2, lettera *b*) della convenzione europea di estradizione del 13 dicembre 1957, anche se non corrispondono esattamente a quelli utilizzati in detta convenzione".

[35] Questa formula è stata preferita a quella della "conformità al diritto nazionale", la quale avrebbe potuto dar origine a complicazioni per via della tassatività delle previsioni di molte legislazioni nazionali circa le autorità abilitate a disporre l'intercettazione (v. *Relazione esplicativa*, cit., p. 22: "poiché, in linea generale, le varie legislazioni nazionali sulle intercettazioni prevedono in modo restrittive le autorità abilitate a disporre intercettazioni, una richiesta emanata da un'autorità straniera rischierebbe di essere contraria alla legge nazionale sulle intercettazioni").

[36] Di "meccanismo rogatoriale semplificato" parlano E. CALVANESE-G. DE AMICIS, *Appunti sulla nuova convenzione*, cit., p. 1060.

[37] Di "*interception en temps réel*", contrapposta all'"*interception* a posteriori" (ossia, alla registrazione delle conversazioni intercettate), parla D. FLORE, *Droit pénal européen*, p. 357.

richiesto proceda, oltre che all'intercettazione, anche alla registrazione delle telecomunicazioni, per poi inviarle all'autorità straniera richiedente, dovrebbe invece costituire un'eccezione (art. 18, § 1, lett. *b*), nel senso che è possibile ricorrervi solo "se non è possibile effettuare la trasmissione immediata". Questa previsione inverte il rapporto regola/eccezione che da sempre caratterizza la prassi tradizionale di mutua assistenza[38]. Essa reca l'impronta dei plenipotenziari del Regno Unito: secondo il Governo britannico, infatti, la registrazione delle conversazioni è il momento che più lede la libertà di comunicazione delle persone[39].

Si è già visto però che gli sviluppi tecnologici prefigurano anche nuovi scenari: 1) in alcuni casi, uno Stato ha la possibilità tecnica di intercettare al di fuori del proprio territorio; 2) in altri, all'opposto, uno Stato non dispone direttamente della tecnologia per intercettare le conversazioni che si svolgono sul proprio territorio. Queste ultime sono le ipotesi legate alla telefonia satellitare, che può essere intercettata solo tramite stazioni di terra (o di ingresso, *gateway*) del segnale satellitare. Se uno Stato non possiede sul proprio territorio una stazione d'ingresso, allora si trova impossibilitato ad effettuare le intercettazioni.

Rispetto a questi scenari, la Convenzione interviene per rimuovere limiti, ma anche per definire confini, partendo da un criterio preciso: il luogo in cui si trova la persona sottoposta ad intercettazione.

A) *Rimuovere limiti*

Si prevede che uno Stato, il quale voglia intercettare una persona che si trovi sul proprio territorio non disponendo di una stazione d'ingresso (art. 18, § 2, lett. *a*), possa chiedere l'accesso ad un altro Stato, il quale potrà concederlo[40] senza particolare formalità (art. 18, § 5, lett. *a*). Anzi, si può addirittura far domanda per ottenere una sorta di autorizzazione "continuata", nel senso che ad un *provider* di servizi telefonici di un paese sia permesso di accedere sempre alla stazione di terra estera, tramite una sorta di "telecomando" (evitando così di dover ogni volta spiccare una richiesta di cooperazione allo Stato estero), "senza coinvolgere lo Stato in cui è situata la stazione di ingresso" (art. 19, §§ 1 e 2)[41].

Si noti che questa forma semplificata di cooperazione di "*interception from a distance*"[42] non esclude la possibilità di spiccare una più tradizionale richiesta di assistenza giudiziaria, nel senso di chiedere allo Stato in cui si trova la stazione di ingresso di procedere ad intercettazione, il che varrà in particolare per i casi di "mancanza di intermediario nello Stato mem-

[38] A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 297.

[39] A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 297.

[40] È stato giustamente notato che l'uso del verbo "potere" nella lett. *a*) dell'art. 18, § 5 ("*may allow*" nella versione inglese) crea qualche ambiguità, specie se raffrontato con il verbo della frase introduttiva del § 5: "si impegna a soddisfare" ("*shall undertake to comply with the request*" nella versione inglese); A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 293.

[41] La situazione può farsi anche più intricata, per quei casi in cui uno Stato voglia intercettare l'utenza satellitare di una persona situata nel territorio di un altro paese in cui non è presente una stazione d'ingresso (art. 18, § 2, lett. *c*). In questi casi, si dovrà fare richiesta di rogatoria allo Stato terzo in cui si trova la stazione di terra (secondo le previsioni dell'art. 18, §§ 3 e 4) ed ottenere poi l'autorizzazione (secondo quanto prescrive l'art. 20) dallo Stato nel cui territorio si trova l'utenza da sottoporre a sorveglianza. Ma è anche possibile richiedere a quest'ultimo Stato di attivare un "telecomando" presso lo Stato terzo che dispone del *gateway* (art. 19, § 3).

[42] L'espressione è di A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 294.

bro richiedente", ossia quando manchi un in quest'ultimo Stato un fornitore di servizi che disponga della tecnologia per accedere alla stazione d'ingresso (art. 19, § 4)[43].

B) *Definire confini*

Se uno Stato membro ha la potenzialità tecnica di intercettare l'utenza di una persona che si trova all'estero[44], deve tuttavia informare lo Stato nel cui territorio quell'utenza si trova, prima di avviare l'operazione, o subito dopo essere venuto a conoscenza dello spostamento della persona (art. 20, § 2)[45].

L'informativa deve contenere un certo numero di indicazioni[46], in particolare: l'indicazione dell'autorità che ha disposto l'ordine di intercettazione, la conferma che si tratti di ordine legittimo riferito ad un'indagine penale, le informazioni ai fini dell'identificazione della persona sottoposta a intercettazione, l'indicazione della condotta criminale soggetta ad indagine e la durata prevista dell'intercettazione (art. 20, § 3). Si tratta, come si può notare, della stessa quantità di informazioni previste dall'art. 18, § 3 per il caso della domanda di rogatoria allo Stato estero per compiere intercettazioni.

Lo Stato informato deve rispondere immediatamente e comunque non oltre le 96 ore (quattro giorni):

a) se consente che l'intercettazione sia effettuata o proseguita (e può subordinare il suo assenso alle condizioni applicabili ad un caso analogo a livello nazionale);

b) se esige invece che l'intercettazione non sia effettuata o sia conclusa, quando essa sia contraria al diritto interno o ricorra uno dei casi previsti dall'art. 2 della Conv. 1959 (ossia, se la domanda è riferita a reati politici o fiscali, ovvero se la domanda è di natura tale da nuocere alla sovranità, alla sicurezza, all'ordine pubblico o ad altri interessi essenziali del paese)[47]. I motivi del diniego dovranno essere attestati per iscritto. In alternativa al rifiuto, si possono porre specifici divieti o condizioni di uso delle intercettazioni, giustificando le restrizioni poste.

Qualora, per assumere la propria decisione, lo Stato informato dovesse attivare procedure particolari, come ad esempio nel caso fosse necessario munirsi di una autorizzazione per la

[43] Secondo la *Relazione esplicativa*, cit., p. 24, la previsione dell'art. 19, § 4 sarebbe essenziale anche per le ipotesi in cui si possa prevedere che il bersaglio si muova verso un altro Stato membro. V. anche A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 285 ss.

[44] Questa situazione potrebbe verificarsi non solo in relazione ad ipotesi di telefonia satellitare, ma anche a forme di telefonia mobile tradizionale. A. WEYEMBERGH-S. DE BIOLLEY, *The EU Mutual Legal Assistance Convention of 2000 and the Interceptions of Telecommunications*, cit., p. 289), riprendendo le parole della relazione introduttiva, circoscrivono questa seconda eventualità ai casi in cui la conversazione su *network* tradizionali (non satellitari) si svolga "*in border zones, because network coverage cannot correspond exactly to a country's borders*". Rimane aperto però il quesito, già sollevato *supra* nel testo (§ 2), se l'intercettazione all'estero di un'utenza mobile nazionale (*id est*, servita da un *provider* telefonico nazionale) configuri o meno una forma di intercettazione oltreconfine: se la risposta fosse positiva anche quest'ipotesi andrebbe inclusa fra le possibilità di intercettazione "extraterritoriale". Ritiene invece che le previsioni della Conv. EU 2000 siano riferibili ai soli casi di telefonia satellitare, D. FLORE, *Droit pénal européen*, cit., p. 358 s.

[45] Si noti che, per espressa previsione dell'art. 20, § 1, questa disciplina si applica esclusivamente alle intercettazioni c.d. giudiziarie. Per una parziale eccezione a questa regola con riferimento alle intercettazione compiute dal "*security service*" del Regno Unito, v. *Relazione esplicativa*, cit., p. 24.

[46] Ma è lasciata agli Stati la possibilità di dichiarare di non avere bisogno delle informazioni previste nell'art. 20 (art. 20, § 7).

[47] Osserva D. FLORE, *Droit pénal européen*, cit., p. 359, che "*on assiste là a un cumul des conditions de l'entraide judiciaire et du droit national de l'État requis*".

peculiare qualifica del soggetto intercettato (membro del Parlamento, avvocato, etc.), può richiedere per iscritto una breve proroga temporale, fino ad un massimo di otto giorni (oltre i quattro inziali).

L'effettività della decisione dello Stato informato trova poi tutela nella previsione dell'art. 20, § 4: finché non abbia assunto le proprie determinazioni, lo Stato membro che effettua l'intercettazione può proseguirla, ma gli è precluso utilizzare le conversazioni già intercettate, se non per provvedimenti urgenti intesi a prevenire un pericolo grave per la sicurezza pubblica o se diversamente convenuto tra gli Stati membri interessati.

Questa disciplina è stata criticata sostenendo che, se è ragionevole il diritto all'informativa, meno ragionevole è che si preveda "un potere [dello Stato informato] di incidere radicalmente su intercettazioni che (per definizione) sono state comunque lecitamente disposte dall'autorità giudiziaria di un altro Stato membro, sino al punto di poterne ordinare la cessazione e l'inutilizzabilità"[48]. Ed ancora si è detto che "la nuova disciplina reca con sé anche il rischio di creare una serie di "trappole" procedurali possibilmente foriere di effetti negativi sull'utilizzabilità stessa degli elementi raccolti", facendo riferimento alla "situazione di incertezza" di ben dodici giorni che lo Stato informato può imporre allo Stato pronto ad intercettare (o che abbia già avviato l'intercettazione)[49].

La critica però non coglie nel segno. A parte che la disciplina suesposta non pare presentare insidie procedurali eccessive, essa serve invece a ripristinare le sovranità statali e, soprattutto, la regola per cui la libertà nel territorio di uno Stato va rispettata secondo le regole poste da quell'ordinamento giuridico, evitando che le autorità di altri paesi possano compiere pericolose e silenziose incursioni nello spazio di libertà garantito da altri paesi. Allo stesso tempo, anche il tempo concesso allo Stato informato per decidere – che solo in casi eccezionali potrà essere di dodici giorni – non danneggia lo Stato che abbia già avviato l'intercettazione, poiché a quest'ultimo è comunque possibile proseguire la sorveglianza e, ricevuto l'assenso, utilizzare tutte le conversazioni captate.

Complessivamente la Conv. EU 2000 sembra distinguersi proprio per il suo approccio prudente ed equilibrato. Nel prevedere un corposo corredo di informazioni per le richieste di intercettazione all'estero e casi aggiuntivi di rifiuto, nel definire il raggio d'azione dell'intercettazione, nello stabilire che ogni forma di sconfinamento debba essere comunicata e ricevere l'assenso dell'autorità straniera, la Conv. EU 2000 si preoccupa di assicurare che la tutela, predisposta a livello nazionale, della libertà di comunicare riservatamente non venga infranta. Senza perdere di vista l'efficienza della cooperazione, la Convenzione mette dunque al centro della propria azione la protezione della libertà[50]. L'insieme di queste regole non sembra rientrare nel *cliché* dell'Unione europea come istituzione votata alla repressione dei crimini più che alla tutela delle garanzie.

[48] L. SALAZAR, *La nuova convenzione sull'assistenza giudiziaria in materia penale (ii)*, cit., p. 1668,

[49] Sempre L. SALAZAR, *La nuova convenzione sull'assistenza giudiziaria in materia penale (ii)*, cit., p. 1668.

[50] Equivalente giudizio è tratto da B. PIATTOLI, *Cooperazione giudiziaria e pubblico ministero europeo*, cit., p. 181: "La normativa in parola deve essere apprezzata sia sotto il profilo della tutela dei diritti individuali, fornendo una disciplina precisa e rigorosa ad una materia particolarmente delicata come quella delle intercettazioni, sia sotto il profilo dell'integrazione procedurale, atteso il riconoscimento di un obbligo specifico di collaborazione in tale settore da parte di tutti i Paesi membri, ridefinendo così i confini concettuali imposti dal principio di sovranità". Similmente, v. D. FLORE, *Droit pénal européen*, cit., p. 356.

6. *Segue*: 2) il superamento dei meccanismi di assistenza giudiziaria

L'azione dell'UE non si risolve dunque solo nella ristrutturazione dei meccanismi di assistenza giudiziaria. Ad essa si affianca l'introduzione di strumenti volti ad agevolare la cooperazione – anche sul fronte dell'effettuazione di intercettazioni – che scavalcano la logica tradizionale della domanda di rogatoria all'estero. In questo secondo filone rientrano anche istituti come le squadre investigative comuni ed organi come *Eurojust*.

Nell'ambito della Conv. EU 2000 si rinviene una previsione dedicata all'istituzione di squadre investigative comuni (art. 13), disciplina poi replicata in una apposita decisione quadro (decisione quadro del 13 giugno 2002 sulle squadre comuni investigative, 2002/465/JHA), varata per via del ritardo nell'entrata in vigore della Convenzione [51]. Sono squadre costituite su accordo delle autorità di due o più stati membri per svolgere indagini di carattere transnazionale [52]. La presenza nella squadra di figure provenienti dagli Stati aderenti consente di operare (*id est*, compiere atti investigativi) sul territorio di ciascuno di tali Stati membri, seguendo ogni volta le regole vigenti in quello Stato (secondo il principio del *locus regit actum*). La costituzione della squadra permette così di evitare il ricorso alle complicate procedure di assistenza giudiziaria, in favore di una più agile ed efficace azione investigativa.

Nell'ambito di questa cornice, fra gli atti che la squadra investigativa comune può compiere rientrano anche le operazioni di intercettazione telefonica, le quali potranno così beneficiare del più agile meccanismo insito in questa forma di cooperazione.

La costituzione di una squadra investigativa comune dovrebbe dunque permettere di intercettare in diversi paesi senza doversi muovere nel più laborioso reticolo delle regole di mutua assistenza giudiziaria prima illustrate, assicurando allo stesso tempo la successiva spendita processuale dei risultati ottenuti con la captazione. Ma su quest'ultimo punto la cautela è d'obbligo, dovendosi tenere conto delle previsioni che circoscrivono l'utilizzazione delle informazioni ottenute, le quali, pur perseguendo l'obiettivo di assicurarne un ampio uso processuale, nondimeno configurano significative eccezioni. Ai sensi dell'art. 13, § 10 Conv. EU 2000 (e dell'equivalente art. 1, § 10 della decisione quadro), le informazioni legalmente ottenute da una squadra investigativa comune e non altrimenti disponibili per le autorità competenti dello Stato membro interessato potranno essere impiegate:

a) per i fini previsti all'atto della costituzione della squadra;

b) per l'individuazione, l'indagine e il perseguimento di altri reati, ma previo accordo dello Stato membro in cui si sono raccolte le informazioni (che potrà negare il consenso solo qualora l'impiego delle informazioni pregiudicasse indagini penali in corso o – deroga significativa – qualora quest'ultimo potesse rifiutare l'assistenza giudiziaria ai fini di tale uso);

c) per scongiurare una minaccia immediata e grave alla sicurezza pubblica (fermi restando i limiti predetti se dovesse scaturirne un'indagine penale);

d) per altri ulteriori scopi, entro i limiti convenuti dagli Stati membri che hanno costituito la squadra.

[51] Ai sensi dell'art. 5 della decisione quadro si prevede infatti che ne cessi il vigore quando la Conv. EU 2000 sia entrata in vigore per tutti gli Stati membri.

[52] Per un'approfondita analisi teorica e pratica sulle squadre investigative comuni, v. C. RIJKEN, *Joint Investigation Teams: principles, practice and problems. Lessons learnt from the first effort to establish a JIT*, in 2 *Utrecht Law Review* (2006), p. 99 ss. In generale, v. M. PLACHTA, *Joint Investigation Teams. A New Form of International Cooperation in Criminal Matters*, in 13 *European Journal of Crime, Criminal Law and Criminal Justice* (2005), p. 284 ss.; C. GUALTIERI, *Joint Investigation Teams*, in 8 *Era Forum* (2007), p. 233 ss. Nella dottrina italiana, v. A. MANGIARACINA, *Verso nuove forme di cooperazione: le squadre investigative comuni*, in *Cass. pen.*, 2004, p. 2189 ss.

Le stesse difficoltà di compatibilità fra sistemi normativi lasciano aperti non pochi problemi sull'uso dibattimentale delle intercettazioni telefoniche. Per fare un esempio concreto delle difficoltà che sorgono, si pensi alla squadra investigativa comune "Drug II", costituita su impulso del Regno Unito con la partecipazione dei Paesi Bassi. A quanto si sa, le intercettazioni svolte nel Regno Unito non sarebbero state utilizzate nei processi olandesi a causa della divergenza fra le discipline nazionali (e, in particolare, della possibilità da parte della polizia inglese di disporre le intercettazioni in assenza di un'autorizzazione giudiziaria e del divieto britannico di utilizzare nel processo i risultati delle captazioni).

Le squadre investigative comuni non sono l'unico strumento che consente di superare i meccanismi – e le complicazioni e lentezze – della mutua assistenza giudiziaria. Un risultato simile potrebbe essere raggiunto anche da *Eurojust*, organo di coordinamento investigativo volto a favorire la cooperazione giudiziaria nelle indagini transfrontaliere e contro la criminalità transazionale, composto da membri designati dai singoli Stati membri (membri nazionali) [53].

Con la riforma del 2008, si sono riscritti, rafforzandoli, i poteri dei membri nazionali dell'organo [54]. Oltre ad una quota di "poteri ordinari", consistenti nel "ricevere, trasmettere, agevolare, seguire e fornire le informazioni supplementari relative all'esecuzione delle richieste e delle decisioni in materia di cooperazione giudiziaria" (art. 9-*ter*), la decisione prevede che i membri siano dotati di poteri da esercitare d'intesa con le autorità nazionali competenti (art. 9-*quater*) o in casi d'urgenza (art. 9-*quinquies*). In queste ultime ipotesi, il membro nazionale può eseguire nel proprio Stato le domande di cooperazione giudiziaria (artt. 9-*quater*, lett. *b* e e 9-*quinquies*, lett. *b*). D'intesa con l'autorità nazionale competente, il membro nazionale potrà poi anche "emettere (o completare) richieste di cooperazione giudiziaria", ma soprattutto "disporre nel proprio Stato misure investigative ritenute necessarie" da Eurojust (art. 9-*quinquies*, lett. *a*) e *c*).

Il conferimento dei più penetranti poteri previsti dagli art. 9-*quater* e 9-*quinquies* può essere derogato qualora sia contrario: *a*) alle norme costituzionali; ovvero *b*) agli aspetti fondamentali del sistema giudiziario penale, questi ultimi declinati secondo tre precise angolazioni (ossia, in relazione alla suddivisione di poteri tra polizia, magistrati del pubblico ministero e giudici, alla divisione funzionale dei compiti tra procure, alla struttura federale dello Stato). Anche in quest'eventualità, tuttavia, il membro nazionale, in qualità di autorità nazionale, dovrebbe essere quantomeno dotato del potere di "presentare all'autorità competente una proposta finalizzata all'esercizio dei poteri di cui agli articoli 9-*quater* e 9-*quinquies*".

Molto dipenderà da come la decisione sarà attuata nei vari Stati membri, ma sulla carta Eurojust dovrebbe avere la possibilità, a determinate condizioni, di presentare, tramite il suo membro nazionale, una richiesta ad un giudice nazionale (o all'autorità equivalente) per ottenere l'autorizzazione ad intercettare.

Come per le squadre investigative comuni, l'azione di *Eurojust* potrebbe consentire di rendere più snella la cooperazione giudiziaria in relazione all'effettuazione di intercettazioni, ora agevolando l'esecuzione delle richieste di cooperazione, ora persino superando le regole di assistenza giudiziaria, ma sempre salvaguardando il rispetto delle prescrizioni poste a livel-

[53] Sul punto, v. G. DE AMICIS, *La costruzione di Eurojust nell'ambito del "Terzo pilastro" dell'Unione europea*, in *Cass. pen.*, 2001, p. 1964 ss. e, di chi scrive, *Eurojust*: il braccio giudiziario dell'Unione, in M.G. COPPETTA (a cura di), *Profili del processo penale nella Costituzione europea*, Torino, 2005, p. 149 ss.

[54] Decisione del 16 dicembre 2008 (2009/426/JHA). Sulla riforma del 2008, v. G. DE AMICIS-L. SURANO, *Il rafforzamento dei poteri di Eurojust a seguito della nuova decisione 2009/426/GAI*, in *Cass. pen.*, 2009, p. 4453 ss.; F. SPIEZIA, *Il coordinamento giudiziario sovranazionale: problemi e prospettive alla luce della nuova decisione 2009/426/GAI che rafforza i poteri di Eurojust*, in *Cass. pen*., 2010, p. 1990 (partic. p. 2000 ss.).

lo nazionale per intercettare. Anche qui, peraltro, rimane aperto il problema dell'utilizzabilità delle intercettazioni compiute: il fatto che l'intercettazione sia stata legittimamente disposta nell'ambito di uno Stato non esclude che essa possa essere considerata inammissibile in un diverso Stato.

7. *Segue*: 3) mutuo riconoscimento probatorio e intercettazioni

L'impegno dell'Unione nel settore delle intercettazioni è stato dunque quello di accrescere l'efficienza nella mutua assistenza giudiziaria, senza però perdere di vista le garanzie. Anzi, l'impressione è che il legislatore europeo, quando efficienza e garanzie fossero irrimediabilmente in collisione, sia stato tendenzialmente disposto a privilegiare le seconde.

Questa chiave di lettura potrebbe forse spiegare il difficile rapporto fra il mutuo riconoscimento e le intercettazioni.

La logica del mutuo riconoscimento è ormai l'ideologia imperante dell'Unione anche nell'ambito dello spazio di libertà, sicurezza e giustizia [55], come prima lo era stata nell'ambito del mercato interno [56]. Negli ultimi anni essa ha iniziato a contaminare anche la materia delle prove. L'esempio per eccellenza è costituito dal mandato europeo di ricerca della prova (MER), adottato con decisione quadro del 18 dicembre 2008 (2008/978/JHA) [57]. Modellato sul mandato di arresto europeo, il mandato probatorio prevede, in essenza, che la decisione di un'autorità statale di raccogliere una prova all'estero sia trasmessa all'autorità di un altro Stato membro per l'esecuzione; l'autorità straniera richiesta può rifiutarne l'esecuzione solo per i motivi espressamente elencati nell'art. 13 della decisione quadro e dispone di ridotti termini temporali per raccogliere la prova. Dall'ambito di applicazione dello strumento restano però espressamente escluse, come si è anticipato, tutte le operazioni di acquisizione di informazioni in tempo reale, fra cui l'intercettazione di comunicazioni (art. 4, § 2, lett. *c*) [58]. Una scelta replicata nella recentissima proposta di direttiva per un "ordine europeo di indagine" (OEI) [59], nuovo strumento sempre ispirato al principio del mutuo riconoscimento e finalizzato a far

[55] Nella vastissima bibliografia sul mutuo riconoscimento all'interno dell'area di libertà, sicurezza è giustizia, v., senza pretesa di completezza, S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo*, in T. RAFARACI (a cura di), *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, Milano, 2007, p. 691 ss.; G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in T. RAFARACI (a cura di), *L'area di libertà sicurezza e giustizia*, cit., p. 691 ss.; O. MAZZA, *Il principio del mutuo riconoscimento nella giustizia penale, la mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in *Riv. dir. proc.*, 2009, p. 393 ss.; S. GLESS, *Mutual recognition, judicial inquiries, due process and fundamental rights*, in J.A.E. VERVAELE, *European evidence warrant: transnational judicial inquiries in the EU*, Intersentia, Antwerpen-Oxford, 2005, p. 121 ss.

[56] La convergenza fra l'area del mercato unico e quella di libertà e sicurezza e giustizia, con la contaminazione di quest'ultima da parte dei principi che caratterizzavano la prima, è illustrata in particolare da A. KLIP, *European Criminal Law*, Intersentia, Antwerp-Oxford-Portland, 2009, p. 15 ss,

[57] Sul mandato di ricerca della prova, v. G. DE AMICIS, *Il mandato europeo di ricerca della prova: un'introduzione*, in *Cass. pen.*, 2008, p. 3033; R. BELFIORE, *Il mandato europeo di ricerca delle prove*, in *Cass. pen.*, 2008, p. 3894 ss; EAD., *Movement of Evidence in the EU: The Present Scenario and Possible Future Developments*, in 17 *European Journal of Crime, Criminal Law and Criminal Justice* (2009), p. 1 ss. V. anche J.A.E. VERVAELE, *Il progetto di decisione quadro sul mandato di ricerca della prova*, in G. ILLUMINATI (a cura di), *Prova penale e Unione europea*, Bologna, 2009, p. 153 ss.

[58] E la stessa acquisizione di tabulati (art. 4, § 2, lett. *e*).

[59] La proposta sull'OEI si può ora leggere anche nella *Gazzetta Ufficiale dell'Unione europea*, C 165, del 24 giugno 2010.

compiere in un altro Stato membro "uno o più specifici atti d'indagine"[60], da cui resta esclusa l'effettuazione di intercettazioni[61].

Non è dunque possibile – né dovrebbe esserlo nel prossimo futuro – che un provvedimento autorizzativo d'intercettazione emesso in un paese membro riceva riconoscimento ed esecuzione all'estero; si dovrà ancora procedere con le regole previste dalla Conv. EU 2000 o – per gli Stati che non abbiano ratificato quella Convenzione – con le tradizionali regole fissate dalla Conv. 1959 (come integrate dalla Convenzione di applicazione dell'accordo di Schengen del 1990). L'esclusione delle intercettazioni dal campo applicativo del MER lascia intatta la sovranità nazionale nel decidere se, quando e come intercettare. La possibilità di incidere sulla libertà di comunicare dei cittadini rimane ancorata alle regole di ciascuno Stato. La presa d'atto della marcata distanza fra le varie discipline nazionali, combinata con la peculiare insidiosità ed invasività di questo mezzo di ricerca della prova, hanno condotto all'emarginazione delle intercettazioni dall'ambito del mutuo riconoscimento. Eppure non in via assoluta.

Si deve tenere in considerazione che, se le operazioni di raccolta di informazioni in tempo reale restano fuori dal mandato di ricerca, all'interno di quest'ultimo ricade invece la trasmissione dei risultati di intercettazioni già autonomamente ottenuti da parte di uno Stato (v. art. 4, § 4 della decisione quadro)[62].

Non è dunque possibile che uno Stato emetta un mandato perché siano condotte all'estero forme di sorveglianza telefonica, ma è consentito invece che si richiedano gli esiti di intercettazioni compiute da un'autorità straniera, le quali sono dunque trattate alla stregua di una prova precostituita. Per dirla con uno slogan: no al mutuo riconoscimento delle decisioni d'intercettazione, sì al mutuo riconoscimento dei risultati delle intercettazioni.

Da un lato, dunque, la scelta di ledere la riservatezza delle comunicazioni tramite un atto intercettivo rimane nella piena disponibilità dei singoli Stati, affidata sovranamente alle regole nazionali. Dall'altra, invece, si comincia a prefigurare lo scenario di una circolazione dei risultati delle intercettazioni compiute in ciascun paese. È una tendenza di cui peraltro si possono cogliere già i segni nella prassi giurisprudenziale. Diverse decisioni della Corte di cassazione italiana hanno ritenuto legittima la ricezione dei risultati delle intercettazioni estere[63],

[60] Per un primo commento alla proposta, v. L. BACHMAIER WINTER, *European investigation order for obtaining evidence in the criminal proceedings. Study of the proposal for a European directive*, in *Zeitschrift fuer Internationale Strafrechtsdogmatik*, 2010, p. 580 ss. e G. DE AMICIS, *L'ordine europeo di indagine penale*, in *http://www.europeanrights.eu/index.php?funzione=S&op=5&id=440*.

[61] Ai sensi dell'art. 3 della proposta, l'OEI non comprende "l'intercettazione e la trasmissione immediata di telecomunicazioni ai sensi dell'articolo 18, paragrafo 1, lett. *a*) della convenzione" (art. 3 lett. *b*) e "l'intercettazione di telecomunicazioni ai sensi dell'articolo 18, paragrafo 1, lettera *b*), laddove riguardino le situazioni di cui all'articolo 18, paragrafo 2, lettere a) e c), e l'articolo 20 di tale convenzione" (art. 3, lett. *c*). Va segnalato, invece, che nel *Libro verde sulla ricerca delle prove in materia penale tra Stati membri e sulla garanzia della loro ammissibilità* (COM/2009/624), la Commissione proponeva uno strumento di acquisizione delle prove fondato sul mutuo riconoscimento, che comprendesse anche le "informazioni acquisite in tempo reale, ad esempio l'intercettazione di comunicazioni" (p. 5).

[62] Lo stesso vale per i tabulati che siano già in possesso dell'autorità straniera.

[63] Si veda, ad esempio, Cass., sez. I, 6 luglio 1998, Bonelli, in *CED*, rv. 211301 ("Possono essere utilizzate in un procedimento italiano le intercettazioni disposte in procedimenti penali svoltisi all'estero, acquisite per rogatoria dall'autorità giudiziaria italiana, purché siano rispettate le condizioni eventualmente poste dall'autorità estera all'utilizzabilità degli atti richiesti e sempre che le intercettazioni stesse siano avvenute nel rispetto delle regole formali e sostanziali che le disciplinano e altresì nel rispetto dei fondamentali principi di garanzia, aventi rilievo di ordine costituzionale, propri del nostro ordinamento (fattispecie in tema di intercettazioni disposte dall'autorità giudiziaria tedesca)"); Cass., sez. V, 26 novembre 1996, Lavorato, in *CED*, rv. 207867 ("In tema di utilizzazione dei risultati delle intercettazioni telefoniche in altri procedimenti, possono essere utilizzate in un procedimento italiano le intercettazioni telefoniche disposte in procedimenti penali esteri, acquisite per rogatoria

anche ove la trasmissione fosse avvenuta al di fuori delle formalità rogatoriali[64]. Orientamenti equivalenti si riscontrano anche in Francia[65] e nel Regno Unito[66].

La disciplina del mandato europeo di ricerca della prova fa emergere la nuova cifra dell'approccio dell'Unione in tema di prove penali: la libera circolazione in Europa della prova (raccolta secondo le regole della *lex loci*), senza preventive armonizzazioni. Per un verso, non si interferisce con le scelte nazionali sul se, quando – sulla base di quali presupposti – e come intercettare. Per l'altro, si legittima che le conversazioni captate nazionalmente possano essere trasmesse alle autorità di un altro Stato membro con l'obiettivo di essere utilizzate processualmente. In questo modo si crea tuttavia una scissione tra i momenti della raccolta/formazione della prova e quello, successivo, della spendita processuale. Due rischi opposti si intravedono così all'orizzonte: da un lato, quello di un rigetto in fase processuale dell'intercettazione effettuata all'estero[67]; dall'altro, quello di un'acritica ricezione all'interno del contesto processuale dei risultati di intercettazioni disposte all'estero, come, si è visto, sta in parte già accadendo in sede giurisprudenziale[68].

La critica a questa tendenza europea favorevole alla libera circolazione della prova raccolta in uno Stato membro – in cui rientrano anche i risultati delle intercettazioni – potrebbe essere sviluppata anche sotto altro profilo: la separazione forzata fra acquisizione/formazione della prova e suo uso dibattimentale si fonda su un isolamento del dato probatorio, il cui valo-

dall'autorità giudiziaria italiana, purché siano rispettate le condizioni eventualmente poste dall'autorità estera all'utilizzabilità degli atti richiesti, come previsto dall'art. 729 cod. proc. pen.").

[64] Così Cass., sez. I, 31 ottobre 2002, Moio, in *CED*, rv. 222984: "In tema di utilizzabilità di atti assunti per rogatoria, le intercettazioni telefoniche ritualmente compiute da un'Autorità di Polizia straniera e da questa trasmesse di propria iniziativa, ai sensi dell'art. 3, comma 1, della Convenzione Europea di assistenza giudiziaria firmata a Strasburgo il 20 aprile 1959, ratificata con l. 23 febbraio 1961, n. 215, e dell'art. 46 dell'Accordo di Schengen, ratificato con l. 30 settembre 1993, n. 388, senza l'apposizione di 'condizioni all'utilizzabilità, alle Autorità italiane interessate alle informazioni, rilevanti ai fini dell'assistenza per la repressione di reati commessi sul loro territorio, possono essere validamente acquisite al fascicolo del pubblico ministero, ai sensi dell'art. 78, comma 2, disp. att. c.p.p., trattandosi di atti non ripetibili compiuti dalla polizia straniera". Sul punto, v. anche E. APRILE, *Nuovi strumenti e tecniche investigative nell'ambito dell'U.E.*, cit., p. 446.

[65] V., ad esempio, nel senso dell'ammissibilità di "*un rapport relatant diverses investigations effectuées en Espagne, dont des écoutes telephoniques autorisées par les tribunaux de Gava et Malaga*", trasmesso dalle autorità di polizia spagnole ai sensi dell'art. 39 della Convenzione di applicazione dell'accordo di Schengen del 1990, Cour de cassation, chambre criminelle, Audience publique du 9 juillet 2003, Bull. Crim. 2003, n. 134 (n. de pourvoi: 03-82.163).

[66] Nel caso *R. v P* deciso dalla House of Lords l'11 dicembre 2000, in 2 *All England Reports* (2001), p. 58, sono state ritenute ammissibili come prova le intercettazioni effettuate in una giurisdizione straniera. Per l'utilizzabilità di tabulati ricevuti dalla polizia straniera (anche alla luce delle regole sull'*hearsay evidence*) v., R. v. O'Connor, Court of Appeal (Criminal Division), 22 giugno 2010, in *England and Wales Court of Appeal Criminal Division*, 2010, p. 2287.

[67] Analizzando questa disciplina da un punto di vista italiano, si sono espresse perplessità sulla sua reale efficacia alla luce delle previsioni del codice di rito italiano. In quest'ultimo, "la circolazione tra procedimenti degli esiti di intercettazioni di comunicazioni, esulando dal sistema di cui agli artt. 78 disp. att. c.p.p. e 238 c.p.p., è oggetto di un'apposita disciplina contenuta nell'art. 270, comma 1, c.p.p. in base al quale i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza. L'art. 270 c.p.p. riduce quindi la permeabilità di un procedimento ai risultati di intercettazioni ad esso estranee; il che difficilmente si concilia con la deroga di cui alla decisione quadro in esame". Se ne è tratta la conclusione che, salve diverse scelte in sede di attuazione, "il già ristretto scopo del mandato d'arresto europeo di ricerca delle prove risulterebbe particolarmente circoscritto nell'ordinamento italiano, e ciò soprattutto rispetto alla deroga apparentemente comprensiva a favore della prova pre-acquisita" (R. BELFIORE, *Il mandato europeo di ricerca*, cit., p. 3900 s.).

[68] V. *supra*, note 63, 65 e 66.

re viene individuato a prescindere dalle modalità di raccolta. All'opposto, va ricordato che le regole che presiedono alla creazione della prova incidono sulla sua forza probatoria e sulla sua capacità persuasiva.

8. Scenari

Gli scenari descritti sollecitano alcune riflessioni. Sul fronte della libertà, l'impegno dell'Unione è stato prevalentemente quello di evitare surrettizie elusioni delle tutele predisposte da uno Stato all'interno del proprio territorio. Uno sforzo apprezzabile, perché permettere che la restrizione delle libertà entro i confini di uno Stato possa avvenire sulla base di regole estere comporterebbe un generalizzato abbassamento della soglia di protezione offerta ai cittadini. Ripristinare la sovranità è dunque il primo passo per tutelare la garanzia di comunicare riservatamente.

In un'ottica di cooperazione europea rimane però aperto il tema della profonda divergenza fra le discipline nazionali, che può minare l'efficacia della collaborazione investigativa. Il problema è acuito dalla tendenza a permettere la circolazione dei risultati delle intercettazioni raccolte in uno Stato. Diventa così sempre più evidente la necessità di procedere ad uno sforzo di armonizzazione, quantomeno in termini di regole minime, in materia di intercettazioni telefoniche. Alla luce della capacità dell'intercettazione di muoversi tanto facilmente fra i confini statali, la soluzione teorica migliore sarebbe quella di armonizzare i presupposti di ricorso allo strumento e di stabilire norme minime comuni di registrazione e trascrizione delle conversazioni: diverrebbe così più agevole anche il trasferimento dei risultati delle intercettazioni.

Da un punto di vista prettamente italiano, invece, non si può che caldeggiare un maggiore rispetto da parte del legislatore delle soluzioni elaborate in sede europea. In particolare, sarebbe opportuno non procrastinare oltre l'attuazione della Conv. EU 2000. In un dibattito politico attuale ossessionato dall'esigenza di tutelare maggiormente la libertà di segretezza delle comunicazioni, non si vede perché si debba attendere ancora, dopo più di un decennio, per dare esecuzione ad un atto europeo che saprebbe garantire le istanze di libertà molto più delle odierne prassi giurisprudenziali. Sebbene circoscritto alla sola cooperazione giudiziaria, sarebbe un segnale che l'obiettivo veramente perseguito dal legislatore è quello di tutelare la libertà di comunicare riservatamente di tutti i cittadini.

CAPITOLO 5

Intercettazioni e terrorismo: un approccio comparato tra legislazioni emergenziali e leggi di riforma

di *Eleonora Colombo*

SOMMARIO: 1. Introduzione alle problematiche del tema e all'obiettivo del contributo. – 2. Le leggi e le riforme della disciplina delle intercettazioni per la prevenzione e repressione del fenomeno terroristico: le esperienze di Italia, Francia e Germania. – 2.1. Italia. – 2.2. Francia. – 2.3 Germania. – 3. La legislazione dell'emergenza per la lotta al terrorismo: l'ordinamento USA, United Kingdom e Federazione russa. – 3.1 USA. – 3.2. United Kingdom. – 3.3. Federazione russa. – 4. Alcuni dati statistici rilevanti. – 5. Conclusioni.

1. Introduzione alle problematiche del tema e all'obiettivo del contributo

Il tema del presente contributo, considerata la vastità di contenuto, richiede di affrontare una serie di problematiche legate in primo luogo alla ricchezza semantica delle due parole chiave: terrorismo ed intercettazione. Sono note le questioni giuridiche affrontate in ambito scientifico, alla ricerca di una definizione comune e condivisa del termine e del fenomeno di terrorismo[1]. L'avvento delle nuove tecnologie ha inoltre generato ulteriori diatribe, specie legate ai mezzi e modalità di controllo dei dati che circolano. Da queste considerazioni preliminari sorge il quesito riguardo quando e come vi sia una effettiva forma di intercettazione di flussi informativi[2].

L'aumento del numero delle intercettazioni autorizzate ed effettuate negli ordinamenti giuridici europei ed europei, siano essi sistemi di *civil law* o di *common law*, pone un interrogativo riguardante i presupposti autorizzativi e legittimanti le richieste di tale mezzo d'indagine[3] dalle diverse normative nazionali, nonché, a livello pratico-applicativo, porta a chiedersi se siano un mezzo essenziale e determinante nella definizione del procedimento penale.

[1] Non è questa la sede per ricostruire ed analizzare le interessanti diatribe tra gli studiosi proprio per dare una definizione circoscritta e condivisa di terrorismo, come non è nemmeno questa la sede per valutare le difficoltà incontrate dagli interpreti all'atto dell'applicazione della norma e dell'irrogazione di una sanzione. Tuttavia si rinvia ad una vasta letteratura scientifica sul tema, preso coscienza che a tutt'oggi non è stata raggiunta una nozione certa di terrorismo ovvero una individuazione univoca delle qualità e degli elementi che un'azione deve avere per essere ricompresa in tale concetto. Si invita, per l'approfondimento sul tema, alla lettura, tra gli altri, di: R. ARNOLD, *The ICC as a new instrument for repressing terrorism*, Ardsley, N.Y., 2004; A. ASTROLOGO, *Prime riflessioni sulla definizione di reato transnazionale nella L. n. 146/2006*, in *Cass. pen.*, 2007, 4; R. BARBERINI *L'approccio giuridico al fenomeno del terrorismo*, in *Gnosis*, 2004; L. BAUCCIO, *L'accertamento del fatto di reato di terrorismo internazionale*, Milano, 2008.

[2] Non saranno qui ricostruire le questioni giuridiche di assoluto fascino accademico e di indubbio risvolto pratico che attengono la comprensione di cose sia e cosa non sia intercettazione.

[3] Così chiamato tecnicamente per non toccare un altro argomento critico circa le diverse categorizzazioni giuridiche proprie di ogni ordinamento nazionale.

Inoltre i costi (già ragguardevoli) delle intercettazioni sostenuti dallo Stato dovrebbero portare a scelte e limitazioni ai soli casi in cui vi sia effettiva necessità, evitando abusi e *mala gestio* del denaro pubblico.

Se i provvedimenti autorizzativi delle intercettazioni (nelle diverse forme) sono di fatto aumentati in modo quasi omogeneo per ogni Paese, la stessa omogeneità non si riscontra nelle disposizioni legislative vigenti nei singoli ordinamenti giuridici.

Quanto al solo reato di terrorismo, in ogni ordinamento giuridico, riconoscendo la pericolosità di tale forma criminosa e nell'intento di portare ad una condizione di sicurezza pubblica, sono date maggiori aperture rispetto alle norme generali sulle intercettazioni.

L'emergenza terrorismo ha portato ogni Stato ad intervenire anche a livello legislativo per prevenire e reprimere in modo rapido e concreto le attività terroristiche già consumate ovvero in preparazione. Ogni ordinamento giuridico ha, però, effettuato delle scelte differenti nelle forme e nei modi d'intervento. Parte della Dottrina distingue tra Stati in cui è stata introdotta una vera e propria normativa emergenziale e Stati in cui, invece, sono stati adottati soltanto degli accorgimenti garantistici più specifici, mediante riforme mirate. Segnatamente, a titolo esemplificativo di queste categorie e quali Stati fortemente interessati dal fenomeno terroristico, Italia, Francia e Germania si sono determinati per una scelta riformistica controllata; gli USA, l'Inghilterra e la Federazione russa hanno introdotto, invece, un microsistema normativo emergenziale.

La *ratio* sottesa alle differenti scelte fatte dai legislatori nazionali non è così ovvia e palese.

Certamente gli Stati Uniti d'America sono stati per primi colpiti dall'attacco diretto di AlQaida l'11 settembre 2001 ed è stato dunque d'obbligo dare una risposta anche legislativa forte. Questa data, rimasta nella storia, ha sviluppato un maggiore interesse e preoccupazione per il fenomeno terroristico, con un intento di protezione da futuri attacchi diretti a sovvertire l'ordine politico e sociale dello Stato colpito. Anche la città di Londra è stata teatro di un fenomeno terroristico perpetratosi proprio nell'orario di punto nella metropolitana cittadina: si giustifica e comprende, dunque, la scelta di introdurre nell'ordinamento una legislazione dell'emergenza. Quanto alla Federazione russa, il Governo ha dovuto e deve affrontare i rischi e i pericoli di terrorismi interni di forze centripete locali, nonché di forze esterne ma adiacenti ai confini dello Stato, con particolare riferimento alle forze terroristiche georgiane. Anche in questa è risibile la necessità di disposizioni emergenziali.

Quanto a Francia, Italia e Germania, essendo tra le maggiori potenze d'Europa e del mondo, sebbene non siano state direttamente colpite da fenomeni terroristici di entità tali da far temere nell'immediato per la sicurezza nazionale[4], sono state soltanto apportate le riforme ritenute necessarie per una maggiore protezione dell'incolumità pubblica rispetto ad un panorama internazionale di generale allarmismo.

Il regime speciale introdotto negli Stati Uniti d'America, UK e Federazione russa[5] era allora giustificato da situazioni socio-politiche di particolare tensione, ma lo stato emergenziale vero e proprio è sempre e permanentemente presente, tale da richiedere la cristallizzazione di

[4] Ricordiamo, però, tra i vari episodi presunti terroristici, la bomba fatta scoppiare nei pressi della caserma dei Carabinieri a Milano, in via Moscova, pochi mesi or sono, per cui il Tribunale di Milano si è pronunciato nei termini del riconoscimento di un coinvolgimento dell'autore del fatto con organizzazioni terroristiche e perciò condannato per tentativo di reato con finalità terroristiche appunto. Non si riporta altro di tale provvedimento se non quanto riportato e reso noto dai media, sebbene non sarebbe di poco interesse una lettura e un'analisi delle motivazioni addotte dall'organo giudicante anche per quanto attiene alla cornice definitoria delle attività con finalità terroristiche.

[5] Come già detto si menzionano solo questi Stati a titolo rappresentativo ed esemplificativo poiché meglio visualizzano e rappresentano una vera e propria legislazione dell'emergenza.

istituti e regole per loro natura provvisorie? Sussiste ancora la necessità di applicare questi regimi restrittivi di libertà in favore del crescente bisogno di sicurezza, sebbene proclamati come provvisori ai soli fini di uno scorcio temporale emergenziale?

Ed ancora, ci si chiede se la cooperazione per la lotta ad un crimine transnazionale quale il terrorismo possa trovare efficace attuazione tra Stati in cui il riconoscimento dei diritti individuali dinnanzi ad uno stato di tensione ed insicurezza diffusa presenta un grado differente di protezione.

La ricostruzione delle normative dei menzionati Stati scelti potrà portare ad alcune considerazioni conclusive, finalizzate a dare una risposta agli interrogativi qui enucleati.

2. Le leggi e le riforme della disciplina delle intercettazioni per la prevenzione e repressione del fenomeno terroristico: le esperienze di Italia, Francia e Germania [6]

Dall'analisi della normativa antiterroristica, di conseguenza anche relativa alle intercettazioni, si osserva ch i diversi ordinamenti giuridici hanno optato per politiche legislative differenti: alcuni hanno prodotto un pacchetto dell'emergenza, altri si sono limitati ad introdurre delle modifiche sulla base delle sopravvenute esigenze di giustizia. In quest'ultima categoria rientrano, tra gli altri, l'Italia, la Germania e la Francia. Suddetti Stati non sono gli unici ad aver scelto questa politica legislativa poiché lo stesso vale a dirsi, per esempio, per la Spagna, nonostante la società sia da lungo tempo colpita da forze terroristiche interne, oltre che da episodi di attivismo terroristico provenienti dall'esterno [7].

In Italia e in Germania le rispettive carte costituzionali garantiscono il diritto alla segretezza delle comunicazioni e segnatamente l'art. 14 Costituzione italiana [8], il paragrafo 10 del Bundesgesetz [9].

In questo quadro garantistico, unitamente alla protezione offerta dall'art. 8 e 10 CEDU e all'articolo 17 del Patto internazionale per i Diritti civili e politici, nonché agli articoli 7 e 8 della Carta di Nizza, deve essere analizzata la normativa nazionale sulle intercettazioni e le deroghe previste al normale regime, nell'ipotesi in cui si proceda o si voglia prevenire il fenomeno terroristico.

[6] Preliminarmente, come dato relativo alle fonti utilizzate, si menziona il Dossier della Camera dei Deputati MLC160022 in materia di comparazione e leggi sulle intercettazioni consultabile sul sito della stessa Camera parlamentare, così come consultato in data 13 maggio 2010.

[7] Alcuni politologi riuniti in un seminario di studi svoltosi a Milano presso Palazzo Clerici dall'ISPI hanno paventato l'ipotesi secondo cui la scelta di questo regime solo riformatore della Spagna è dettato dalla presenza già costante di strumenti adatti, prima utilizzati per le sole forze terroristiche interne.

[8] È noto il testo del menzionato articolo con le correlate garanzie della riserva di legge e di giurisdizione i cui ai commi 1 e 2.

[9] Ai sensi di tale articolo il segreto della corrispondenza e così pure il segreto postale e delle telecomunicazioni sono inviolabili: vige il principio di riserva di legge quanto alle possibili previsioni limitative di tale diritto. Lo stesso articolo prevede che nel caso in cui la limitazione sia finalizzata alla difesa dell'ordinamento costituzionale liberale e democratico o dell'esistenza o della sicurezza della Federazione o di un Land, la legge stessa può stabilire che la misura restrittiva non venga comunicata all'interessato e che il ricorso giurisdizionale sia sostituito da un esame da parte di organi parlamentare istituiti all'uopo.

2.1. Italia

L'ordinamento giuridico italiano è particolarmente interessato alla materia delle intercettazioni, tanto che le disposizioni a riguardo sono state oggetto di plurimi dibattiti ed interventi riformatori e tutt'ora al Parlamento si sta discutendo la c.d. "legge bavaglio" che mette a confronto i punti di vista delle forze politiche opposte e che ha portato, altresì, ad un intervento del Comitato per i Diritti Umani delle Nazioni Unite, il quale ha censurato in alcuni aspetti il ddl in esame.

Le intercettazioni, quale genere di prova a sorpresa, irripetibili e sottratte, dunque, alla garanzia del contraddittorio richiedono una particolare cautela. Nella prassi giudiziaria italiana, *ex adverso*, si riscontra un generale *favor* ed attualmente sono pochi i casi in cui non si riscontri una interpretazione giurisprudenziale ampia della disciplina delle intercettazioni, riducendo al minimo la portata dei limiti e contenendo i casi di inutilizzabilità.

Le disposizioni che regolano questo mezzo di ricerca della prova si trovano negli artt. 266 e ss. c.p.p.

Le normative speciali hanno previsto fattori di espansione dell'ambito di applicazione di questo istituto per alcune categorie di reato e segnatamente per le investigazioni di criminalità organizzata e di terrorismo. Premesso ed indicato ciò, si rinvia al contributo specifico di chi si occupa del rapporto tra intercettazioni e criminalità organizzata nell'ordinamento giuridico italiano.

Preme qui precisare che per tali fattispecie criminose bastano sufficienti indizi di reato per ottenere l'autorizzazione alle intercettazioni e basta che queste captazioni siano necessarie per lo svolgimento delle indagini, senza che siano determinanti per la loro prosecuzione.

Gli oneri di motivazione dei provvedimenti autorizzativi non sono molto gravosi e, sul punto, la giurisprudenza di Legittimità tende a consentire spesso una motivazione *per relationem* con riferimento, da parte del PM, all'annotazione di PG, e da parte del GIP alla richiesta del PM.

Un'interpretazione ormai costante della Corte di Cassazione, legata al costante aumento della commissione di crimini transnazionali, statuisce che le intercettazioni legittimamente effettuate in Italia, conformemente alla legge nazionale, sono utilizzabili anche quando l'altro interlocutore che conversa con l'utenza italiana sia straniero o comunque ubicato in territorio estero.

Come verrà meglio precisato in altro contributo scientifico [10], le intercettazioni in materia di criminalità organizzata e di terrorismo hanno, inoltre, dei termini di durata più ampi rispetto alle regole generalmente applicabili.

2.2. Francia

Il quadro normativo francese in materia di intercettazioni è definito, principalmente, entro i parametri della legge 91-646 del 10 luglio 1991 che ne consente il ricorso solo alla pubblica autorità e per tutelare un interesse generale. La legge distingue due tipi di intercettazioni di telecomunicazioni: giudiziarie e amministrative o di sicurezza [11].

[10] Si rimanda al contributo di D. RASCHELLÀ in questo stesso volume.

[11] Per intercettazioni giudiziarie si intendono quelle operazioni di captazione delle comunicazioni – indipendentemente dal mezzo utilizzato ed interessato – che sono messe in atto a seguito di un provvedimento dell'autorità giurisdizionale che ne legittima le operazioni; per intercettazioni amministrative o di giustizia si inten-

L'art. 32 del Codice delle poste e delle comunicazioni elettroniche definisce il termine *telecomunicazione* nel seguente modo: "tutte le trasmissioni, emissioni o ricezioni di segni, segnali, scritti, immagini, suoni o informazioni di qualsiasi natura emessi attraverso filo, fibre ottiche, radioelettricità o altri sistemi elettromagnetici".

Le intercettazioni giudiziarie, in un primo momento, erano prive di una regolamentazione scritta, pur essendo abitualmente effettuate per plurimi procedimenti penali, con ciò portando a numerosi abusi per cui la Francia ha subito condanne dalla Corte europea dei diritti dell'uomo [12]. A seguito di questi provvedimenti contrari, il legislatore francese ha introdotto la citata legge del 1991, con la previsione di modifiche del codice di procedura penale, inserendo gli articoli da 100 a 100-7. In particolare, l'art. 100 definisce i parametri entro cui possono essere chieste e disposte le intercettazioni di comunicazione, attribuendo la competenza ed i poteri di controllo e garanzia al giudice istruttore. I presupposti richiesti sono assai stringenti e restrittivi. Le intercettazioni sono subordinate a dei minimi edittali previsti per i reati per cui si procede: la fattispecie non deve essere punita con una pena detentiva non inferiore ai due anni nel massimo e possono essere disposte solo se sono ritenute necessarie allo svolgimento delle indagini. La decisione in merito non ha valenza giurisdizionale ma solo garantistica e di mero controllo della sussistenza dei parametri richiesti *ex lege*, pertanto non richiede alcuna motivazione e non è prevista l'impugnazione. Il provvedimento deve però contenere delle informazioni precise e specifiche, rese in forma scritta, identificando l'oggetto dell'intercettazione, il reato per cui si procede e la durata delle operazioni (art. 100-1 c.p.p. francese). La durata non può superare quattro mesi e l'autorizzazione può essere rinnovata e prorogata, previo controllo del giudice sulla permanenza dei presupposti di cui all'art. 100 c.p.p. (art. 100-2 c.p.p. francese).

Dal punto di vista strettamente empirico-fattuale, le operazioni vengono svolte o dal giudice istruttore direttamente ovvero da un ufficiale di polizia giudiziaria ed entrambi possono valersi della collaborazione di operatori qualificati, obbligati a mantenere il segreto istruttorio ed il segreto sulla corrispondenza [13] (art. 100-3).

Le code de procedure penale dispone altresì che venga redatto un verbale ove indicare la data e l'ora di inizio e di fine delle operazioni di intercettazione e le registrazioni debbono poi essere debitamente sigillate e custodite (art. 100-4). La trascrizione delle comunicazioni intercettate è invece limitata alle sole parti utili per l'accertamento della verità ed è effettuata dal giudice istruttore ovvero dall'ufficiale di polizia giudiziaria su delega di quest'ultimo, con l'ausilio di un interprete nel caso in cui sino in lingua straniera. Il verbale delle trascrizioni confluisce poi nel fascicolo del dibattimento e le registrazioni vengono conservate fino a che sussiste una necessità di ordine pubblico, secondo le disposizioni dell'art. 100-5 c.p.p. La distruzione delle registrazioni avviene su ordine del Procuratore della Repubblica o del Procuratore generale ovvero *ex lege* al termine di prescrizione dell'azione penale (art. 100-6). L'art. 100-7 c.p.p. dispone dei limiti soggettivi alle intercettazioni al fine della protezione di più alti interessi e diritti fondamentali riconosciuti dall'ordinamento giuridico [14].

dono, invece, quelle operazioni captative compiute dagli organi di *intelligence*, al di fuori di un procedimento penale già formalmente iscritto ed instaurato.

[12] Nel caso Huvig c. Francia (1990) della Corte europea dei Diritti dell'Uomo, lo Stato è stato condannato in quanto la legge regolatrice non indicava con chiarezza in quali circostanze e sotto quali condizioni il potere pubblico fosse abilitato ad operare intercettazioni telefoniche, potenzialmente pericolose per il diritto al rispetto della vita privata

[13] Per segreto sulla corrispondenza si deve ritenere sia il contenuto che i dati esterni della comunicazione intercettata.

[14] Più in particolare, l'art. 100-7 c.p.p. francese esclude dalle intercettazioni i parlamentari senza previo av-

Con decreto 2006-1405 del 17 novembre 2006 è stata istituita, presso il Ministero di Giustizia francese, la Delegazione delle intercettazioni giudiziarie. Quest'organo, sottoposto al controllo del Segretario generale del Ministero e diretto da un magistrato, ha il compito di razionalizzare in ambito interministeriale le procedure, i mezzi tecnici, i costi, la raccolta dati e le autorizzazioni all'effettuazione di intercettazioni.

Le disposizioni di legge fin'ora ricordate attengono alle sole ipotesi di intercettazioni giudiziarie. Diversa regolamentazione è invece prevista per le cd. intercettazioni di sicurezza essendo, per natura, differenti già per il loro carattere amministrativo. Sono disposte dal Governo e vengono poi effettuate dalla polizia amministrativa. La legge di riferimento è la n. 646 del 1991, così come modificata dalla legge 2004-669. Hanno carattere preventivo ed eccezionale e pertanto sono sottoposte ad uno stretto controllo di legalità che ne assicuri la trasparenza nelle operazioni e l'efficacia dei risultati. Il campo si attiene in particolare alla prevenzione di attentati alla sicurezza nazionale, la salvaguardia del potenziale scientifico ed economico della Francia, la prevenzione del terrorismo, della criminalità organizzata, della ricostituzione dei gruppi sovversivi interni, sciolti in base ad una legge francese del 1936. Il carattere di eccezionalità richiede un rigoroso bilanciamento tra gli interessi della giustizia e della sicurezza e la garanzia dei diritti fondamentali previsti dalla Costituzione francese quali la segretezza della corrispondenza, la libertà individuale, il diritto alla riservatezza. L'autorizzazione scritta e motivata è formalizzata dal Ministro della Difesa o dal Ministro dell'Interno o dal Ministro delle Dogane territorialmente competente. Le intercettazioni di sicurezza possono essere disposte per un termine non superiore ai quattro mesi, con possibilità di proroga per un tempo equivalente nel caso di permanenza dei presupposti applicativi. Come per le intercettazioni giudiziarie, è redatto il verbale delle attività e vengono trascritte le sole registrazioni di comunicazioni necessarie e rilevanti. Quanto alle operazioni di distruzione, queste devono avvenire dopo dieci giorni dalle registrazioni e, comunque, all'intervenuta non indispensabilità delle trascrizioni.

La legge del 1991 [15], all'art. 13, al fine di garantire il carattere di eccezionalità delle intercettazioni di sicurezza, ha istituito la Commissione nazionale di controllo quale organo di controllo sugli eventuali abusi perpetrati dagli organi dell'esecutivo [16]. La Commissione presenta un rapporto annuale al Primo ministro avente ad oggetto le intercettazioni di sicurezza, dall'autorizzazione alle operazioni, alle procedure intermedie, alla registrazione, trascrizione e distruzione dei dati raccolti.

Non ritenendo sufficienti queste procedure di intercettazione per far fronte al crescente fenomeno terroristico, sia nel senso della prevenzione sia nel senso della repressione, il 23 novembre 2005 è stata votata una legge anti-terrorismo, proposta dal Ministro dell'Interno francese Nicolas Sarkozy e accolta a larga maggioranza dei deputati dell'Assemblea nazionale. Tale legge apre all'intercettazione ed al controllo sulle comunicazioni, autorizzando altresì

viso al Presidente dell'assemblea da parte del giudice istruttore; i magistrati per cui deve essere notiziato il presidente ovvero il procuratore generale della giurisdizione interessata; gli avvocati nel rispetto delle comunicazioni con i propri assistiti, per cui deve essere data pronta comunicazione al Presidente dell'Ordine di appartenenza.

[15] Il riferimento alla legge n. 669 del 1991 si deve intendere nella sua versione originale laddove non sono intervenute delle modifiche e con le successive modifiche laddove è stata riformata nel 2004.

[16] L'importanza del ruolo di questa Commissione e la sua posizione di garante si riflette altresì nella composizione. Quest'organo amministrativo indipendente è presieduto da una personalità designata dal Presidente della Repubblica, il quale resta in carica per sei anni, sulla base di una lista di quattro nomi proposta congiuntamente dal vicepresidente del Consiglio di Stato e dal primo presidente della Corte di Cassazione. Esso comprende tra i suoi membri un deputato ed un senatore; sono incompatibili con questo incarico coloro che svolgono già attività di Governo; il mandato non può essere rinnovato e si può concludere anticipatamente su dimissioni presentate dalla persona a suo tempo nominata ovvero su decisione della Commissione stessa.

gli organi di polizia ad ottenere i dati esterni delle comunicazioni dagli operatori telefonici, dagli *Internet Service Providers*, dagli *Internet Cafes*. Nel mese di dicembre dello stesso anno anche il Senato ha dato voto favorevole alla legge, contrariamente a quanto atteso, sebbene siano state sollevate più contestazioni concernenti la mancanza di una disposizione specifica che preveda l'intervento dell'organo giurisdizionale nelle procedure di raccolta dati e poi di intercettazione.

Tale norma anti-terrorismo, entrata in vigore nel gennaio 2007 e adottata mediante una procedura d'emergenza, mette a confronto il diritto alla libertà personale e l'interesse al mantenimento di uno stato di sicurezza pubblica. Agli organi di polizia sono dati ampi poteri di disporre intercettazioni nei casi in cui vi sia il semplice sospetto di attività terroristiche. La stessa legge legittima l'installazione di videocamere di sorveglianza in aree pubbliche quali stazioni, chiese, moschee.

Per dare attuazione a questa normativa e per renderla più efficace, nel maggio dello stesso anno è stato attivato un nuovo sistema di intercettazione sul territorio francese in grado di captare tutti i dati comunicativi che circolano sulla rete internet e a mezzo *mobile phone*: uno strumento antiterrorismo o una minaccia ai diritti civili dei cittadini francesi [17]?

2.3. Germania

Il contrasto al terrorismo internazionale non ha dato luogo in Germania ad una autentica legislazione dell'emergenza, a differenza di quanto era accaduto negli Anni '70 per finalità di contrasto al terrorismo di sinistra [18]. L'unica legislazione che presenta i caratteri dell'emergenza è il *LuftSiG* del 2004 con il quale sono state dettate una serie di regole in materia di sicurezza del traffico aereo, prescrivendo controlli minuziosi sui passeggeri ed i loro dati identificativi, sui bagagli e gli oggetti trasportati.

Il rigetto di una formazione emergenziale è significativo di un approccio ragionato e meno frettoloso, considerato anche che parte delle materie coinvolte non sono di piena competenza del parlamento federale ma sono suddivise tra competenza centralizzata e competenza

[17] Per avere un inquadramento più specifico sulla legge antiterrorismo è possibile visionare l'intero testo normativo nel web tramite qualsiasi motore di ricerca. Quanto alle discussioni sorte intorno alle singole disposizioni normative è possibile ottenere una documentazione più dettagliata dal sito *www.edri.org*, un portale che informa e riporta discussioni sulle tematiche legate, in particolare, al rapporto tra diritto e mondo digitale. Il sistema di intercettazione introdotto in applicazione della legge antiterrorismo francese del 2007 è installato dalle forze di polizia e si collega agli operatori di connettività e di telefonia. Nonostante i contrasti emersi in sede parlamentare tra le diverse forze politiche e nonostante siano stati sollevati più giudizi di costituzionalità, la Corte costituzionale francese ne ha decretato la piena legittimità e conformità alla Carta costituzionale. Secondo le stime di alcuni esperti di settore, la piattaforma di intercettazione può assolvere fino a circa 20 mila richieste l'anno.

Si riporta inoltre una curiosità sempre in materia di intercettazioni di cui, però, non si è potuto ottenere un riscontro diverso dalla fonte da cui è stata carpita che, però, risale al gennaio del 2007: pare che nel 2008 sia stato messo sul mercato per i soli membri del governo francese un telefono cellulare progettato e prodotto negli stabilimenti Thales (la società di riferimento è una multinazionale globale che si occupa di elettronica specializzata ed applicata al settore aerospaziale, al settore della difesa, nonché di *information technology*), denominato *Teorem*, in grado di sfuggire a qualsiasi forma di intercettazione e che consente di ricevere ed effettuare telefonate in maniera criptata, con la garanzia di una protezione piena del diritto alla riservatezza e segretezza delle comunicazioni.

[18] In tale situazione l'ordinamento aveva reagito apportando significative modifiche al codice di procedura penale (StO), introducendo delle misure afferente il diritto di difesa, limitando i poteri dell'imputato di conferire con il proprio difensore e imponendo l'interposizione di un soggetto terzo designato dall'autorità giudiziaria. Nello stesso contesto sono state anche introdotte delle disposizioni normative nel campo del cd. "trattamento massivo dei dati" o *Raster fahndung*, operato dalla polizia giudiziaria su autorizzazione dell'autorità giudiziaria.

decentrata e territoriale dei *Lander:* per esempio, la legislazione penale e di procedura penale è propria dell'ambito federale, mentre l'organizzazione dei servizi giudiziari e di polizia è propria di ogni *Land.*

Più in particolare, la strategia del legislatore tedesco in materia di terrorismo è volta maggiormente alla prevenzione dei pericoli e non alla repressione dei fenomeni criminosi. Nonostante questo generale approccio di politica criminale è stata introdotta la fattispecie di terrorismo internazionale nel codice penale tedesco (par. 129-b *Strafgesetzbuch*).

Dopo un primo pacchetto anti-terrorismo del 9 gennaio 2002 (*Terrorismusbekampfungsgesetz*) è stata introdotta un'ulteriore legge anti-terrorismo nel 2007, oltre alle ulteriori riforme intervenute nelle materie di interesse, ai fini della prevenzione e lotta al fenomeno terroristico e con specifico riguardo all'istituto delle intercettazioni.

Sono state sfruttate le potenzialità applicative della nota G10 del 1963 in materia di intercettazioni d'*intelligence.* Tale legislazione ha inciso sull'iniziativa e l'autorizzazione per l'intercettazione di comunicazioni e di flussi informatico-telematici per fini di *intelligence* ed è stata oggetto di modifiche con l'entrata in vigore della disciplina anti-terrorismo del 2007[19]. Già con il pacchetto anti-terrorismo del 2002 sono stati attribuiti ampi poteri di intercettazione ai servizi di sicurezza federale (*Bundesverfassungschutz*), potendo essi impiegare mezzi invasivi della riservatezza in luogo dell'interesse alla protezione dei singoli e alla sicurezza pubblica, per la prevenzione e repressione di attività terroristiche. Sempre nel 2002 è entrata in vigore nell'ordinamento tedesco la legge che prevede la formazione di Servizi Investigativi Doganali legittimati a svolgere delle intercettazioni preventive, fondate sul mero sospetto che si stiano preparando delle attività criminose contrarie al bene giuridico della sicurezza e dell'ordine pubblico (comprendendo in questa sfera il fenomeno terroristico).

La Corte costituzionale tedesca ha censurato parzialmente la normativa sulle intercettazioni ambientali con provvedimento del 3 marzo 2004 di natura additiva, introducendo l'obbligo di interrompere suddetto tipo di intercettazione allorché questa invada la sfera intima dell'individuo, in luogo di un più blando stralcio postumo.

Fino dall'adozione del *Terrorismusbekampfungsgesetz* del 1° gennaio 2002 vi è stato uno spostamento netto verso la preventivizzazione del fenomeno terroristico, lasciando ampi poteri d'indagine (compresa la possibilità di procedere ad intercettazioni) anche alle Autorità di polizia e non solo al Pubblico Ministero, il quale ha sempre più assunto un ruolo marginale di supervisore. La funzione di prevenzione si sostanzia precipuamente in un incremento delle potenzialità degli organi dell'*intelligence*, anche mediante una netta separazione funzionale tra servizi di informazione e sicurezza e servizi di polizia.

La menzionata legge del 2002 ha ridefinito le competenze del *Bundesverfassunschutz* con estensione alla raccolta e valutazione di informazioni ad ampio raggio nel rispetto di attività contrarie "alla comprensione tra i popoli" e alla pace, con piena disponibilità di mezzi tecnici eventualmente invasivi della riservatezza della persona. Ogni potere attribuito è subordinato all'autorizzazione del responsabile del servizio[20].

[19] La legge del 1963 è stata più volte oggetto di giudizio di costituzionalità dinnanzi alla Corte costituzionale tedesca ed è stata altresì oggetto di censure dinnanzi la Corte europea dei Diritti dell'Uomo (si ricorda, tra gli altri, il caso *Klass e altri v. Germania*), in relazione alle poche garanzie dei diritti fondamentali e dei diritti garantistici delle procedure autorizzative ed applicative delle operazioni di intercettazione, specie in relazione alle ampie libertà lasciate agli organi dell'*intelligence.*

[20] Per mero tuziorismo espositivo, si precisa che il contenuto del pacchetto anti-terrorismo tedesco del 2002 ha un contenuto molto più ampio e complesso di quello ivi riportato per interesse per l'argomento in analisi. Specie si trovano plurime disposizioni normative in ordine al trasferimento di dati all'estero e alla raccolta di informazioni e molto altro ancora. Il settore bancario e creditizio è molto interessato dalla norma ed il crescente

Nel contesto del codice di procedura penale tedesco, la materia delle intercettazioni è disciplinata in particolare agli articoli 110a e 100b, quanto alle intercettazioni nell'ambito di inchieste giudiziarie. Tali disposizioni sono il risultato di una riforma avvenuta con la legge del 21 dicembre 2007 [21].

L'art. 100a *StPO* prevede che possano essere effettuate intercettazioni e registrazioni di conversazioni telefoniche nei confronti di una o più persone sospettate di aver commesso, in prima persone ovvero in qualità di concorrente, uno dei gravi reati elencati nelle medesima disposizione e sanzionati con una pena detentiva non inferiore nel massimo a cinque anni. Il provvedimento è sussidiario. Il controllo è ammissibile soltanto qualora la direzione delle indagini e/o la perquisizione dell'abitazione della persona interessata risultino particolarmente complesse con l'utilizzo di strumenti diversi.

L'art. 100b *StPO* legittima le intercettazioni e le registrazioni di conversazioni telefoniche soltanto se disposte da parte del tribunale e su richiesta dell'organo dell'accusa ovvero direttamente da quest'ultimo in caso di pericolo imminente. L'ordinanza così sottoscritta dal procuratore deve essere ratificata e convalidata dal giudice entro i tre giorni successivi.

Le intercettazioni possono essere disposte per un termine limite pari a tre mesi, con possibilità di proroga per ulteriori tre mesi purché sussistano tutti i requisiti di cui all'art. 100a *StPO*.

Chiunque fornisca a scopo commerciale servizi di comunicazione è obbligato, sulla base del contenuto dell'ordinanza applicativa emessa dall'autorità competente, a consentire al giudice, al procuratore e agli investigatori della polizia l'intercettazione e la registrazione delle telefonate.

In caso vengano meno i presupposti autorizzative delle intercettazioni, queste devono essere immediatamente sospese e di ciò ne è data immediata comunicazione al giudice e ai fornitori dei servizi di comunicazione interessati. I dati sensibili e le informazioni raccolte possono essere utilizzati in altri procedimenti penali a fini di prova nella misura in cui emergano fatti e cognizioni necessari per le indagini di uno dei reati di cui all'art. 100a del codice di procedura penale tedesco. Viceversa, se la documentazione non è più di alcuna utilità ai fini dell'azione penale allora deve essere immediatamente distrutta sotto il controllo della procura.

3. La legislazione dell'emergenza per la lotta al terrorismo: l'ordinamento USA, United Kingdom e Federazione russa

Gli attentati alle *Twin Towers* dell'11 settembre 2001 hanno fortemente inciso sulla reazione legislativa degli americani i quali si sono visti direttamente colpiti nei luoghi rappresen-

interesse per quest'ambito proprio nell'ottica di prevenzione e repressione del terrorismo è da tempo sentita a livello comunitario per cui sono stati emanati diversi atti normativi UE, specie direttive, interessate sul punto.

Merita menzione altresì la legge 6 agosto 2002 sull'uso dell'*IMSi catcher* per la localizzazione dei telefoni la quale introduce nell'ordinamento procedurale penale il paragrafo 100-i, consentendo l'uso di suddetto strumento in presenza della commissione di gravi reati e, in via residuale, in ipotesi in cui non è possibile procedere alla localizzazione o alla sorveglianza di un soggetto mediante l'utilizzo di un diverso mezzo tecnico. Il procedimento autorizzativo è definito con rinvio a quello per l'autorizzazione delle intercettazioni di conversazioni telefoniche e di conseguenza sono richiesti i medesimi requisiti, compresa la competenza del giudice.

[21] Suddetta riforma è stata attuata al fine di dare attuazione alla Direttiva 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, nonché per conformità ad alcune sentenze del Tribunale costituzionale federale, in particolare la sentenza del 27 luglio 2005 la quale ha stabilito chiaramente che nell'ambito delle intercettazioni sono necessarie delle previsioni specifiche volte alla protezione della sfera privata dell'individuo.

tativi del sistema. Tale episodio terroristico ha avuto una rilevanza internazionale così forte da influenzare anche le scelte di riforma legislativa di altri ordinamenti giuridici. La necessità avvertita da alcuni Stati di far fronte al fenomeno del terrorismo internazionale ha indotto ad attenuare lo *standard* di garanzia delle libertà individuali dei cittadini per aumentare il grado di sicurezza pubblica.

Gli USA, l'Inghilterra e la Federazione russa sono chiari esempi di un particolare modello assiologico di formazione normativa con funzione emergenziale, mediante l'introduzione di disposizioni di legge in maniera affrettata.

3.1. USA [22]

Dopo due settimane dall'attentato di *Ground Zero*, il Senato statunitense ha approvato con un solo voto contrario il c.d. *USA Patriot Act*, convertito in legge a firma del Presidente Bush in data 26 ottobre 2001. Tale legge amplia le possibilità di procedere ad intercettazioni di comunicazioni telefoniche e telematiche per le forze di polizia [23]. Gli aspetti emergenziali della normativa in analisi sono molto chiari e si rilevano già nella procedura seguita per l'approvazione, avvenuta in tempi ristretti, adducendo la necessità di contrastare imminenti attacchi terroristici [24].

Questa norma è stata oggetto di censure fin dalla sua emanazione al fine di eliminare le clausole volte a limitare la vigenza delle disposizioni fortemente limitative del diritto alla riservatezza. Nel 2003, su iniziativa governativa, è stato approvato il *Patriot Act II*, un atto normativo caratterizzato da disposizioni assai invasive delle libertà individuali. In particolare il riferimento è alla disciplina delle intercettazioni di comunicazioni telefoniche o telematiche: sono previste ampie possibilità di espletamento di operazioni di captazione sia in ipotesi di un'indagine giudiziaria sia in un ambito di prevenzione mediante attività d'*intelligence*. Già prima delle riforme legislative a seguito dei fatti di terrorismo dell'11 settembre, il F*oreign Intelligence Surveillance* sottraeva al giudice ordinario la competenza ad autorizzare attività di sorveglianza, lasciando tale attribuzione al *Chief Justice*, ovvero ad una corte speciale, richiedendo non già la sussistenza di gravi indizi della commissione di gravi reati, ma la mera dimostrazione dell'utilità per l'acquisizione di informazioni d'indagine riguardanti cittadini stranieri o statunitensi.

Ancora più invasiva della sfera privata appare la disciplina approntata nelle sezioni 214 e 216 del *Patriot Act* nella misura in cui estende a tutte le comunicazioni mediante mezzi elettronici il regime di sorveglianza in precedenza limitato alle comunicazioni telefoniche.

Il menzionato *Patriot Act* del 2001 [25] era stato adottato come legislazione d'emergenza e pertanto destinata ad avere una durata limitata, precisata nella sezione 224 che indicava la data del 31 dicembre 2005. Invece, dopo due proroghe, l'ultima prevista in scadenza il 10 marzo

[22] Per una ricostruzione della normativa anti-terrorismo statunitense in generale e non solo limitata alla materia delle intercettazioni si rinvia alla lettura di A. MANNA, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in *Riv. it. dir. e proc. pen.*, 2004, 4, p. 1022 ss.

[23] Gli ampliamenti all'attività degli organi di polizia con il *Patriot Act* non hanno interessato soltanto le intercettazioni bensì una serie di altre attività tra cui le perquisizioni in abitazioni private.

[24] Per una disamina completa del testo del *Patriot Act* nonché per un'analisi delle procedure di approvazione si rinvia alla consultazione di uno dei siti di riferimento: *ex multis* si enuncia il sito *www.aclu.org*.

[25] L'articolo scientifico di F. CERQUA, *I profili processuali della legge antiterrorismo USA: brevi cenni*, in *Cass. pen.*, 2006, 5, p. 1948 ss. analizza compiutamente, sebbene sinteticamente, gli aspetti procedurali più significativi della normativa antiterrorismo americana, dandone uno spaccato molto chiaro ed utile ai fini di un'indagine della *ratio* generale della legge.

2006, il Congresso degli Stati Uniti ha approvato a larga maggioranza il rinnovo del *Patriot Act* rendendo permanenti un vasto numero di disposizioni, eccetto quelle in materia di intercettazioni di comunicazioni su apparecchi telefonici (c.d. *roving wiretap*). In questo contesto è cresciuto il senso di pericolo per la limitata garanzia e protezione del diritto alla privacy ed alla riservatezza delle comunicazioni, considerati gli ampi poteri discrezionali lasciati nelle mani delle agenzie investigative generali per la disposizione di intercettazioni telefoniche e, più in generale, per il controllo delle comunicazioni.

Il Quarto Emendamento della Costituzione federale americana è finalizzato a prevenire le interferenze "arbitrarie ed oppressive" dell'autorità giurisdizionale sul diritto alla privacy e sulla sicurezza personale di ogni singolo cittadino [26].

La disciplina delle intercettazioni, dopo le riforme attuate dal *Patriot Act*, è stata nuovamente oggetto di modifiche nel 2008, anno in cui, su esortazione del Senato statunitense e per volere del Presidente G.W. Bush, è stata ampliata la possibilità di compiere tali operazioni captative di flussi di comunicazioni telefoniche e telematiche per finalità di prevenzione e contrasto al fenomeno terroristico. Nel luglio 2008 suddetta legge è stata approvata anche dalla Camera ed è entrata in vigore all'interno degli Stati Uniti. La norma, tra l'altro, prevede una garanzia di impunità alle compagnie telefoniche che consegnino alle autorità federali i tabulati o le conversazioni effettuate all'interno dell'ordinamento americano.

Le libertà di intercettazione ed ascolto di comunicazioni si allargano oltre i confini nazionali: il Governo, infatti, può compiere le intercettazioni nei confronti di cittadini non americani per un termine massimo di sette giorni, anche senza una previa autorizzazione dell'autorità giudiziaria nelle ipotesi di necessità ed urgenza. Nell'ottica della protezione della nazione e dei cittadini, le risultanze delle intercettazioni restano assolutamente segrete ed utilizzate per i soli fini di giustizia [27].

Solo nel 2009 è stata abrogata la legge sulle intercettazioni nella parte in cui consentiva di procedere ad operazioni captative di comunicazioni telefoniche autorizzate sulla base di un mero sospetto di compimento o preparazione di atti terroristici.

Si rileva dunque che una legislazione quale il *Patriot Act*, inizialmente pensata, voluta e votata come legge dell'emergenza (sia nel contenuto sia nella procedura) è divenuta invece una norma permanentemente presente, efficace ed applicata nell'ordinamento giuridico americano [28].

3.2. United Kingdom

La principale fonte normativa in materia di intercettazioni nel Regno Unito è costituita dal

[26] In questi termini si è espressa la Corte Suprema Federale, *ex multis*, nella causa *Camara v. Mun. Court*, 387 U.S. 532, 528 (1967) ove i giudici hanno altresì affermato che il Quarto Emendamento stabilisce diritti "*basic to a free society*".

[27] Questo è forse uno degli elementi preponderanti che portano gli americani comunque ad accogliere una legge che permette ampi poteri di intercettazione poiché, oltre ad avere sempre un fondato timore di subire ulteriori e, se possibile, più gravi attacchi terroristici dopo quello dell'11 settembre 2001, sanno anche che le attività degli organi governativi e/o investigativi mediante l'utilizzo di strumenti captativi di comunicazioni restano nel pieno riserbo (nella maggior parte dei casi) e vengono solo utilizzate per le finalità per cui sono state compiute e solo dagli organi competenti.

[28] Per un approfondimento sul tema del rapporto tra l'interesse alla sicurezza pubblica ed il diritto alla *privacy*, con particolare riferimento al caso americano, si invita alla lettura di G. FROSIO, *Cosa resta della privacy? Diritto alla riservatezza dell'uomo medio dopo l'11 settembre*, in *Cyberspazio e diritto*, vol. 6, n. 2, Modena, 2005, p. 173 ss.

Regulation of Investigatory Powers Act del 2000 (RIPA), il quale ha attuato un'organica riforma della precedente regolamentazione del 1985, rivedendo i poteri investigativi delle autorità inquirenti e degli organi di polizia[29].

Essa delinea un quadro di garanzie mediante la previsione di una cornice di delimitazione delle finalità per le quali può essere legittimato l'uso di strumenti investigativi di intercettazione, gli obblighi di supervisione della magistratura, il riconoscimento del diritto all'opposizione da parte dei soggetti interessati all'effettuazione di tali operazioni e/o alla loro prosecuzione.

Dunque un interesse espresso del legislatore verso un bilanciamento tra gli opposti interessi, al fine di tutelare al massimo grado i diritti fondamentali sanciti dallo *Human Rights Act* del 1998[30].

Dal 2000 sono stati emanati una serie di *Statutory Instruments:* delle regolamentazioni afferenti taluni profili specifici, alla stregua di veri e propri codici di condotta. Tra questi, il 24 novembre 2005 è stato emanato il codice di conservazione dei dati delle comunicazioni (*data retention*), intervenuto a corredo della legislazione anti-terrorismo del 2001.

Le disposizioni raccolte nel RIPA quanto alle intercettazioni delle comunicazioni prevedono la captazione di comunicazioni a mezzo postale o con sistemi di telecomunicazione da parte delle autorità proposte alla tutela dell'ordine pubblico e dei servizi di sicurezza, previa autorizzazione dell'autorità ministeriale. Tale *warrant* è rilasciato purché siano sussistenti i fondamentali requisiti di necessità e proporzionalità e purché le intercettazioni siano necessarie a proteggere la sicurezza nazionale, individuale o a prevenire atti di criminalità di particolare gravità (quali ovviamente gli atti terroristici). In sede di autorizzazione è necessario accertarsi che le informazioni che si vogliono acquisire mediante un'intercettazione non possano essere ottenute in altro modo. Agli operatori di sistemi di telecomunicazione è richiesto, d'altra parte, di provvedere affinché i sistemi a loro disposizione siano tecnicamente configurati in modo tale da permettere di eseguire un'intercettazione.

Sulla corretta applicazione delle disposizioni del RIPA in materia di intercettazioni è preposto a vigilare lo *Interception of Communications Commissioner*, il quale pubblica annualmente un rapporto sull'attività svolta in materia.

La validità del provvedimento autorizzativi delle intercettazioni è di tre mesi, rinnovabile per altri tre o sei mesi a seconda che l'attività investigativa riguardi la criminalità organizzata oppure la sicurezza dello Stato[31].

Con l'entrata in vigore del *Terrorism Act* il 30 marzo del 2006 sono stati estesi i poteri investigative e i poteri dell'*intelligence*, altresì aumentando i termini di durata delle autorizzazione per le intercettazioni.

Tuttavia nel dicembre del 2009 il ministero dell'interno britannico ha preso una posizione significativa, ritenendo che le intercettazioni non possano essere ammesse nei processi che si

[29] Tale riforma legislativa si è resa necessaria in ragione della crescente evoluzione tecnologica e, soprattutto, dalla diffusione di apparecchi per le comunicazioni elettroniche sempre più sofisticati, nonché dei dispositivi di crittografia.

[30] Ciò non significa che con tale norma non si riscontrino disposizioni restrittive delle libertà personali a fronte della crescente preoccupazione e paura nei confronti del fenomeno terroristico. Sin dal 2000 nel Regno Unito spesso il legislatore si è interrogato circa la necessità di introdurre delle norme limitative della sfera dei diritti del singolo per finalità di prevenzione e repressione del terrorismo.

[31] Il materiale tratto dalle intercettazioni, oltre a dover provvedere a garantire al massimo grado il diritto alla *privacy* di terzi eventualmente ed incidentalmente interessati, non può essere diffuso, riprodotto o conservato se non nei limiti delle finalità per cui sono state autorizzate oltre che per taluni scopi di interesse pubblico quali, ad esempio, la tutela della sicurezza nazionale. Raggiunte tali finalità il materiale suddetto deve essere distrutto.

celebrano nelle aule dei tribunali inglesi e gallesi per incompatibilità con il sistema legale vigente nel Regno Unito. La legge britannica, infatti, prevede che tutti i metodi di acquisizione delle prove e degli elementi di prova debbano essere rivelati alla difesa, pena l'inutilizzabilità. Pertanto le intercettazioni, per loro natura, sono sconosciute al soggetto che le subisce inconsciamente e dunque risultano essere illegittime per l'ordinamento giuridico britannico. D'altro canto, come rilevato dall'ex giudice londinese, sir Geoffrey Grigson, che senso avrebbe palesare delle attività di intelligence, vanificandone il ruolo e le finalità? La domanda resta aperta ed è certamente occasione di dibattito.

Si precisa però che il Comitato per i diritti Umani delle Nazioni Unite nel 2008 ha censurato la legge antiterrorismo britannica del 2006 sotto plurimi aspetti e, tra l'altro, per assenza di una proporzionalità tra le esigenze e le finalità di sicurezza pubblica, prevenzione e repressione del fenomeno terroristico e rispetto e garanzia dei diritti fondamentali del singolo cittadino [32].

3.3. Federazione russa

In base all'art. 23 della Costituzione russa del 1993 "ciascuno ha diritto all'inviolabilità della vita privata, alla riservatezza personale e familiare, alla difesa del proprio onore e del buon nome. Ciascuno ha diritto alla segretezza della corrispondenza, delle conversazioni telefoniche, delle comunicazioni postali, telegrafiche ed altre".

Ciò nonostante, specie per far fronte a fenomeni di terrorismo interno ed alle crisi diplomatiche con la vicina Georgia e, ancora più in particolare, dopo i noti fenomeni di terrorismo accaduti in Ossezia nella vicenda della scuola di Beslan, si è reso necessario un intervento limitativo delle libertà sempre più stringente e specifico.

L'art. 186 del codice di rito ammette le operazioni di intercettazione nei casi in cui vi sia un fondato sospetto che una conversazione telefonica o una conversazione possa contenere delle informazioni rilevanti per i fini della giustizia.

L'art. 165, invece, regola le modalità attraverso cui viene emesso il provvedimento autorizzativo per qualsiasi attività di indagine: sulla base della richiesta della pubblica accusa titolare del procedimento ovvero dall'esperto che effettivamente compirà le operazioni, decide il giudice istruttore.

Ai sensi del comma 3 del menzionato art. 186, la richiesta di intercettazioni è vincolata nel contenuto e richiede una precisione delle informazioni richieste, dei motivi, della fonte interessata, anche per il fine della tutela del diritto alla riservatezza delle comunicazioni e conversazioni, come garantito costituzionalmente.

Ne possono fare richiesta anche la persona offesa, i prossimi congiunti dei testimoni e i testimoni stessi.

Il termine massimo di durata è previsto in sei mesi. Delle conversazioni intercettate deve essere redatto un verbale specifico sulle operazioni compiute e al termine deve essere disposta la trascrizione delle conversazioni così captate.

Parallelamente alla disciplina delle intercettazioni del codice di procedura penale russo, trova applicazione la legge federale n. 144-FZ, una legge speciale in materia di indagini giudiziarie. Suddetta norma si applica alle attività investigative segrete (art. 1) e quando tali atti

[32] Per maggiori delucidazioni sul punto si invita alla lettura del *General Report del Counsil of Europe*, redatto a cura di S. BRAMAN, *Conference on Anti-terrorism legislation in Europe since 2001 and its impact on freedom of expression and information*, in *www.coe.int* (consultato il 4 giugno 2009).

siano compiuti al fine di prevenire e reprimere i fenomeni criminosi, di ricercare i responsabili, nonché di raccogliere le informazioni utili per la pace e la sicurezza della nazione (art. 2).

Il materiale probatorio raccolto in violazione di questa legge federale ed in violazione dei diritti e delle libertà fondamentali deve essere distrutto (art. 5).

Le informazioni ottenute mediante le intercettazioni, considerato l'alto grado di invasività di questo mezzo d'indagine, devono essere custodite con particolare attenzione per evitarne l'indebita diffusione (art. 8). Tali notizie, infatti, sono coperte dal segreto, salvo che l'interessato dia un'autorizzazione scritta alla diffusione.

Un forte inasprimento della disciplina delle intercettazioni si è avuto con la legge federale n. 35-FZ, entrata in vigore nel 2006 e discussa a seguito dei fatti di Beslan del 2004.

Ai sensi dell'art. 11 della legge, nell'ambito delle operazioni antiterrorismo è possibile controllare comunicazioni e conversazioni effettuate con qualsiasi mezzo e senza limiti di durata. Tuttavia è necessario precisare che tale norma dovrebbe trovare applicazione soltanto nei casi di dichiarato stato di emergenza per la minaccia terroristica o comunque per una generica minaccia alla sicurezza pubblica.

Questa normativa, pur essendo stata oggetto di plurime critiche e denunce per contrasto alle garanzie dei diritti fondamentali riconosciuti a livello nazionale e sovranazionale, non è stata dichiarata incostituzionale.

Il Governo, addirittura, in base alla legge 35-FZ, può captare delle comunicazioni anche senza l'autorizzazione del giudice [33].

4. Alcuni dati statistici rilevanti

I dati statistici sul numero di intercettazioni che vengono effettuate ed autorizzate, nonché sui costi della giustizia per questa attività sono utili ai fini delle considerazioni critiche di conclusione.

L'Osservatorio sulla Legalità e sui Diritti riporta alcuni interessanti numeri: in Italia si fanno circa centomila intercettazioni l'anno, in Francia circa ventimila, in Gran Bretagna cinquemilacinquecento e in USA millesettecentocinque [34]. Tali dati, però, riguardano soltanto le intercettazioni disposte per autorizzazione della magistratura dunque, oltre a tenere conto del rapporto con il numero di notizie di reato che vengono iscritte in ogni ordinamento ed il numero di cittadini di ogni nazione, bisogna altresì considerare che in molti Paesi le intercettazioni sono disposte da altri soggetti pubblici: per esempio in Inghilterra le più diverse autorità compiono operazioni di ascolto delle conversazioni su circa mille persone ogni giorno.

Secondo uno studio pubblicato sul quotidiano *Le Figaro* nel luglio del 2009, in Francia le intercettazioni sono aumentate del 440% nel 2008 rispetto al 2001. Il *Sole 24 Ore*, invece, ha riportato i dati delle intercettazioni in Germania nel 2008 per cui sono stati emessi in tale anno tredicimilanovecentoquarantanove decreti di intercettazione (un incremento di circa 11% rispetto al 2007) ma solo seicentoventotto per indagini afferenti a fenomeni di terrorismo.

Quanto ai costi delle operazioni di intercettazione, secondo i dati pubblicati dal quotidiano *Il Sole 24 Ore*, in Francia nel 2009 sono stati spesi trentatre milioni di euro, a cui bisogna aggiungere le spese di locazione dei materiali; in Italia, sempre nel 2009, sono stati spesi circa

[33] Per un maggiore approfondimento sul tema delle intercettazioni nella Federazione russa e per i riferimenti bibliografici di maggiore rilevanza in materia ci si permette di rinviare a E. COLOMBO, *Le intercettazioni telefoniche nella Federazione russa*, in *Cass. pen.*, 2008, 3, p. 1230 ss.

[34] Non è stato però possibile indagare le modalità di raccolta e di elaborazione dei dati statistici qui riportati.

duecentosettanta milioni di euro. Sempre secondo il medesimo rapporto statistico, ogni intercettazione effettuata per una linea fissa costa non meno di cinquecento euro e su telefono mobile non meno di cento euro.

5. Conclusioni

Dalla ricostruzione della disciplina delle intercettazioni ed in particolare delle intercettazioni per la prevenzione e la repressione del fenomeno terroristico si comprende, con le dovute differenze tra le leggi, che vi è una sottile linea di confine ed un labile limite di bilanciamento tra il diritto alla *privacy* e alla riservatezza delle comunicazioni da un lato con l'interesse alla sicurezza pubblica dall'altro.

La necessità di bilanciamento tra opposte esigenze è centrale quando si tratta di alcune forme di criminalità di particolare allarme sociale, quali il terrorismo.

Ebbene, nonostante vi sia un'attenzione alla garanzia del diritto alla *privacy* sia nelle leggi fondamentali dei singoli ordinamenti, sia a livello comunitario ed internazionale, contestualmente si rileva che l'interessa al mantenimento di una situazione di tranquillità e sicurezza nazionale e internazionale, allo stato, prevale. Ciò è in parte confermato anche dall'aumento costante e continuo del numero di intercettazioni effettuate.

La tendenza alla restrizione del diritto alla riservatezza è attestata anche dalla Convenzione di Budapest sul *cyber crime* nelle cui norme gli organi di polizia trovano l'ampliamento dei propri poteri anche di intercettazione sia telematiche sia informatiche.

Oltre al menzionato problema di tipo qualitativo circa il confine delle opposte esigenze, vi è anche un problema quantitativo nel rapporto tra intercettazioni e terrorismo. Come visto, le operazioni di captazione delle diverse comunicazioni hanno dei costi ragguardevoli (oltre all'impegno del personale). Pertanto è necessario chiedersi se siano così importanti e cruciali al fine della prevenzione e della repressione del fenomeno terroristico.

I dati statistici che si sono potuti rilevare quanto alla Germania, portano a concludere che la prevenzione e la repressione del fenomeno del terrorismo non passano per il tramite delle intercettazioni. Essendoci però questo dato limitato ad un solo Stato non è possibile compiere delle considerazioni generali e resta, dunque, il dubbio se vi siano degli strumenti d'indagine meno invasivi e più efficaci delle intercettazioni.

Il rischio è che si venga a creare un generale e condiviso approccio al fenomeno del terrorismo volta all'introduzione di una legislazione dell'emergenza, con la paura che si giunga ad una normalizzazione dell'emergenza stessa.

D'altro canto, come rilevato dal Consiglio d'Europa[35], si verifica un enorme scarto tra quanto è previsto nella legge e quanto viene attuato nella prassi poiché questa è spesso influenzata da forze informali, private e/o socio-culturali: tali forze però incoraggiano un'armonizzazione delle normative nazionali al fine di una maggiore efficacia delle politiche di cooperazione giudiziaria e di polizia.

La guerra al terrorismo si sta ripercuotendo in modo significativo sul regime interno dei diritti, sebbene in maniera differenziata nei vari ordinamenti giuridici nazionali.

Resta palese una generale spinta verso una maggiore comunanza di principi tra le diverse normative nazionali interne, al fine di uno sviluppo della cooperazione cercata e voluta dai più.

[35] Il riferimento è al già menzionato rapporto curato da S. BRAMAN, *Conference on Anti-terrorism*, cit.

CAPITOLO 6

Intercettazioni e lotta alla pedopornografia

di *Marta Doniselli*

SOMMARIO: 1. Premessa. – 2. Brevi osservazioni sulla recente normativa comunitaria in materia di contrasto alla pedopornografia *on line*. – 3. Il ruolo delle intercettazioni nella lotta alla pedopornografia *on line*: quadro normativo italiano e generali problematiche delle intercettazioni informatiche. – 3.1. *Segue*: la distinzione fra intercettazioni informatiche o telematiche ed altre attività investigative di contrasto alla pedopornografia. – 4. Conclusioni.

1. Premessa

Dato il tema del presente Convegno e la brevità del tempo a mia disposizione, mi limiterò ad affrontare le problematiche delle intercettazioni solo con riferimento a quelle ammesse nei procedimenti per i reati di pedopornografia a mezzo Internet, i quali rappresentano una *species* del più ampio *genus* dei c.d. crimini informatici, latamente intesi.

Cercherò di fare sul tema qualche breve osservazione, senza pretesa di esaustività, fornendo preliminarmente il quadro normativo, comunitario e nazionale, entro cui questo si colloca.

2. Brevi osservazioni sulla recente normativa comunitaria in materia di contrasto alla pedopornografia *on line*

L'impegno comunitario nella lotta alla pedopornografia *on line* risale ad oltre un decennio fa [1].

Fin dai primi atti dell'UE, emerge la consapevolezza della natura transnazionale di questo tipo di crimini e dell'urgente necessità di uniformare le legislazioni degli Stati Membri, sia dal punto di vista della legge penale sostanziale [2], con un omogeneo riconoscimento delle condotte penalmente rilevanti, sia attraverso l'armonizzazione delle procedure. Ciò al fine di dotare il processo penale, soprattutto nella fase d'indagine, degli adeguati strumenti di preven-

[1] Fra gli atti comunitari più risalenti si segnalano l'esortazione del Consiglio Europeo di Vienna del'11-12 dicembre 1998 per assicurare sul piano europeo e internazionale misure efficaci contro la pedo-pornografia su Internet, la decisione n. 276/1999 CE del Parlamento Europeo e del Consiglio di adozione di un piano comunitario per promuovere l'uso sicuro di Internet attraverso la lotta alle informazioni illecite e alla loro diffusione attraverso la Rete, la decisione del 29 maggio 2000 del Consiglio con cui l'UE pone le basi per un'attività di contrasto condivisa contro la *pedopornografia on line*.

[2] Sul tema M. D'AMICO, *L'Europa e la lotta alla pornografia infantile. Verso un diritto penale europeo?*, in *Quad. cost.*, 2000, 3, p. 696 ss.

zione e repressione, resi necessari dall'inesorabile sviluppo tecnologico.

Le tecnologie offrono, infatti, all'utente forme sempre nuove di perpetrazione di tali delitti, in cui si annidano ampie aree di impunibilità, spesso legate a problematiche tecniche connesse allo strumento informatico [3].

La predisposizione da parte degli Stati Membri di misure procedurali che garantiscano un effettivo accertamento delle condotte criminose, da un lato, e il rispetto dei diritti di difesa [4], dall'altro è una preoccupazione costante, al centro della politica criminale dell'UE.

Fra le decisioni più risalenti, ma più significative per quanto riguarda gli aspetti di diritto processuale, vi è certamente la Decisione del Consiglio del 29 maggio 2000, relativa alla lotta contro la pedopornografia infantile su Internet [5].

L'art. 4 della Decisione invita gli Stati Membri a verificare regolarmente "*se i progressi tecnologici rendono necessaria, al fine di mantenere l'efficacia della lotta contro la pornografia infantile su Internet, una modifica della loro procedura penale, nel rispetto dei principi fondamentali*" e a novellare, nell'eventualità, la propria normativa. Viene sollecitata, inoltre, la creazione di unità specializzate preposte a questo tipo di indagini e l'introduzione di strategie investigative "tatticamente" [6] indispensabili per scoprire le identità degli autori degli illeciti, fra le quali, ad esempio, il differimento dell'esercizio dell'azione penale [7].

Fra gli atti comunitari più recenti in materia, invece, deve essere segnalata la Convenzione del Consiglio d'Europa STCE n. 201 sulla protezione dei bambini contro lo sfruttamento e l'abuso sessuale, firmata a Lanzarote il 25 ottobre 2007.

La Convenzione, passata inosservata sia da parte della dottrina, ma anche da gran parte degli Stati Membri [8], contiene una disciplina organica e minuziosa delle misure che nei vari settori, compreso quello della giustizia penale, devono essere adottate per contrastare il fenomeno dello sfruttamento sessuale dei minori. In essa un intero capitolo, il IV, è dedicato alle norme procedurali e alle modalità di indagine. Le indicazioni riguardano lo "statuto" del minore – testimone [9], la posizione della vittima nel procedimento [10], la necessità che l'avvio delle indagini e la loro prosecuzione avvenga senza ritardo e senza ostacoli, rappresentati dalle

[3] Sul tema F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 163.

[4] Sul tema D. DELL'ORTO, *Pedopornografia on line e indagini informatiche – Complessità e peculiarità tecnico-giuridiche della materia*, in *Cass. pen*., 2007, p. 879 ss.

[5] Decisione 2000/375/GAI, in *G.U.* 9 giugno 2000, L. 138.

[6] Il termine è tratto dal testo della Decisione in commento. Sul punto anche S. MASSA, *Nuove forme di devianza ai danni dei minori e risposte normative*, Napoli, 2002, p. 97 ss.

[7] Il nostro ordinamento aveva già in precedenza attuato questa indicazione, rendendola compatibile con il principio di obbligatorietà dell'azione penale *ex* art. 112 Cost., attraverso il disposto di cui all'art. 14, comma 3 della legge n. 269 del 1998: "*L'autorità giudiziaria può, con decreto motivato, ritardare l'emissione o disporre che sia ritardata l'esecuzione dei provvedimenti di cattura, arresto o sequestro, quando sia necessario per acquisire rilevanti elementi probatori* (…)".

[8] La Convenzione è stata firmata da trentatré Stati Membri, ma ratificata solo da cinque, fra cui non vi è l'Italia. La Convenzione, ratificata per prima dalla Gran Bretagna il 10.3.2009, e poi a seguire dall'Albania, dalla Danimarca, dai Paesi Bassi e dalla Repubblica di San Marino, entrerà in vigore per questi Stati in data 1.07.2010. In Italia la legge di "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguamento dell'ordinamento interno*" è stata approvata dalla Camera il 19 gennaio 2010 ed è attualmente all'esame del Senato.

[9] Art. 35 della Convenzione.

[10] Artt. 31 e 36 della Convenzione.

condizioni di procedibilità o dall'intervento della prescrizione [11] e la possibilità che i servizi investigativi possano identificare le vittime attraverso l'esame del materiale pedopornografico (foto, videoregistrazioni, ecc.). Si insiste, inoltre, sull'opportunità di investigazioni "speciali" [12] e di operatori (organi che conducono le indagini, autorità giudiziaria, avvocati, ecc.) che godano di una preparazione adeguata, a tutela tanto della bontà dell'accertamento, quanto dei diritti dei soggetti coinvolti [13].

La Convenzione è l'unico atto comunitario, fra quelli che si occupano della tematica in esame, a dire espressamente che le misure procedurali adottate per la lotta alla pedopornografia, devono tener conto dei diritti della difesa e dei principi dell'equo processo, enunciati all'art. 6 CEDU.

L'annotazione non è di poco conto, se si considera la recente tendenza, anche italiana, a contenere l'allarme sociale per questo tipo di reati, mediante l'irrigidimento della disciplina processuale e l'applicazione di istituiti a tutela della vittima, ma fortemente limitativi dei diritti di libertà dell'imputato [14].

L'importanza della Convenzione è sottolineata anche dai recentissimi atti comunitari che propongono l'abrogazione della Decisione Quadro 2004/68/GAI [15], fino ad ora considerata il monito principale per il riavvicinamento delle legislazioni degli Stati Membri in questa materia.

Il riferimento è:

– alla raccomandazione del Parlamento Europeo del 3 febbraio 2009 al Consiglio, che esorta a "*rivedere la Decisione Quadro (...) in modo da elevare il livello di protezione almeno sino a quello previsto dalla Convenzione del Consiglio d'Europa e da restringere il campo sugli abusi connessi a Internet e ad altre tecnologie della comunicazione*" [16];

– alla proposta di Decisione Quadro del Consiglio del 25 marzo 2009 [17], che definisce la Convenzione come "*lo strumento che, allo stato attuale, assicura la massima protezione dei minori sul piano internazionale*";

– alla proposta di Direttiva del Parlamento Europeo e del Consiglio del 29 marzo 2010 [18],

[11] La necessità che le indagini prendano avvio senza ritardo è enunciato all'art. 30, n. 3 della Convenzione, che incoraggia le parti ad eliminare dal sistema qualsiasi elemento che possa essere impediente rispetto al perseguimento di questi tipi di crimini. Ad esempio, sollecita la procedibilità d'ufficio e l'irretrattabilità della querela (art. 32), la possibilità di continuare le indagini anche dopo il compimento della maggior età da parte dell'offeso a seconda della gravità del reato per cui si procede (art. 33) e che le stesse non siano ostacolate dall'incertezza sull'età della vittima. (art. 34).

[12] All'art. 30, n. 5, la Convenzione sollecita gli Stati a prevedere indagini sotto copertura, per rendere più efficaci e proficue le operazioni degli inquirenti. Le operazioni sotto copertura sono disciplinate nel nostro ordinamento dall'art. 14 legge n. 269 del 1998.

[13] Artt. 34 e 36 della Convenzione. Questi contenuti sono ripresi dalla Proposta di Direttiva del Parlamento Europeo e del Consiglio del 29 marzo 2010, all'art. 14, rubricato "*Indagini e azione penale*".

[14] Il riferimento è alla recente legge n. 38 del 2009, che introduce la custodia cautelare in carcere obbligatoria per gli indagati di reati sessuali, la nuova misura cautelare del divieto di avvicinamento dei luoghi frequentati dalla persona offesa, l'estensione dei casi di assunzione della testimonianza in incidente probatorio e l'accesso al gratuito patrocinio da parte dell'offeso in deroga ai limiti di reddito previsti. La legge modifica inoltre il trattamento penitenziario previsto per i condannati per reati sessuali, riducendo drasticamente l'accesso ai benefici, già fortemente ridimensionato ad opera della legge n. 38 del 2006.

[15] Decisione Quadro a cui l'Italia si è adeguata con la legge n. 38 del 2006, che novella la normativa dei reati sessuali proprio con riferimento alle fattispecie di pedopornografia *on line*, in parte introdotte dalla legge n. 269 del 1998.

[16] La Raccomandazione è la 2010/C 67 E/06, in *G.U.* 18 marzo 2010.

[17] (SEC-2009-355) (SEC-2009-356).

[18] COM (2010) 94 def.; 2010/0064 (COD).

secondo cui con l'integrazione delle disposizioni della Convenzione nella normativa dell'UE "*si otterrà una più rapida adozione delle norme nazionali rispetto al processo nazionale di ratifica e si garantirà un miglior monitoraggio dell'attuazione*".

Dall'analisi di questi atti comunitari si evince, da un lato, l'inadeguatezza dello strumento convenzionale per attuare l'armonizzazione delle legislazioni, ai fini della prevenzione e repressione della pedopornografia *on line*, dall'altro, l'insufficienza della Decisione Quadro 2004/68/GAI di fronte alla rapida evoluzione tecnologica, che ha fortemente condizionato le modalità di compimento e di contrasto di questo fenomeno criminale.

Secondo la proposta del 29 marzo 2010, infatti, la Decisione "ravvicina le normative soltanto per quanto riguarda un numero limitato di reati, non si occupa delle nuove forme di abuso e sfruttamento che si avvalgono delle tecnologie informatiche, non elimina gli ostacoli all'azione penale al di fuori del territorio nazionale, non va incontro alle esigenze specifiche delle vittime né prevede misure adeguate per prevenire i reati" [19].

Mai come da queste ultime proposte emerge la necessità di trasformare la procedura, da "cenerentola" [20] a "principessa"!

Si auspica, dunque, un rapido sviluppo di regole procedurali comuni, che accompagni quell'armonizzazione del diritto sostanziale, da più tempo sollecitata e, in parte, già avvenuta a livello europeo.

3. Il ruolo delle intercettazioni nella lotta alla pedopornografia *on line*: quadro normativo italiano e generali problematiche delle intercettazioni informatiche

La cornice normativa che legittima il ricorso alle intercettazioni nei procedimenti riguardanti i reati di *pedofilia on line* è rappresentata dagli artt. 266, comma 2, lett. f-*bis*) [21] e 266-*bis* c.p.p. [22].

L'art. 266 c.p.p., che, come noto, stabilisce i limiti di ammissibilità delle intercettazioni, è stato modificato dalla legge n. 269 del 1998 [23]. Attraverso l'inserimento, nel comma 2, della lett. f-*bis*), ha consentito le intercettazioni di comunicazioni e di conversazioni telefoniche e tra presenti anche nei procedimenti per il reato di pornografia minorile di cui all'art. 600-*ter*, comma 3, c.p.

[19] La Decisione Quadro 2004/68/GAI, a cui l'ordinamento italiano ha dato attuazione con la legge n. 38/2006, non contiene riferimenti alla normativa processuale, ad eccezione di qualche indicazione sul riparto di giurisdizione, nel caso di reato commesso, anche solo parzialmente, sul territorio dello Stato, da un cittadino dello Stato oppure da una persona giuridica con sede nel suo territorio (Art. 8 "*Giurisdizione ed esercizio dell'azione penale*").

[20] La definizione del diritto processuale quale "cenerentola" della scienza penale risale ad un celebre scritto di F. CARNELUTTI, pubblicato nella *Rivista di diritto processuale* del 1946, vol. I, p. 1 ss.

[21] "*Art. 266. Limiti di ammissibilità. 1. L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati (...) f-bis) delitti previsti dall'articolo 600-ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1 del medesimo codice*".

[22] "*Art. 266-bis. Intercettazioni di comunicazioni informatiche o telematiche. 1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi*".

[23] Legge 3 agosto 1998, n. 269, "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*".

La *ratio legis* della novella è evidentemente quella di potenziare gli strumenti investigativi a disposizione nei procedimenti per tal genere di delitti, vista le peculiari modalità di realizzazione delle condotte incriminate.

La dottrina[24] si è dimostrata concorde nel ritenere necessaria questa modifica. Senza tale interpolazione, infatti, le operazioni intercettative sarebbero state consentite solo in presenza di una delle circostanze aggravanti di cui al secondo comma dell'art. 600 *sexies* c.p., stante i limiti edittali dei reati inclusi dall'art. 266, lett. a), c.p.p.[25].

Questa lettera è stata poi ulteriormente "ritoccata" dalla legge 6 febbraio 2006, n. 38 "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*", che ha esteso le intercettazioni anche ai casi in cui il materiale pedopornografico ottenuto mediante lo sfruttamento di minori di anni diciotto, distribuito, divulgato, diffuso o pubblicizzato anche a mezzo telematico[26], sia rappresentato dalle immagini virtuali, di cui all'art. 600-*quater* 1 c.p., realizzate utilizzando immagini di minori.

L'art. 266-*bis* c.p.p., oltre che legittimare il ricorso all'intercettazione di flussi telematici per i reati previsti dall'art. 266 c.p.p., dispone che tal tipo di operazione possa essere effettuata in tutti i procedimenti per reati compiuti attraverso la tecnologia informatica, indipendentemente dalla loro cornice edittale[27].

La lettura combinata degli artt. 266 e 266-*bis* c.p.p. impone, quindi, di concludere che le intercettazioni di comunicazioni informatiche o telematiche sono consentite non solo nel caso del reato di cui all'art. 600-*ter*, comma 3, c.p.p., ma anche per fattispecie meno gravi come quelle previste dall'art. 600-*ter*, comma 4, c.p., riguardante la cessione anche gratuita di materiale pornografico prodotto mediante lo sfruttamento sessuale di minori, e dall'art. 600-*quater* c.p. relativo all'atto di procurarsi o disporre lo stesso materiale, quando commessi mediante l'uso delle tecnologie informatiche.

Rimangono fuori dall'applicazione del combinato disposto degli artt. 266 e 266-*bis* c.p.p. dunque, solo le fattispecie delittuose sessualmente connotate, che non si realizzano attraverso lo strumento informatico e per il cui accertamento non è necessario procedere all'intercettazione di flussi telematici.

È interessante notare che l'art. 3 del d.d.l. n. 1348 "*Misure contro gli atti persecutori*" presentato dal Ministro per le Pari opportunità Carfagna e dal Ministro della Giustizia Alfano prevedeva la modifica dell'art. 266, lett. f), estendendo così l'ammissibilità delle intercettazioni telefoniche, ambientali e telematiche (visto il richiamo dell'art. 266-*bis* c.p.p. ai reati elencati nell'art. 266 c.p.p.), anche ai procedimenti per il "nuovo" reato di "atti persecutori".

L'art. 3 del d.d.l. n. 1348 è poi stato trasposto nell'art. 9 del d.l. n. 11 del 2009, convertito

[24] In questo senso V. MUSACCHIO, *Brevi considerazioni sulla nuova normativa penale "antipedofilia"*, in *Giust. pen*., 1998, II, p. 670; N. GALANTINI, *Commento all'art. 12 l. 269/1998*, in A. CADOPPI (a cura di), *Commentari delle norme contro la violenza sessuale e della legge contro la pedofilia*, Padova, 2002, p. 772; G. SPANGHER, *Le norme di diritto processuale penale*, in *Dir. pen. proc.*, 1998, 10, p. 1232.

[25] Ai sensi dell'art. 266, lett. a), le intercettazioni di comunicazioni e conversazioni, anche fra presenti, è ammessa per delitti sessualmente connotati, diversi da quello previsto dall'art. 600-*ter*, comma 3, c.p., quali il delitto di prostituzione minorile (art. 600-*bis*, comma 1, c.p.), il delitto di pornografia minorile (art. 600-*ter*, commi 1 e 2, c.p.), il delitto di violenza sessuale (art. 609-*bis* c.p.), il delitto di atti sessuali con minorenni (art. 609-*quater* c.p.) e il delitto di violenza sessuale di gruppo (art. 609-*octies* c.p.).

[26] È questa la condotta prevista e punita dall'art. 600-*ter*, comma 3, c.p.

[27] Secondo N. GALANTINI, *op. cit.*, p. 772, l'art. 266-*bis* c.p.p. è norma autonoma rispetto all'art. 266 c.p.p. con riferimento ai reati commessi attraverso le tecnologie informatiche.

senza modificazioni nella legge n. 38 del 2009[28], privato, però, della parte in cui disponeva la modifica dell'art. 266, lett. f), c.p.p.).

La disciplina sulle intercettazioni non è stata, quindi, modificata dalla recente legge n. 38 del 2009[29].

La proposta, poi caduta, di estendere le intercettazioni anche ai procedimenti per il reato c.d. di *stalking*, del tutto coerente con la tendenza della recente legge a rafforzare i poteri di indagine nel perseguimento dei delitti sessuali, non appare irragionevole, stante le molteplici condotte (per altro non specificate nell'art. 612-*bis* c.p.p.[30] e la diversa tipologia dei mezzi utilizzabili (telefono, PC, ecc.) per realizzare l'intromissione continua e inopportuna nella sfera privata della vittima e concretare questa subdola forma di molestia.

Le intercettazioni telematiche incontrano, nei procedimenti per i reati di *pedo-pornografia on line,* gli stessi problemi in tema di compatibilità con i diritti costituzionalmente garantiti, primi fra tutti il diritto alla segretezza delle comunicazioni di cui all'art. 15 Cost. e il diritto di difesa *ex* art. 24 Cost., che si pongono con riferimento a procedimenti per reati di tipo diverso, commessi attraverso la Rete.

Si pensi, ad esempio, al problema di determinare il *locus commissi delicti,* al fine di individuare la legge applicabile e la giurisdizione competente e i susseguenti limiti a cui le intercettazioni possono essere sottoposte[31] oppure ancora al ricorso ad impianti esterni gestiti da privati, che, per quanto riguarda le intercettazioni telematiche o informatiche, è ammesso al pari dell'uso degli impianti collocati in Procura (art. 268, comma 3 e 3-*bis* c.p.p.)[32].

A tal proposito, il codice di rito nulla dispone con riferimento alle intercettazioni di flussi telematici[33] affidate a fornitori privati di servizi di comunicazione elettronica, alle modalità

[28] Ultima legge in ordine cronologico che apporta sostanziali modifiche, anche procedurali, alla disciplina legislativa in materia di reati sessuali.

[29] Il recentissimo d.d.l. n. 1415 in materia di intercettazioni, attualmente ancora all'esame delle Camere, estende la possibilità di ricorrere a questo mezzo di ricerca della prova anche nel caso in cui si proceda per il reato di atti persecutori, di cui all'art. 612-*bis* c.p., grazie all'emendamento apportato dal Senato all'originario art. 1, comma 9.

[30] In senso critico A. AGNESE-G. PULIATTI, *Violenza sessuale e stalking*, Forlì, 2009, p. 74 ss.

[31] L'individuazione del *locus commissi delicti* con riferimento a reati c.d. informatici è problematica proprio a causa della tecnologia utilizzata per la loro perpetrazione, all'immaterialità e alla velocità di diffusione del dato informatico. Pur potendosi considerare come commessi all'estero i delitti commessi da soggetti che utilizzino *servers* collocati al di fuori del territorio italiano non sempre è nota la localizzazione del sito a cui si chiede l'accesso. Vi è inoltre il problema della contemporaneità dell'evento, che potrebbe portare all'attivazione di giurisdizioni diverse. Una delle soluzioni proposte dalla dottrina è quella di utilizzare come criterio di individuazione della competenza territoriale il vincolo che lega l'utente al *provider*, determinando così il collegamento fra soggetto-utente autore del delitto e territorio. Così N. GALANTINI, *op. cit.*, p. 779. Attualmente si prospettano a livello internazionale due diversi approcci: ai fini della determinazione della competenza e della legge applicabile, viene considerato da una parte il luogo dell'azione (ovvero il luogo di immissione della rete dei dati), dall'altro il luogo dell'evento (ovvero il luogo della ricezione dei dati da parte dei destinatari/vittime). Il criterio dell'azione, quello maggiormente diffuso, ha lo svantaggio di consentire all'autore dell'illecito di scegliere *ex ante* la legge applicabile, individuando le aree in cui le condotte non sono riconosciute come reati oppure sono sottoposte a sanzioni più lievi. L'insufficienza di questo criterio è dimostrata dall'applicazione, anche da parte dell'Italia *ex* art. 6, comma 2, c.p., del c.d. principio di ubiquità, che è rappresentato dal cumulo del criterio dell'azione con quello dell'evento. Così D. D'AGOSTINI, *Diritto Penale dell'Informatica*, Forlì, 2007, p. 176 ss.

[32] La disposizione secondo N. GALANTINI, *op. cit.*, p. 773, annulla la portata precettiva dell'art. 271, comma 1, c.p.p. sull'inutilizzabilità delle intercettazioni effettuate in violazione delle disposizioni sull'uso degli impianti prescritti.

[33] Sulla lacunosità della disciplina codicistica in tema di intercettazioni informatiche o telematiche F. RUGGIERI, *op. cit.*, p. 163.

con cui pongono in essere le operazioni captative autorizzate, al trattamento dei dati e alla loro trasmissione all'autorità giudiziaria.

Per ridimensionare l'evidente vuoto di tutela nei confronti della sfera privata degli indagati e dei terzi, potenzialmente lesa dall'elevato numero di dati personali elaborati [34], è intervenuto il Garante per la privacy che, con il provvedimento del 15 dicembre 2005, ha impartito ai gestori per le intercettazioni nuovi accorgimenti da adottare nell'eseguire le operazioni richieste (come ad es. l'individuazione più selettiva del personale incaricato a trattare i dati, la maggior protezione dei dati per il periodo in cui essi giacciono nei *data base* dei gestori, attraverso strumenti di avanzata cifratura, l'immediata cancellazione dei dati dopo la loro comunicazione all'autorità giudiziaria, ecc.), al fine di imporre che tali operazioni avvengano nel rispetto dei diritti delle persone, anche nella fase che precede l'acquisizione dei dati da parte dell'autorità giudiziaria e che non trova disciplina nel codice di rito.

La condivisione di un *modus operandi* comune, improntato al rispetto del diritto alla privacy dei soggetti coinvolti dovrebbe, in qualche misura, garantire l'indagato sull'integrità, sull'attendibilità e soprattutto sulla genuinità dei dati a proprio carico, spesso compromessa dalla scarsa competenza tecnica degli addetti alle operazioni di intercettazione e dall'eccessiva leggerezza nella manipolazione dei dati.

Si pone, inoltre, il problema di circoscrivere l'oggetto delle intercettazioni informatiche, alla luce delle nuove tecnologie.

Come si è visto, il legislatore detta una differente disciplina con riferimento alle intercettazioni "vocali", rigorosamente normata, e alle intercettazioni di flussi telematici, che risulta disciplinata unicamente per rinvio alla prima.

Il fenomeno della convergenza tecnologica ha consentito il superamento della vecchia struttura delle telecomunicazioni, in cui ciascun servizio possedeva la sua rete di trasmissione. La piattaforma elettronica, quale canale di trasmissione dei dati, unita alla digitalizzazione dei servizi di telefonia, ha come conseguenza pratica quella di "*far apparire la vecchia telefonata come un semplice flusso informatico*", di talché, disponendo un'intercettazione telematica, soggetta, come si è visto, a parametri meno rigorosi, potrebbero captarsi dati inerenti ad una conversazione vocale, con evidenti problemi di inutilizzabilità delle informazioni così ottenute [35].

Si rendono, quindi, opportuni decreti autorizzativi delle intercettazioni, che stabiliscano le modalità delle operazioni in maniera più precisa e circoscritta, al fine di prevenire da parte delle autorità d'indagine, l'acquisizione di informazioni destinate ad essere colpite dalla sanzione dell'inutilizzabilità.

3.1. *Segue*: la distinzione fra intercettazioni informatiche o telematiche e altre attività investigative di contrasto alla pedopornografia

Nell'attività d'indagine per reati sessuali perpetrati attraverso lo strumento informatico, le

[34] I dati attengono, in particolare, all'identità dei soggetti sottoposti ad intercettazione, all'arco temporale di svolgimento dell'intercettazione e ai dati di traffico telefonico o telematico inerenti alle linee intercettate (data, ora, numero chiamato e durata della comunicazione o conversazione).

[35] Così L. LUPARIA, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 166 ss. Sempre con riferimento alla problematica dell'estensione dell'oggetto delle intercettazioni telematiche, l'autore cita come problematiche anche le c.d. "intercettazioni parametriche", che avvengono attraverso la captazione di dati per parole chiave. Questa modalità di intercettazione consente alle autorità di monitorare e filtrare tutto il traffico regionale o nazionale afferente ad un determinato *provider*, con conseguente lesione della *privacy* dei cittadini che ne utilizzano i servizi.

intercettazioni non rappresentano il mezzo di ricerca della prova più invasivo e lesivo dei diritti costituzionalmente tutelati.

Il legislatore italiano, anticipando le indicazioni fornite dalle fonti comunitarie [36], che suggeriscono forme di "investigazioni speciali"al fine di porre in essere un contrasto efficace al fenomeno, ha consentito, attraverso l'art. 14 della legge n. 269/1998, una serie di attività di indagine "*under cover*" che possono essere così sintetizzate.

La polizia postale e delle telecomunicazioni può procedere:

- all'utilizzo di indicazioni di copertura per attivare siti c.d. "civetta", diretti ad attirare eventuali pedofili [37] (art. 14, comma 2, legge n. 269 del 1998);
- all'acquisto simulato di materiale pedopornografico e alla partecipazione a relative attività di intermediazione (art. 14, comma 1, legge n. 269 del 1998);
- alla realizzazione e gestione di aree di comunicazione, quali *newsgroups* e *chatrooms*, scambio su reti o partecipazione ad esse (art. 14, comma 2, legge n. 269 del 1998).

Le intercettazioni informatiche o telematiche non vanno confuse con l'attività di contrasto, sopra descritta [38].

Nell'attività di intercettazione telematica, infatti, la polizia giudiziaria si limita ad apprendere, in tempo reale, comunicazioni che avvengono fra terzi, svolgendo un ruolo passivo, senza condizionare in alcun modo i contenuti delle conversazioni intercettate.

Nell'attività di contrasto, invece, il ruolo della polizia è attivo e si spinge fino all'incitamento alla commissione del reato, assumendo la veste di "agente provocatore" [39] sulla base, però, di una notizia di reato e di un decreto autorizzativo emanato dall'autorità giudiziaria.

L'attività di contrasto, come definita dall'art. 14 legge n. 269 del 1998 e dettagliata dalla Suprema Corte, deve essere distinta non solo dalle intercettazioni di comunicazioni, ma anche dall'attività investigativa, molto frequente nei procedimenti per reati di pedopornografia *on line*, che consiste nell'accesso da parte della polizia giudiziaria, a *files*, condivisi in rete, mediante un programma *di file sharing* [40], liberamente e gratuitamente reperibile in Internet, senza che tale accesso sia accompagnato da modalità tipiche di contrasto, quali l'acquisto simulato o l'intermediazione dei prodotti esistenti nelle cartelle condivise [41].

Per questo tipo di attività, così come per la semplice scoperta di un sito web, di carattere pedopornografico, in cui qualsiasi utente della rete, autorità o privato, può imbattersi anche occasionalmente ed accedervi mediante una *password* [42], non è necessario il ricorso allo strumento delle intercettazioni. Viceversa, potrà essere necessario procedere all'intercettazione di flussi telematici per risalire, attraverso l'indirizzo IP, all'identità dell'utente, che condivide in Rete immagini o filmati di contenuto illecito. A tal proposito, la Corte di Cassazione ha specificato che l'attività di intercettazione di comunicazioni informatiche o telematiche, regolar-

[36] V. *supra*, par. 2.

[37] Sulla problematica relativa al sequestro del materiale acquisito attraverso siti web "civetta" E. APRILE, *Limiti alla utilizzabilità processuale del sequestro di materiale informatico acquisito mediante siti web "civetta*", in *Dir. Internet*, 2005, 1, p. 39 ss.

[38] Cass., sez. III, 11 febbraio 2002, n. 5397.

[39] Cass., sez. V, 19 gennaio 2004, n. 21778; di recente Cass., sez. III, 6 ottobre 2009, n. 41743.

[40] Come ad esempio WINMIX, E-MULE, BITORRENT ecc. Sono programmi, scaricabili gratuitamente da Internet, che consentono di condividere con altri utenti cartelle o *files* e che spesso sono utilizzati per detenere e scambiare immagini pedopornografiche.

[41] Cass., sez. III, 5 febbraio 2009, n. 13729. Sulla distinzione fra accesso a *files* condivisi in rete e attività di contrasto *ex* art. 14, legge n. 269 del 1998 anche Cass., sez. V, 10 gennaio 2004, n. 21778.

[42] N. GALANTINI, *op. cit*., p. 781 ss.

mente autorizzata dall'autorità giudiziaria, comprende anche l'identificazione del soggetto che utilizzi un determinato *user name*[43].

Il decreto di cui all'art. 267 c.p.p. non autorizza, quindi, le autorità preposte solo ad avviare l'attività intercettativa, ma anche a ricavare dall'indirizzo IP le generalità dell'utente[44], attraverso una richiesta rivolta all'Internet Service Provider[45].

Se gli assegnatari di tali IP sono provider italiani, il reperimento delle informazioni avviene in modo agevole mediante il decreto di acquisizione dei *files di log*, notificato allo stesso provider. Se gli IP sono stati assegnati da fornitori di servizio Internet situati all'estero, allora tale attività verrà demandata all'Interpol.

Secondo le indicazioni comunitarie, la corretta conservazione dei dati presso gli ISP (Internet Service Provider) è un elemento di grande importanza per reprimere il fenomeno della pedopornografia *on line,* al punto che, fra le "misure appropriate di tipo volontario o coer-

[43] Cass., sez. III, 6 ottobre 2009, n. 41743.

[44] La c.d. interrogazione anagrafica. Fra le altre attività, diverse dalle intercettazioni strettamente intese, per cui l'autorità giudiziaria si avvale del supporto dei *providers*, vi sono la localizzazione dell'utenza, l'identificazione della linea chiamante o della linea connessa, il tracciamento, la sospensione o la limitazione dei servizi agli utenti, la documentazione del traffico pregresso contabilizzato e la documentazione integrale del traffico storico. Non essendo attività tipizzate dal codice di rito, pongono una serie di dubbi sul loro inquadramento nelle tradizionali categorie e conseguentemente sulla disciplina applicabile. Il problema è ancor più rilevante se si considera che, come affermato dal Garante della *privacy* nel provvedimento del 15 dicembre 2005*,* "*a differenza di quanto avviene in occasione delle conversazioni telefoniche intercettate, i fornitori hanno la possibilità di conoscere tali informazioni prodotte o raccolte nel compimento delle predette operazioni. Sono i fornitori, infatti, ad estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria, ad organizzarli in tabulati e a spedirli al richiedente. In tutte queste fasi, i dati restano nella disponibilità del fornitore e non può essere escluso che gli incaricati operanti in ambito aziendale debbano poterli conoscere, anche in parte, per svolgere alcune tra le operazioni medesime*".

Un correttivo alla questione può forse rinvenirsi nel "nuovo" comma 4-*ter* dell'art. 132 cod. privacy, secondo cui il provvedimento dell'autorità giudiziaria diretto ai *providers* "*può prevedere (…) l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi*".

[45] La disciplina della conservazione dei dati di traffico a fini investigativi è contenuta nell'art. 132 del d.lgs. 30 giugno 2003, n. 196 (cod. privacy). La norma, che fino alle recenti modifiche disciplinava solo la conservazione dei dati del traffico telefonico, disciplina attualmente anche la conservazione dei dati del traffico telematico presso i fornitori di servizi. Attraverso l'inserimento dei commi 4-*ter*, 4-*quater* e 4 *quinquies* ad opera della legge 18 marzo 2008, n. 48 di ratifica della Convenzione di Budapest, vengono stabiliti gli obblighi di conservazione e custodia dei dati da parte dei provider su ordine dell'autorità giudiziaria, che abbia bisogno dei dati per lo svolgimento delle investigazioni preventive di cui all'art. 226 disp. att. c.p.p. oppure per la repressione di specifici reati. La norma non indica quali sono i reati per cui l'autorità giudiziaria può impartire particolari ordini di conservazione e custodia. Ci si deve chiedere se tali ordini possono riguardare qualunque tipo di reato, per cui l'acquisizione di tali dati si renda necessaria oppure solo per i più gravi, fra i quali, si pensa, rientrano certamente i reati di pedopornografia *on line*. Sarebbe stata opportuna una maggior precisione del legislatore in tal senso, anche al fine di evitare forzate interpretazioni in via analogica di norme dettate per istituti diversi, come ad esempio l'art. 266 c.p.p. e un'eccessiva intrusione, da parte dell'autorità procedente, nella sfera privata dei cittadini. Ciò sarebbe stato coerente anche con le indicazioni fornite dalla Corte Costituzionale n. 372/06, secondo cui: "*la tutela del diritto alla riservatezza può subire variazioni in rapporto all'esigenza concreta … a seconda della gravità dei reati da perseguire … è sufficiente che la maggiore o minore limitazione (del diritto alla riservatezza) sia posta in rapporto con la maggiore o minore gravità attribuita dal legislatore a reati diversi, individuati secondo scelte di politica criminale … Fermo restando il criterio generale di bilanciamento in astratto, spetta al legislatore individuare specifici equilibri non manifestamente irragionevoli*".

Viene, inoltre, meno il regime "differenziato" di conservazione e di acquisizione dei dati, che il legislatore aveva previsto per i reati di cui all'art. 407, comma 2, lett. a), c.p.p., in seguito all'abrogazione dei commi 2 e 4 dell'art. 132 da parte del d.lgs. 30 maggio 2008, n. 109, in attuazione alla dir. CEE 2006/24/CE sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico.

citivo, atte ad eliminare la pornografia infantile su Internet" la Decisione 2000/375/GAI indica anche quelle mirate a sollecitare i fornitori di servizi Internet a "*conservare (...) i dati relativi a tale traffico, quando applicabile e tecnicamente fattibile – soprattutto ai fini delle azioni penali qualora si sospetti l'abuso sessuale di bambini, nonché la produzione, il trattamento e la diffusione di materiale di pornografia infantile – per il tempo eventualmente specificato dalla legislazione nazionale applicabile*[46]*, al fine di rendere tali dati disponibili per essere esaminati dalle autorità preposte all'applicazione della legge, secondo le norme procedurali applicabili*"[47].

Ancora qualche riflessione sulle operazioni di accesso a *files,* condivisi in rete, mediante un programma di *file sharing*.

I *files* sono situati sull'hard disk del computer dell'utente che li condivide mediante la tecnologia di *peer to peer* e sono visibili da tutti coloro che abbiano "scaricato" il programma[48].

I *files* possono avere contenuti leciti, come ad esempio musica o films, oppure contenuti illeciti, quali ad esempio, quelli di carattere pedopornografico.

L'utente che si imbatte, attraverso uno di questi programmi, in immagini di tal contenuto viene certamente in contatto con una notizia di reato[49].

Il privato può solo darne avviso alle autorità competenti[50], senza chiaramente poter risalire all'identità di colui che ha condiviso, divulgandoli, i contenuti illeciti.

La polizia postale, invece, non solo dovrà comunicare la notizia di reato, così acquista, al pubblico ministero, ai sensi dell'art. 347 c.p.p., ma potrà risalire anche all'identità anagrafica dell'utente, attraverso le operazioni sopra descritte, solo se regolarmente autorizzate dall'autorità giudiziaria.

A voler essere rigidamente garantisti, di fronte all'assenza di precise indicazioni legislative, sorge qualche dubbio sulla legittimità di tale attività e sull'utilizzabilità dei risultati così conseguiti, se si guarda al valore preventivo che essa può assumere.

---

[46] Nel nostro ordinamento la disciplina della conservazione dei dati di traffico telematico è contenuta nell'art. 132 del d.lgs. 30 giugno 2003, n. 196 (Cod. Privacy): i *provider* sono tenuti a conservare i dati del traffico telematico per dodici mesi dalla data della comunicazione. Su richiesta dell'autorità giudiziaria, in particolari casi indicati nel comma 4-ter dell'art. 132 Cod. Privacy, essi saranno tenuti a conservare e proteggere i dati con le modalità specificate dall'autorità stessa per un periodo non superiore a 90 giorni. Il provvedimento dell'A.G. è prorogabile per una durata massima non superiore a 6 mesi.

[47] Art. 3, lett. c), Decisione 2000/375/GAI del Consiglio del 29 maggio 2000 pubblicata in *G.U.* 9 giugno 2000, L. 138.

[48] La condivisione in Rete mediante un programma di *files sharing*, integra la condotta penalmente rilevante punita dall'art. 600-*ter*, comma 3, c.p.p. e non quella meno grave, della detenzione di materiale pedopornografico di cui all'art. 600-*quater* c.p. che è, secondo giurisprudenza costante, ipotesi residuale rispetto a tale fattispecie. Così Cass., sez. III, 7 giugno 2006, n. 20303; Cass., sez. III, 9 dicembre.2009, n. 8285.

[49] Anche questa operazione ha degli aspetti problematici, a cui si intende solo accennare. Solo alcuni programmi di *files sharing*, fra cui ad esempio e-mule, consentono una visione in "anteprima" dei *files* a cui si intende accedere, senza quindi dover procedere al "download" per vederne il contenuto. Altri programmi (come ad esempio Bitorrent), invece, non consentono la visione in anteprima del *files*, ma costringono l'utente che voglia vederne il contenuto a "scaricarlo" sul PC. In tal caso, se il contenuto del *files* ha carattere pedopornografico, potrebbe configurarsi a carico dell'utente, il reato di detenzione di materiale pornografico *ex* art. 600-*quater* c.p. Può essere il caso dell'utente curioso oppure il caso, ancor più difficile da dipanare, di colui che scarica *files* ingannato dal nome che viene loro attribuito dall'utente che li condivide e che non fanno pensare ad un contenuto illecito.

[50] Questo tipo di segnalazione deve essere inviata al Centro nazionale per il Contrasto della pedopornografia sulla Rete Internet disciplinato dall'art. 14 *bis* legge n. 269 del 1998. È stabilito un obbligo di segnalazione/denuncia, ai sensi dell'art. 14 *ter* legge n. 269 del 1998, solo a carico dei *providers*, ma non a carico dei privati.

Il disposto generale di cui all'art. 330 c.p.p. e alcune pronunce giurisprudenziali in argomento [51], non sembrano bastevoli a colmare le lacune dovute ad un legislatore che, irrispettoso della riserva di legge, non si è ancora fatto carico di disciplinare in maniera chiara e dettagliata le molteplici attività investigative, rimesse all'iniziativa della polizia giudiziaria e attuabili mediante queste nuove modalità.

L'elemento dell'extraprocessualità di tale investigazione richiama immediatamente alla mente le c.d. intercettazioni preventive, di cui all'art. 226 disp. att. c.p.p.

Di fronte alla generale tendenza al potenziamento degli strumenti di contrasto della pedopornografia *on line*, viene da chiedersi come mai il legislatore italiano non abbia inserito all'interno del testo dell'art. 226 disp. att. c.p.p., i reati di cui agli artt. 600-*ter* e 600-*quater* c.p.

Così facendo avrebbe legittimato il ricorso alle c.d. intercettazioni preventive, telefoniche e telematiche, attualmente possibili solo per "prevenire" delitti di particolare gravità, quali quelli di criminalità mafiosa e di terrorismo (art. 407, comma 2, lett. a), n. 4, anche per le ipotesi *de quibus*.

Alla luce della delicatezza dello strumento che, utilizzato in una fase extraprocedimentale e in assenza di una *notitia criminis*, si presta ad usi distorti lesivi delle fondamentali garanzie di difesa, la "svista" del legislatore non può che tranquillizzare coloro che ritengano la disciplina in materia di pedopornografia, già sufficientemente orientata in senso preventivo [52], date le previsioni dell'art. 14 legge n. 269 del 1998.

La disciplina delle intercettazioni preventive pone effettivamente una serie di problematiche dovute all'"opacità" dei controlli sulle operazioni svolte, destinata a condizionare la spendibilità dei risultati così ottenuti all'interno del processo e all'eterogenesi dei suoi fini, che la norma mal chiarisce.

Sotto questo profilo, l'attività preventiva di cui all'art. 226 disp. att. c.p.p. deve essere distinta dall'attività di contrasto prevista dal legislatore contro la pedopornografia, che appare certamente più rispettosa dei diritti dell'indagato [53].

Quest'ultima, infatti, anche alla luce dell'interpretazione giurisprudenziale dell'art. 14 legge n. 269 del 1998, rappresenta attività procedimentale nell'ambito della fase di indagine; presuppone, per il suo avvio, l'esistenza di una *notitia criminis* che si riferisca ad uno dei reati tassativamente elencati al comma 1 dell'art. 14 legge n. 269 del 1998, deve essere autorizzata dall'autorità giudiziaria e ha la finalità, ben definita dalla norma, di "*acquisire elementi di prova*" in ordine a quei reati specificamente indicati.

Si ritiene, inoltre, che per considerare compatibile il disposto di cui all'art. 14 legge n. 269 del 1998 con la riserva di legge, imposta nel nostro ordinamento dalla Carta costituziona-

[51] Cass., sez. V, 10 gennaio 2004, n. 21778, che distingue tale attività da quella di contrasto *ex* art. 14 legge n. 269 del 1998 e Cass., sez. III, 2 febbraio 1998, n. 3261 secondo cui "*è da escludere che possano essere promosse indagini preliminari non già sulla base di una notizia di reato ma al fine di eventualmente acquisirla, con indagini a tappeto ed in forma indiscriminata, dirette ad accertare se eventualmente ipotetici reati sono stati commessi. Una tale attività è consentita agli organi di polizia nell'esercizio della propria attività amministrativa di prevenzione e repressione dei reati ed in quanto è svolta al di fuori delle norme del codice di rito va effettuata sul pieno rispetto della altrui libertà, fatti salvi, ovviamente, gli specifici poteri di accertamento attribuiti da specifiche disposizioni di legge*".

[52] A. MACCHIA, *Pedofilia, quali rischi se la tutela finisce per spingersi troppo avanti*, in *Dir e giust*., 2002, 9, p. 16 ss.

[53] Tra i tanti che evidenziano i profili di garanzia dell'"attività provocatoria" introdotta dal legislatore del 1998 rispetto all'analoga disciplina prevista in materia di stupefacenti, B. ROMANO, voce *Pedofilia*, in *Dig. disc. pen.*, II, Torino, 2002, p. 627; G. MELILLO-C. MOTTA, *Linee di una possibile evoluzione normativa della figura dell'agente provocatore*, in *Arch. nuova proc. pen*., 2000, 2, p. 131 ss.

le e, ora anche dalla CEDU[54], l'elencazione delle attività di contrasto (acquisto simulato, attività di intermediazione, utilizzazione di indicazioni di copertura per attivare siti nelle reti, ecc.) in esso contenuta, debba considerarsi tassativa e non meramente esemplificativa.

Esser di diverso avviso comporterebbe legittimare, nell'ambito dell'attività investigativa di prevenzione e lotta alla pedopornografia, qualsiasi attività atipica che possa, in via interpretativa, trovare cittadinanza fra le righe della norma, in violazione della riserva di legge.

Le intercettazioni telematiche possono riguardare, oltre che il traffico IP sviluppato su linee telefoniche o collegamenti a banda larga, anche le comunicazioni di posta elettronica.

Anch'esse, infatti, sono spesso veicolo di immagini o filmati di contenuto pedopornografico e costituiscono un mezzo di collegamento fra pedofili, soprattutto se facenti parte di organizzazioni criminali, di carattere internazionale.

Fra le tecniche investigative molto usate nelle indagini per i reati di *pedopornografia on line* vi è quella che viene atecnicamente definita come "duplicazione della casella di posta elettronica".

È una particolare forma di intercettazione, che avviene mediante un inoltro automatico della corrispondenza ricevuta e spedita dall'intercettato, mediante un account di posta elettronica dato dal fornitore[55]. Tale modalità intercettativa consente alle autorità preposte di acquisire, in tempo reale, la posta in arrivo e trasmessa dal giorno di inizio delle operazioni. L'inoltro automatico può avvenire essenzialmente attraverso l'installazione di un c.d. *Trojan Hourse*[56] nel computer del soggetto la cui posta elettronica deve essere intercettata oppure attraverso la tecnica dello *sniffing*[57], che consente, attraverso la captazione dei dati che transitano nella Rete, di acquisire *login*, *passwords* e altri elementi all'insaputa del titolare.

Per dovere di completezza corre evidenziare che una parte della dottrina processual-penalistica ha avanzato delle perplessità sull'inquadramento di questa operazione nella disciplina

[54] Le recenti sentenze della Corte costituzionale n. 348 e n. 349 del 2007, n. 39 del 2008, n. 311 e n. 317 del 2009 e, da ultimo, la n. 93 del 2010, hanno determinato una sorta di "rivoluzione copernicana" nella gerarchia delle fonti del diritto, stabilendo la diretta applicabilità nel nostro ordinamento delle norme contenute nella Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali e attribuendo loro la qualifica di norme interposte, superiori alla legge ordinaria e inferiori solo alla Costituzione. *Rebus sic stantibus*, l'interpretazione non tassativa dell'art. 14 legge n. 269 del 1998, viola certamente la riserva di legge, se non con riferimento ai parametri costituzionale che tutelano la riservatezza delle comunicazioni (artt. 13, 14 e 15), con riferimento all'art. 8 CEDU. Sul punto S. MARCOLINI, *Le c.d. perquisizioni on line*, in *Cass. pen.*, 2010, 3, p. 1224 ss.

[55] D. D'AGOSTINI, *op. cit*., p. 175. È di questo avviso anche il Granate della Privacy che nel provvedimento sulla sicurezza delle intercettazioni del 15 dicembre 2005, inquadra questa attività come intercettazione informatica o telematica.

[56] Un *Trojan Horse* è un programma, costituito da una parte server, installata nel computer infetto e da una parte client residente nel computer dell'attaccante. Questa consente il controllo da remoto del computer compromesso, naturalmente all'insaputa del proprietario. L'attribuzione del termine "Cavallo di Troia" ad un programma o, comunque, ad un file eseguibile, è dovuta al fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende un *trojan*. L'utente sarà portato ad "aprirlo", poiché celato dietro a *link* apparentemente innocui e, automaticamente ad installarlo, senza sapere che, tramite questo programma, terzi possono apprendere flussi di dati diretti verso il suo IP. Sulle problematiche giuridiche legate ai c.d. *trojan* nelle indagini per reati di pedopornografia *on line*: D. DELL'ORTO, *op. cit*., p. 879 ss.

[57] "*L'attività di monitorare i pacchetti di rete che arrivano al proprio computer si chiama sniffing. Ogni sistema su una rete IP scambia informazioni con altri sistemi tramite singoli pacchetti che hanno un IP sorgente e un IP destinazione. Tipicamente un computer analizza e processa solo i pacchetti che arrivano al suo dispositivo di rete (una scheda ethernet, un modem ecc.) che hanno come IP di destinazione il proprio o che sono pacchetti di broadcast, indirizzati cioè ad ogni indirizzo IP attivo nello stesso network IP. L'attività di sniffing il più delle volte è necessaria per monitorare e diagnosticare problematiche di rete ma può essere impropriamente utilizzata per intercettare informazioni sensibili di terzi, come login e password di accesso ad un determinato servizio*".

delle intercettazioni [58], ma in assenza di precise indicazioni normative e giurisprudenziali in merito, non si vede in quale altro modo definire e, conseguentemente, disciplinare, un'attività di tal genere, che consente di intercettare la corrispondenza, attraverso la captazione in tempo reale, di un flusso informatico di dati, all'insaputa del mittente.

Per la somiglianza di tale attività in termini di risultati e di tecnologie utilizzate, si potrebbe pensare ad assimilare l'impropriamente detta "duplicazione della casella di posta elettronica" alle c.d. perquisizioni *on line*. L'osservazione, inconfutabile, che nel caso di captazione di *e-mail*, si versi nel campo delle comunicazioni strettamente intese, è argomentazione ulteriore a sostegno dell'applicabilità, a tale operazione, della disciplina delle intercettazioni di cui agli artt. 266 e ss. c.p.p. [59].

Vi sono poi altre forme di acquisizione della posta elettronica, che non devono essere confuse con le intercettazioni.

Si pensi, ad esempio, all'acquisizione successiva delle *e-mail* conservate presso il provider oppure all'apprensione dei messaggi di posta, situati sull'*hard disk* del PC dell'utente.

Le lacune che la normativa presentava con riferimento al sequestro di dati informatici (e quindi anche della posta elettronica), messe in evidenza, con preoccupazione, dalla dottrina più attenta [60], sono state, però, parzialmente colmate dalla legge di ratifica della Convenzione di Budapest [61], che ha "ritoccato" l'art. 254 c.p.p. imponendo alla polizia giudiziaria delegata al sequestro di consegnare all'autorità giudiziaria i dati senza apprenderne i contenuti e che ha disciplinato *ex novo* il sequestro dei dati informatici presso il provider, mediante l'inserimento nel codice di procedura penale dell'art. 254-*bis*.

4. Conclusioni

Il fenomeno della *pedopornografia on line* è in continua evoluzione.

Qualche dato può essere d'aiuto a chiarirne la dimensione.

Secondo il 14° Rapporto Annuale di Telefono Arcobaleno [62] solo nell'anno 2009 sono stati scoperti ben 49.393 siti pedofili in 35 diversi paesi, anche extraeuropei, di cui 3500 finanziati attraverso inserzioni pubblicitarie. Sono 7.000 in più rispetto all'anno precedente.

Ogni settimana nascono 20 nuovi gruppi pedofili nei *social-network* e sono circa 100.000 i visitatori che, mediamente, in un giorno, accedono ad un sito pedofilo [63].

L'avvento di tecnologie sempre nuove determina la nascita di nuove condotte penalmente rilevanti e di nuove modalità di perpetrazione del reato e rende, pertanto, necessario fornire al processo penale nuovi poteri, soprattutto in sede di indagine, e nuovi strumenti di contrasto che siano efficaci e idonei alla repressione di questi "nuovi" crimini.

La loro natura transnazionale rende necessaria una cooperazione fra le varie autorità, co-

[58] Così L. LUPARIA, *op. cit*., p. 171

[59] S. MARCOLINI, *op. cit*., p. 1228 ss.

[60] N. GALANTINI, *op. cit*., p. 780; F. RUGGIERI, *op. cit*., pp. 160-161. Più ampiamente con riferimento al sequestro probatorio del PC: A. CHELO MANCHIA, *Sequestro probatorio di computers: un provvedimento superato dalla tecnologia?*, in *Cass. pen*., 2005, 5, p. 1634 ss.; S. LOGLI, *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in *Cass. pen*., 2008, 7-8, p. 2952 ss.

[61] Più precisamente dall'art. 8, comma 4, legge 18 marzo 2008, n. 48

[62] È la principale Organizzazione internazionale impegnata, dal 1996, nel contrasto della pedofilia *on line* e nella lotta contro ogni nuova forma di riduzione in schiavitù dei bambini.

[63] L'indagine si è estesa anche a paesi come gli USA, la Cina, la Russia, il Giappone, l'Australia, la Corea e la Nuova Zelanda.

me suggerita anche dalle fonti comunitarie che, a livello processuale che riguardi il coordinamento in fase di indagine attraverso la condivisione di strategie investigative comuni, rispettose, in egual modo, delle garanzie procedurali minime che assistono i soggetti coinvolti.

Occorre prestare attenzione allo spostamento, a tratti preoccupante, dell'asse, nel bilanciamento fra l'interesse generale al perseguimento di reati così odiosi e la tutela delle vittime, da un lato, e il ridimensionamento dei diritti di libertà che assistono colui o colei che, ai sensi dell'art. 27 della Costituzione, non può essere considerato colpevole fino a condanna definitiva, dall'altro.

Non vi è chi non veda le immense difficoltà nel porre un solido argine al dilagare del fenomeno, attraverso misure che non solo siano efficaci rispetto al raggiungimento dell'obiettivo, ma che siano al contempo rispettose dei diritti degli indagati.

Una disciplina generale, dettata e pensata per le intercettazioni telefoniche, non sembra essere più sufficiente a disciplinare la materia.

Appare necessaria una normativa più sistematica che trovi una chiara enunciazione all'interno della sua sede naturale, ovvero il codice di rito, e che risolva legislativamente le problematiche sollevate dall'impatto delle nuove tecnologie, tenendo conto dei diritti fondamentali dell'imputato, senza lasciarsi sopraffare dalle esigenze, pur legittime, di sicurezza collettiva.

Un bel passo in avanti, in questo direzione, è stato certamente compiuto attraverso la legge di ratifica della Convenzione di Budapest sul Cybercrime, che ha modernizzato alcuni mezzi di ricerca della prova "tradizionali" adattandoli alla nuova realtà telematica e in tema di conservazione dei dati informatici che, da sempre, hanno preoccupato la dottrina per la loro intrinseca volatilità e vulnerabilità [64].

Nella lotta alla pedopornografia molto ancora c'è da fare, ma la strada da seguire è ormai tracciata, confidando in un legislatore dinamico e freddo, che si dimostri pronto ad adattare le "tattiche" investigative alle innovazioni tecnologiche e alla trasformazione dei comportamenti deviati, senza farsi eccessivamente condizionare dall'allarme sociale generato dall'"orco nero".

[64] N. GALANTINI, *op. cit*., p. 772.

CAPITOLO 7

Criminalità organizzata: tutela della privacy ed esigenza di sicurezza collettiva. Le deroghe alla tutela della privacy nelle intercettazioni finalizzate all'accertamento dei reati di criminalità organizzata di tipo mafioso

di *Domenico Raschellà*

1. Premessa

Già in tempi ormai remoti autorevole dottrina individuava la necessaria correlazione tra l'evoluzione ed il progresso tecnologico, economico e sociale e la sempre maggiore fragilità delle difese inerenti la sfera della vita privata del cittadino [1].

Tale correlazione, ad avviso del sottoscritto, pare appropriata, infatti, la scoperta di nuovi strumenti tecnologici e i vari mezzi di comunicazione di massa consentono di carpire aspetti della vita privata dell'individuo e diffonderli in un brevissimo lasso di tempo.

Il riconoscimento del diritto alla riservatezza nell'ordinamento giuridico italiano è frutto di una lenta evoluzione dottrinale, giurisprudenziale e normativa, che, specialmente nell'ultimo decennio, si è svolta parallelamente ad un approfondimento della sua tutela a livello europeo.

In Italia una disciplina sistematica attinente alla tutela dei dati personali si è avuta solo a seguito dell'attuazione della direttiva CE 46/95 che ha portato all'emanazione della legge n. 675 del 1996 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), ora confluita nel d.lgs. n. 196/2003 – Codice in materia di protezione dei dati personali [2].

L'evoluzione normativa è frutto anche della maggiore attenzione che alcuni studiosi hanno dedicato al diritto alla riservatezza durante la metà degli anni cinquanta. La giurisprudenza, accompagnata dalla riflessione dottrinale, ricollegava il diritto alla riservatezza all'art. 2 della Costituzione quale norma a carattere aperto che garantiva i diritti inviolabili dell'uomo [3].

[1] F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, p. 1080.

[2] A. DI MARTINO, voce *Riservatezza*, in *Enc. dir.*, XIII, Milano, 2008, p. 643.

[3] G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali*, Milano, 2004, p. 11 ss.

La Corte costituzionale ha tuttavia ridimensionato la tesi dell'art. 2 Cost. come clausola aperta cercando di tutelare altri diritti costituzionalmente garantiti e meritevoli di tutela, segnatamente la libertà di manifestazione del pensiero.

Dagli anni '60, la stessa Corte ha espressamente fatto riferimento al diritto alla riservatezza, lo ha individuato quale limite al diritto alla manifestazione del pensiero [4] e in materia di intercettazioni telefoniche, che qui più ci interessa, il diritto alla riservatezza è stato posto in contrapposizione all'interesse pubblico alla repressione dei reati [5].

La stessa Corte ha, quindi, posto in contrapposizione il diritto alla riservatezza con l'esigenza di sicurezza e repressione dei reati.

Invero, proprio quando i reati diventano più cruenti e gravi, quanto la comunità e lo Stato nulla possono contro un certo tipo di criminalità, quanto la tutela di alcune garanzie potrebbe pregiudicare la sicurezza dell'intera collettività e l'efficienza delle indagini, l'utilizzo di strumenti invasivi e la conseguente limitazione della tutela e delle garanzie individuali paiono indispensabili.

Il legislatore italiano, già nel passato, sulla scia dell'emergenza sorta dal proliferare della criminalità organizzata di tipo terroristico e mafioso, ha promulgato norme a discapito delle garanzie individuali ed espressamente rivolte al contrasto di particolari forme di criminalità.

Stante la forte incisività che le intercettazioni telefoniche e ambientali hanno nel diritto alla privacy degli "*intercettati*", il presente lavoro, lungi dal volere essere esaustivo, è volto ad individuare alcune peculiarità in tema di intercettazioni telefoniche ed ambientali quando, le indagini riguardano reati di criminalità organizzata e quanto il soggetto da intercettare appartiene alle organizzazioni predette e si trova nello status di latitante.

2. Criminalità organizzata e tutela della privacy: il problema definitorio

Il processo penale relativo ai delitti che sono tipica manifestazione della criminalità organizzata presenta rispetto a quello ordinario delle indubbie peculiarità, tanto da giustificare l'affermazione *doppio binario* che intende rimarcare le diversità esistenti tra il processo penale ordinario e quello relativo ai reati di criminalità organizzata.

Tuttavia, un preliminare problema da affrontare riguarda la definizione di delitti di criminalità organizzata, stante l'assenza di una chiara definizione legislativa [6] e le forti deroghe di

[4] Corte cost., sent. nn. 122 del 1970, 2 del 1972, 34 del 1973.

[5] Corte cost., sent. nn. 366 del 1991, 81 del 1993, 63 del /1994, 281 del 1998. Per maggiori approfondimenti relativi all'evoluzione della tutela del diritto alla riservatezza e alla privacy si veda: A. BALDASSARE *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974; G. BUSIA, *Riservatezza*, in *Dig. disc. pubbl.*, Agg., I, Torino, 2002, p. 476 ss.; A. CERRI, *Riservatezza III) Diritto Costituzionale*, in *Enc. giur. Treccani*, XXVII, Agg., 1995, Roma, p. 1 ss.; A. DI MATTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, in S. PANUNZIO (a cura di), *I diritti fondamentali e le Corti in Europa*, Napoli, 2005, p. 365 ss.; M.G. LOSANO, *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001; F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali*, Milano, 2004; D. CALDIROLA, *il diritto alla riservatezza*, Padova, 2006.

[6] A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 82. A livello legislativo il termine "criminalità organizzata" sembra essere emerso per la prima volta espressamente, nell'art. 14 d.l. 15 dicembre 1979, n. 625 (convertito nella legge 6 febbraio 1980, n. 15) che, modificando il comma 3 dell'art. 340 c.p.p. abrogato permise al P.M. di delegare alla polizia giudiziaria l'esame di corrispondenza, atti e documenti presso banche, e il relativo sequestro, purché le indagini riguardassero certi reati; fra i quali appunto quelli di criminalità organizzata. L'espressione, peraltro, era stata già da tempo adottata nel linguaggio della giurisprudenza con riferimento alle misure di prevenzione, nell'area di operatività della legge 27 dicembre 1956, n. 1423 (cfr. Cass.,

diritti costituzionalmente garantiti, tra cui il diritto alla riservatezza, quando il reato è ascrivibile alla nozione di delitto di criminalità organizzata.

Nel corso degli anni, in dottrina si sono sviluppate diverse interpretazioni del termine criminalità organizzata; spesso contrastanti.

Una **prima tesi** partendo dal riferimento ai delitti di criminalità organizzata contenuto nell'art. 2, n. 48 della legge delega al codice di procedura penale[7], ha interpretato la disposizione attuativa ravvisando il collegamento con l'art. 407, comma 2, lett. a), c.p.p. ed individuando nell'elenco ivi specificato i reati di criminalità organizzata[8].

Tuttavia, le modifiche subite dall'art. 407 c.p.p. hanno fatto naufragare lo sforzo di cercare un'accettabile nozione di delitti di criminalità organizzata rinviando al predetto articolo che, oggi, menziona delitti che possono essere ascritti alle associazioni criminali e altri che nulla c'entrano con il crimine organizzato.

Altra dottrina ha sostenuto che i delitti di criminalità organizzata possono ricomprendersi in tre categorie: i delitti di competenza delle DDA e della DNA, i reati per cui la Procura Generale presso la Corte d'appello può esercitare il potere di avocazione, tutti i restanti reati contemplati nell'art. 407, comma 2, lett. a), c.p.p., per i quali il Procuratore generale presso la Corte d'appello ha un potere di coordinamento senza possibilità di avocazione[9].

Una conclusione del genere non pare appagante, poiché il novero dei delitti di criminalità organizzata comprenderebbe così alcuni delitti (l'omicidio, la rapina, l'estorsione) che possono si essere manifestazione di criminalità organizzata, ma che hanno una tale diffusione da essere spesso frutto di "*criminalità disorganizzata*"[10]. Fondare quindi l'applicazione di una

sez. I, 17 gennaio 1968, Chirco), mentre, a seguito dell'introduzione dell'art. 416-*bis* c.p. (in forza dell'art. 13 della legge 13 settembre 1982, n. 646), il lessico precedentemente utilizzato anche per designare le caratteristiche dei reati di associazione per delinquere di cui all'art. 416 c.p. (Cass., sez. II, 26 novembre 1984 Mantegna) e di sequestro di persona a scopo di estorsione (Cass., sez. II, 29 aprile 1986 Cocuzza), subì un ulteriore processo di definizione (ma non di corrispondente delimitazione) in conseguenza dell'aggiunta dell'attributo di tipo mafioso. Successivamente, l'art. 4 del d.l. 10 luglio 1987, n. 272, nel modificare, ancora una volta, l'art. 340, ult. comma, c.p.p., aggiungeva ai reati in ordine ai quali era consentita la delegazione ad ufficiali o agenti di polizia giudiziaria, per procedere al sequestro presso banche, il delitto di cui all'art. 630 c.p. già considerato, peraltro, dalla giurisprudenza come delitto di criminalità organizzata. Inoltre il termine criminalità organizzata prima dell'entrata in vigore del nuovo codice è stato riscontrato anche nell'art. 13, comma 2, legge 10 ottobre 1986, n. 663 ("*Modifiche alla legge sull'ordinamento penitenziario e sulla esecuzione delle misure privative e limitative della libertà*"), la quale stabiliva che: la detenzione domiciliare non può essere concessa quando è accertata l'attualità di collegamenti del condannato con la criminalità organizzata.

[7] L'espressione criminalità organizzata emerge nella legislatura IX, più in particolare, nella seduta dell'Assemblea della Camera del 18 luglio 1984 fu approvato un emendamento destinato a divenire poi la direttiva n. 48 della legge-delega, che prevedeva la possibilità di concludere le indagini preliminari entro due anni in caso di processi di criminalità organizzata.

[8] G. CONSO, *La criminalità organizzata nel linguaggio del legislatore*, in *Giust. pen*., 1992, III, c. 385 ss.

[9] Da considerare che attualmente per via del d.l. 18 ottobre 2001 n. 374 convertito in legge 15 dicembre 2001, n. 438 modificativo dell'art. 51 c.p.p., comma 3-*quater*; è stata attribuita all'ufficio della procura presso il tribunale capoluogo del distretto la potestà di investigare i delitti consumati o tentati con finalità di terrorismo. Il potere di avocazione del procuratore generale presso la corte d'appello è disciplinato dall'art. 372 c.p.p. ove sono elencati una serie di delitti.

[10] Infatti l'art. 407, comma 2, lett. a), c.p.p. fa riferimento agli artt. 575 c.p. (omicidio), 628, comma 3 c.p. (Rapina aggravata), 629, comma 2, c.p. (Estorsione aggravata), art. 630 c.p. (sequestro di persona a scopo di estorsione). Inoltre altri delitti sono oggi contemplati nell'art. 407, comma 2, lett. a) che possono essere manifestazione di criminalità organizzata oppure no, sono i delitti previsti dagli artt.: 600 (Riduzione o mantenimento in schiavitù o in servitù), 600-*bis*, comma 1 (Prostituzione minorile), 600-*ter*, comma 1 (Pornografia minorile), 601 (Tratta di persone), 602 (Acquisto e alienazione di schiavi), 609-*bis* (Violenza sessuale) nelle ipotesi aggravate previste dall'art. 609-*ter* (Circostanze aggravanti della violenza sessuale), 609-*quater* (Atti sessuali con mino-

normativa piuttosto che di un'altra, sulla base di una nozione desunta da una esegesi che conduce a risultati cosi contrastanti con la realtà e con l'esperienza quotidiana non sembra possibile.

Altra tesi ricostruisce la materia su basi diverse; **partendo dal particolare istituto dell'avocazione** [11].

Se infatti, l'esigenza di rendere effettivo il collegamento e coordinamento delle indagini è un obbiettivo primario che il legislatore persegue nel caso dei delitti intesi come manifestazione del crimine organizzato, l'avocazione è l'istituto predisposto a tale esigenza; la sua previsione in ordine a determinati delitti vale come possibile guida normativa per l'individuazione dei reati di criminalità organizzata.

Nel senso che i delitti indicati nell'art. 51, comma 3-*bis*, c.p.p., per i quali è possibile l'avocazione da parte del Procuratore Nazionale Antimafia a norma dell'art. 371-*bis* c.p.p., sono espressione dei delitti di criminalità organizzata di tipo mafioso; mentre quelli previsti nell'art. 372, comma 1-*bis*, c.p.p., per i quali è prevista l'avocazione da parte del Procuratore generale presso la Corte d'appello, rappresentano i delitti di criminalità organizzata eversiva o comune [12].

Altro autore sviluppa un attenta classificazione partendo dai reati di cui all'art. 407, comma 2, lett. a), c.p.p. [13] e suddivide, predetti reati in: un primo gruppo di delitti definiti di "***grave allarme sociale***", indicati dall'art. 407, comma 2, lett. a), c.p.p., per i quali il legislatore presume la complessità delle indagini, tanto dall'aver esteso la loro durata fino a due anni. Il secondo gruppo è previsto dall'art. 372 c.p.p. [14]; il cui comma 1-*bis* contempla una parte dei delitti di grave allarme sociale, precisamente quelli che presuppongono un livello relativamente alto di organizzazione criminale. Isolando tali delitti, li definisce complessivamente delitti tipicamente riconducibili a organizzazioni criminali di tipo comune o eversivo o delitti organizzati comuni [15].

renni), 609-*octies* (Violenza sessuale di gruppo) del codice penale. Da ultimo l'art. 1, legge 15 luglio 2009, n. 94 ha inserito tra i reati di cui all'art. 407 c.p.p. quelli previsti dall'art. 12, comma 3 (Immigrazione clandestina) del testo unico di cui al d.lgs. 25 luglio 1998, n. 286.

[11] La locuzione delitti di criminalità organizzata si ritrova, tra le diverse norme, anche nelle seguenti: nell'art. 274, lett. c), c.p.p. in relazione alle esigenze cautelari quando vi è il concreto pericolo che l'imputato commetta delitti di criminalità organizzata; nella norma che disciplina la non operatività della sospensione dei termini delle indagini preliminari nei procedimenti per reati di criminalità organizzata (art. 240-*bis* disp.att. c.p.p. e art. 21-*bis*, d.l. 8 giugno 1992, n. 306); la locuzione ricorre anche nel processo penale a carico di imputati minorenni ove nell'art. 37, comma 2, d.p.r. 22 settembre 1998, n. 448 in tema di applicazione provvisoria di misure di sicurezza, si richiamano i gravi delitti di criminalità organizzata, l'art. 13 del d.l. 13 maggio 1991, n. 152 che prevede uno specifico regime per le intercettazioni telefoniche e ambientali, l'art. 1 d.l. 31 maggio 1991, n. 164 convertito con modifiche dalla legge 22 luglio 1991, n. 221 individua un presupposto per lo scioglimento dei consigli comunali e provinciali nei collegamenti diretti o indiretti degli amministratori con la criminalità organizzata, l'art. 4-*bis* ordinamento penitenziario in relazione alla concedibilità di benefici penitenziari, l'art. 18-*bis* ordinamento penitenziario disciplina i colloqui investigativi richiama i delitti di criminalità organizzata.

[12] P.L. VIGNA, *Le nuove indagini preliminari nei procedimenti per i delitti di criminalità organizzata*, in AA.VV., *Processo penale e criminalità organizzata*, a cura di V. GREVI, Bari, 1983, p. 75.

[13] G. TURONE, *Le indagini collegate nel nuovo c.p.p.*, Milano, 1992, p. 50 ss.

[14] L'art. 372 c.p.p. è stato modificato dal d.l. 9 settembre 1991, n. 292 e dal d.l. 20 novembre 1991, n. 356 convertiti rispettivamente in legge 8 novembre 1991, n. 356 e 20 gennaio 1992, n. 8.

[15] I delitti contemplati dall'art. 372, comma 1-*bis* sono: associazione con finalità di terrorismo e di eversione; attentato per finalità terroristiche o eversive; devastazione, saccheggio e strage; guerra civile; sequestro di persona a scopo di terrorismo e di eversione; cospirazione politica mediante associazione; banda armata; associazione per delinquere nei casi in cui sia obbligatorio l'arresto in flagranza; strage.

Il terzo gruppo è quello previsto dal codice di procedura penale nell'art. 51, comma 3-*bis*, c.p.p. che individua i delitti organizzati mafiosi [16].

Taluno ritiene, invece, che sia necessario limitare la categoria concettuale delitti di criminalità organizzata ai **fenomeni criminosi più rilevanti** sul piano della capacità di condizionamento dell'economia e dell'impresa [17] senza arenarsi in vincoli normativi quali l'art. 407 o 372, comma 1-*bis*, c.p.p.

Infatti, l'una e l'altra delle citate disposizioni, hanno di mira l'enucleazione delle ipotesi delittuose per le quali sussistono esigenze di coordinamento delle indagini [18]. È però necessario distinguere le strutture organizzate rudimentali, idonee alla realizzazione degli atti delittuosi pianificati dal gruppo, dai fenomeni criminali connotati dalla dotazione di apparati organizzativi finalizzati sistematicamente alla produzione ed all'investimento di ricchezza penalmente illecita, vale a dire le forme delinquenziali associative individuate dall'ulteriore comune denominatore della ricerca e del controllo di aree di mercato illegale secondo criteri quasi aziendali. Conseguentemente, le indagini concernenti strutture organizzate, stabilmente e secondo qualificate dimensioni, in funzione del commercio illecito di stupefacenti ovvero di armi o con altri scopi idonei a influenzare l'economia pubblica possono essere definiti come indagini inerenti delitti di criminalità organizzata.

Pertanto, l'area dei delitti di criminalità organizzata rimarrebbe limitata ad una significativa dimensione imprenditoriale escludendo così le aggregazioni criminali occasionali e rudimentali.

Altro autore, in contrapposizione al precedente, afferma l'appartenenza alla categoria dei "*delitti di criminalità organizzata*" di **tutti i delitti associativi**, dei reati che rappresentano l'attuazione del fine associativo e di quelli pur integranti soltanto una fattispecie concorsuale personale, ma implicanti l'esistenza di un'organizzazione [19].

Altri ancora, adottando un **criterio soggettivo**, ritengono che i delitti di criminalità organizzata comprendano tutti i reati che necessariamente presuppongono l'esistenza di un livello alto di **capacità criminale di chi ne è responsabile** [20] e, ancora, c'è chi sostiene che, tutte le ipotesi di concorso di persone nel reato allorquando vi sia comunque una suddivisone di compiti al fine di collaborare al raggiungimento del medesimo obiettivo antigiuridico, siano configurabili come delitti di criminalità organizzata [21].

Le tesi maggiormente restrittive sarebbero da condividere, o forse sono imposte dalla stessa Carta Costituzionale, quando si tende ad applicare le forti deroghe prevista dall'art. 13

[16] G. TURONE, *Le indagini collegate nel nuovo c.p.p.*, cit., p. 52. La classificazione dell'autore è accolta anche da L. FERRAJOLI, *Il coordinamento delle indagini nei procedimenti per delitti di criminalità organizzata*, in AA.VV., *Mafia e criminalità organizzata*, Torino, 1995, p. 479.

[17] G. MELILLO, *La ricerca della prova fra clausole generali e garanzie costituzionali: il caso della disciplina delle intercettazioni nei procedimenti relativi a delitti di criminalità organizzata*, in *Cass. pen*., 1997, p. 3522.

[18] Sulle scelte normative in tema di connessione e coordinamento delle indagini preliminari cfr. L. FERRAJOLI, *Il coordinamento delle indagini nei delitti di criminalità organizzata*, cit., p. 539 ss., G. TURONE, *Le indagini collegate nel nuovo codice di procedura penale*, cit., p. 1 ss., G. TURONE, *Il delitto di associazione mafiosa*, Milano, 1995, p. 387 ss., C. TAORMINA, *Spunti per una procedura differenziata in materia di criminalità organizzata*, in *Giust. pen*., 1991, III, c. 129 ss.

[19] C. TAORMINA, *op. cit*., c. 129 ss.

[20] A. SPATARO, *Le intercettazioni telefoniche: problemi operativi e processuali*, in *Corso di aggiornamento sulle tecniche di indagine "Giovanni Falcone"*, in *Quad. CSM*, 1994, 69, I, p. 137.

[21] D. MANZIONE, *Una normativa di emergenza per la lotta alla criminalità organizzata e la trasparenza e il buon andamento dell'attività amministrativa (d.l. n. 152 del 91 e l. n. 203 del 91): uno sguardo d'insieme*, in *Legisl. pen*., 1992, p. 852.

del d.l. n. 152 del 1991 alla disciplina delle intercettazioni, considerato che, la norma speciale comprime il diritto inviolabile alla libertà e segretezza delle comunicazioni e quindi il diritto alla privacy.

Propendendo per la soluzione più restrittiva, i delitti di criminalità organizzata sarebbero quelli indicati nell'art. 51, comma 3-*bis*, c.p.p., a cui fanno riferimento gli artt. 54-*ter* e 371-*bis* c.p.p.[22]. Si deve, quindi, guardare solo ed esclusivamente ai delitti previsti dall'art. 51, comma 3-*bis*[23] e per quanto concerne i reati di criminalità organizzata terroristica all'art. 51, c. 3-*quater* e 372, comma 1-*bis*, c.p.p.

Tuttavia, delle osservazioni riguardo le tesi su esposte paiono necessarie.

In primo luogo, alcuni reati previsti dall'art. 372, comma 1-*bis*, c.p.p., sono molto lontani dal significato comune di criminalità organizzata; per fare un esempio, il delitto di ***strage***: ove compiere "*al fine di uccidere … atti tali da porre in pericolo la pubblica incolumità*" (art. 422 c.p.) non comporta necessariamente che si disponga di moduli organizzativi complessi e tendenzialmente stabili; basta uno psicopatico, che sappia maneggiare armi o esplosivi.

Inoltre, pur riferendoci quando parliamo di delitti di criminalità organizzata al solo art. 51, comma 3-*bis*, c.p.p., affermando quindi una tesi maggiormente restrittiva e selettiva rispetto alle altre esposte, non si risolve l'amplia formulazione dell'articolo che considera i delitti commessi avvalendosi delle condizioni previste dall'art. 416-*bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo. Si tratta, in effetti, di una "*breccia*" attraverso la quale potrebbero passare numerose ipotesi di reato. In altri termini, nemmeno l'art. 51, comma 3-*bis*, c.p.p. sembra essere costruito in termini tassativi e dettagliati[24].

La giurisprudenza, dal canto suo, ha avuto diverse occasioni per tentare di chiarire il termine criminalità organizzata, spesso, proprio a proposito dell'applicazione della normativa speciale in tema di intercettazioni, ma pare non aver trovato comunque un equilibrio.

Un primo orientamento**,** maggiormente restrittivo, ritiene che, nel vigente ordinamento l'espressione delitti di criminalità organizzata ha un significato ben preciso che tende ad individuare non una fattispecie autonoma, ma una categoria di reati definita chiaramente attraverso l'analitica individuazione delle fattispecie fatta dagli artt. 407, comma 2, lett. a), l'art. 372, comma 1-*bis*, l'art. 51, comma 3-*bis*, c.p.p.[25].

---

[22] A. CAMON, *op. cit*., p. 79 ss.; O. LUPACCHINI, *La definizione legislativa di criminalità organizzata*, in *Giust. pen*., 1992, I, p. 183; G. CONSO, *op. cit*., pp. 386-392.

[23] In questo senso esplicitamente O. LUPACCHINI, *op. cit*., p. 183 ss., ma sembra orientato nella stessa direzione R. ORLANDI, *Il procedimento penale per fatti di criminalità organizzata dal maxi-processo al grande processo*, in G. GIOSTRA-G. INSOLERA (a cura di), *Lotta alla criminalità organizzata: gli strumenti normativi*, Milano, 1995, p. 88.

[24] A. CAMON, *op. cit*., p. 87. Secondo V. BORRACCIETTI, *Criminalità organizzata e funzioni del pubblico ministero*, in G. GIOSTRA-G. INSOLERA (a cura di), *Lotta alla criminalità organizzata*, cit., p. 105 "*la categoria è talmente vasta che potrebbe rientrarvi qualsiasi reato*"; confronta anche R. ORLANDI, *op. cit*., p. 88, nota 15.

[25] In motivazione si legge che "*il riferimento ai delitti di criminalità organizzata, poiché incide sui provvedimenti limitativi della libertà personale è tassativo e non può andare oltre le ipotesi espressamente previste. Sicuramente tra tali delitti non rientra quello previsto dall'art. 73 d.p.r. 9 ottobre 1990, n. 309 e di conseguenza non si estende a tale reato il regime particolare per l'autorizzazione di intercettazioni telefoniche, introdotto con l'art. 13 del d.l. 152 del 1991 convertito in l. 12 luglio 1991, n. 203; tuttavia l'intercettazione deve ritenersi legittimamente disposta, e perciò utilizzabile a fine di prova, quando sia stata autorizzata con riferimento ad un'ipotesi delittuosa rientrante nella categoria dei reati di criminalità organizzata ed all'esito dell'istruttoria l'azione penale venga esercitata per la violazione dell'art. 73 d.p.r. 9.10.1990, n. 309*". Vedi sul punto Cass., sez. VI, 27 maggio 1995, Galvanin, in *Cass. pen*., 1996, p. 998. Non risultano precedenti con riferimento particolare al significato della espressione "*delitti di criminalità organizzata*".

In senso contrario, ***altro orientamento***, ha affermato che nella nozione di "*criminalità organizzata*" devono farsi rientrare le attività criminose più diverse, purché realizzate da una pluralità di soggetti i quali, per la commissione di reati, abbiano costituito un apparato organizzativo [26], la cui struttura assume un ruolo preminente rispetto ai singoli partecipanti. Non può, invece, accettarsi un'interpretazione restrittiva che intenda circoscrivere la categoria dei reati di criminalità organizzata nei ristretti confini di cui agli artt. 407, comma 2, lett. a), 372 comma 1-*bis*, 51 comma 3-*bis* c.p.p.; un interpretazione di tal genere, infatti, contrasterebbe con il dato letterale della norma in tema di intercettazioni e, soprattutto, con la *ratio* della deroga [27].

In altre pronunce, la Suprema Corte di Cassazione ha statuito che la nozione "*criminalità organizzata*" resta rigorosamente ancorata a criteri sociologici e criminologici che sono in grado di definire con sufficiente specificità i reati in esame. Il concetto criminalità organizzata comprende le attività criminose più diverse, purché realizzate da una pluralità di soggetti che, per la commissione di più reati, abbiano costituito un apparato organizzativo, quindi, in cui la struttura organizzata assume ruolo preminente rispetto ai singoli partecipanti [28].

In **conclusione**, pare potersi dedurre che, nella gran parte dei casi, la giurisprudenza è orientata a far rientrare nel concetto di criminalità organizzata le attività criminose di qualsiasi tipo, purché realizzate da una pluralità di soggetti dotati di un apparato organizzato appositamente costituito per la commissione di più reati [29].

Da questa ricostruzione della dottrina e della giurisprudenza è evidente che non esiste un concetto chiaro, tassativo e determinato di delitti di criminalità organizzata, alcune volte si tende ad ampliare il concetto comprendendo diverse tipologie di delitti ed altre volte, ma con minore ricorrenza, si tenta invece di vincolarlo con specifici riferimenti normativi contenuti nel codice.

Guardando infine alla prospettiva criminologica e/o sociologica vengono richiesti, al fine del positivo riconoscimento di un fenomeno di criminalità organizzata, requisiti ulteriori rispetto ad una semplice attività criminale realizzata in forma associativa e sia pure finalizzata ad obiettivi di profitto illecito dei singoli protagonisti. Tuttavia, la definizione acquisita in tali scienze non è certo adeguata al mondo del diritto, soprattutto quando si cerca tassatività [30].

[26] Cass., sez. VI, 25 novembre 2003, Matarrelli, in *Guida dir*., 2004, 17, p. 95.

[27] Deroga che è riconoscibilmente volta a concedere più incisivi strumenti di indagine, quando l'ipotesi di accusa comprenda delitti che, per la modalità di commissione, per il coinvolgimento di più persone, per il presupposto organizzativo che li caratterizza, appaiono potenzialmente e particolarmente destabilizzanti dell'ordine sociale vedi: Cass., sez. V, 20 ottobre 2003, n. 46221, Altamura, in *Guida dir*., 2004, 10, p. 98.

[28] Cass., sez. VI, 7 gennaio 1997, n. 7, Pacini Battaglia, in Cass. pen., 1997, p. 1930; Cass., sez. I, 13 luglio 1998, Ingrosso, in *Mass. uff.* 211167 e in *Giust. pen*., 1999, III, p.360; Cass., sez. I, 27 gennaio 2005, p.g. in proc. Tomasi, in *Mass. uff.* 230454 e in *Ind. pen*., 2006, 1, p.133.

[29] Cass., sez. VI, 4 marzo 1997, Pacini Battaglia, cit., p.344, con nota di CARMONA; Cass. pen., sez. I, 2 luglio 1998, n. 3972; Cass. pen., sez. V, 20 ottobre 2003, n. 46221, in Cass. pen., 2005, 2, p. 521; Cass. pen., sez. I, 20 dicembre 2004, n. 2612, in *CED Cass*., 2005, RV230454; Cass. pen., sez. un., 22 marzo 2005, n. 17706, in *CED Cass*., 2005, RV230895.

[30] G. FIANDACA, *Criminalità organizzata e controllo penale*, in *Ind. pen*., 1991, p. 25 ss.; M. MADDALENA, *I problemi pratici nelle inchieste di criminalità organizzata nel nuovo processo penale*, in AA.VV., *Processo penale e criminalità organizzata* (a cura di GREVI), Bari, 1993, pp. 79-83.

3. Le deroghe alle garanzie individuali in tema di intercettazioni telefoniche, ambientali e preventive

Come noto le intercettazioni telefoniche hanno un'alta capacità invasiva nella sfera individuale dei soggetti e ledono gravemente la privacy degli intercettati.

Sicuramente, una forte incidenza di tale strumento d'indagine in Italia si ha anche per la diffusione numerica-quantitativa che certamente deriva anche dalla necessità di contrastare forme di criminalità organizzata non presente in altri stati.

Riguardo alle intercettazioni telefoniche, per meglio comprendere la valenza delle deroghe vigenti, ad avviso di chi scrive, è necessaria una breve premessa storica.

Le intercettazioni sono uno strumento utilizzato spesso per la ricerca della prova e, già in passato, il largo utilizzo ha costituito oggetto di dispute, in quanto, originariamente il codice di procedura penale del 1930 ammetteva intercettazioni illimitate a disposizione della P.G.

Dopo l'approvazione della Carta Costituzionale, l'art. 15 Cost. non permetteva più detta disciplina, richiedendo provvedimenti motivati da parte dell'autorità giudiziaria per poter limitare la segretezza delle comunicazioni; pertanto, un primo intervento di interpolazione si verificava nel 1955 con legge n. 517 che, imponeva un intervento autorizzativo dell'autorità giudiziaria più vicina [31].

Con la successiva legge n. 98 del 1974, oltre al provvedimento motivato dell'autorità giudiziaria, furono imposti limiti oggettivi e di durata alle intercettazioni telefoniche, comunque, meno stringenti per i reati gravi rispetto ai quali appariva giustificata l'invadenza della privacy del cittadino [32].

In seguito, la ricerca di maggiore tutela dell'inviolabilità e segretezza delle comunicazioni, non solo sotto il profilo di riserva di giurisdizione ma anche sotto quello di riserva di legge, sancita dall'art. 15 della Costituzione e dall'art. 8 CEDU, hanno imposto l'adozione del criterio interpretativo secondo cui nella materia *de qua* tutto ciò che non è previsto non è consentito [33].

Prendendo atto di dette fonti, il Parlamento nel delegare il Governo per l'emanazione del nuovo codice di procedura penale ha imposto una serie di direttive piuttosto dettagliate [34].

La scoperta poi di mezzi della tecnica sempre più incisivi della sfera privata del cittadino consente oggi la **simultanea esistenza di diverse tipologie di intercettazioni**: l'intercettazione vera e propria (art. 266 c.p.p.), intesa come ascolto delle comunicazioni, l'intercettazione del flusso di informazioni relativo ai sistemi informatici o telematici (art. 266-*bis* c.p.p.), l'intercettazione per rintracciare il latitante (artt. 295, comma 3 e 3-*bis* c.p.p.), le intercettazioni preventive (art. 226 disp. att. c.p.p.) [35].

---

[31] F. CORDERO, *Procedura penale*, Milano, 2001, p. 848; cfr. art. 7 legge n. 517 del 1955.

[32] M. PISANI-A. MOLARI-V. PERCHINUNNO-P. CORSO, *Manuale di diritto processuale*, Bologna, 2004, p. 246.

[33] F. DINACCI, *L'irrilevanza processuale delle registrazioni di conversazioni tra presenti*, in *Giur. it*., 1994, p. 67; F. CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. proc. pen*., 1991, p. 157; A. PACE, *Art. 15*, in *Comm. della Cost. Branca*, Bologna-Roma, 1977, p. 90; su posizioni parzialmente differenti, L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, pp. 28-42; A. CAMON, *op. cit*., p. 34.

[34] Dalla legge delega si ricavano una serie di direttive, sia in ordine al profilo della legittimazione a disporre le operazioni di captazione (art. 2, n. 37), sia in ordine alla specifica determinazione degli altri principi di garanzia; cui si è dovuto necessariamente attenere il legislatore delegato (art. 2, n. 41).

La dettagliata disciplina concernente le intercettazioni prevista dagli artt. 266-271 c.p.p. deriva dallo sviluppo storico sopra specificato. V. GREVI, *Le prove* in G. CONSO-V. GREVI, *Compendio di procedura penale*, Padova, 1996, p. 358.

[35] F.P. GIORDANO, *Le indagini preliminari*, Padova, 2002, p. 347.

La disciplina delle intercettazioni, analiticamente prevista dal nuovo codice di procedura penale, subiva profonde modifiche nel 1992 per via del dichiarato intento legislativo orientato a facilitare la "*caccia ai latitanti*" nei reati di mafia. Venne, quindi, disposta un'estensione nell'uso dello strumento delle intercettazioni per alcune tipologie di reati e la normativa risulta ancora vigente e consolidata nel nostro ordinamento [36].

Tanto premesso, si evince come, negli anni passati, il legislatore ha previsto delle garanzie riguardo alle intercettazioni grazie all'aumento della sensibilità inerente la tutela della privacy, ma ha, contemporaneamente, derogato le stesse quando le indagini riguardavano reati gravi.

La normativa vigente, pur avendo perfezionato e concretamente attuato il sistema delle garanzie individuali, ha disposto specifiche deroghe riguardanti i gravi reati di criminalità organizzata.

Una prima deroga alla disciplina ordinaria delle intercettazioni e ravvisabile nei presupposti richiesti per disporle quando le indagini riguardano delitti di criminalità organizzata o di minaccia col mezzo del telefono [37].

Gli indizi da "***gravi***" sono degradati a "***sufficienti***", e l'intercettazione non deve essere più "***assolutamente indispensabile per la prosecuzione delle indagini***" ma semplicemente "***necessaria per lo svolgimento delle indagini***" [38].

In concreto, si è attuato un arretramento delle garanzie determinato dai periodi di emergenza vissuti nella lotta alla criminalità organizzata; taluno ha saggiamente sostenuto che è naturale potenziare i mezzi di investigazione che hanno dato i risultati migliori nel contrasto al crimine quando aumenta l'allarme sociale [39].

Dal punto di vista tecnico, tracciare un ***confine tra "gravi indizi" e "sufficienti indizi"*** è impossibile, ma il senso della norma è chiaro, invita i magistrati a non farsi troppi scrupoli nell'emettere il decreto di autorizzazione per le intercettazioni [40].

Per quanto riguarda ***il requisito della necessità***, l'innovazione ha un significato più preci-

---

[36] V. GREVI, *Nuovo codice di procedura penale e processi di criminalità organizzata un primo bilancio*, in AA.VV., *Processo penale e criminalità organizzata*, cit., p. 14. La disciplina generale delle intercettazioni, come accennato, è normata dagli artt. 266 ss. c.p.p., tale disciplina subisce delle deroghe rilevanti – apportate dal d.l. 13 maggio 1991, n. 152 convertito in legge 12 luglio 1991, n. 203 e dal d.l. 18 ottobre 2001, n. 374 convertito in legge 15 dicembre 2001, n. 438 – nel caso in cui si proceda per reati di criminalità organizzata.

[37] A.A. DALIA-M. FERRAIOLI, *Manuale di procedura penale*, Padova, 2003, p. 515, A. CAMON, *op. cit*., p. 79. Le deroghe sono dovute all'art. 13, d.l. 13 maggio 1991, n. 152 (conv. dall'art. 1, legge 12 luglio 1991, n. 203) e modificato dall'art. 3 *bis* d.l. 8 giugno 1992, n. 306 (conv. dall'art. 1, legge 7 agosto 1992, n. 356) introduce deroghe alla disciplina ordinaria delle intercettazioni (artt. 266 e ss.) in tema di delitti di criminalità organizzata o di minaccia col mezzo del telefono. Successivamente l'art. 3 del d.l. 18 ottobre 2001, n. 374, conv. in legge 15 dicembre 2001, n. 438 rubricato "*Disposizioni urgenti per contrastare il terrorismo internazionale*", ha esteso la disciplina derogatoria in tema di intercettazioni per i delitti di criminalità organizzata e di minaccia col mezzo del telefono, ai procedimenti previsti dall'art. 270-*quater* c.p. e ai delitti di cui all'art. 407, comma 2, lett. a), n. 4, c.p.p.

[38] A. CAMON, *op. cit*., p. 79, in giurisprudenza vedi: Cass., sez. VI, 25 novembre 2003, Matarrelli, in *Guida dir*., 2004, 17, p. 95 ove si legge "*Con riferimento all'attività di intercettazione in tema di indagini relative a delitti di criminalità organizzata (articolo 13 del decreto legge 13 maggio 1991 n. 152, convertito in legge 12 luglio 1991 n. 203), sussistono deroghe rispetto alla disciplina ordinaria (articolo 267 del c.p.p.) riguardo ai relativi presupposti: l'autorizzazione a eseguire le intercettazioni telefoniche viene concessa allorché le stesse appaiono 'necessarie' (e non 'assolutamente indispensabili'), in presenza di 'sufficienti' (e non 'gravi') indizi di reato, 'per lo svolgimento' (e non per 'la prosecuzione') delle indagini*".

[39] A. CAMON, *op. cit*., p. 82.

[40] F. CORDERO, *Codice di procedura penale commentato*, Torino, 1990, p. 310.

so; non è necessario che l'intercettazione sia l'unico strumento efficace a disposizione dell'accusa, anche se sussistono mezzi meno lesivi è legittimo optare per questo [41]. In sostanza si ha l'abolizione del principio di "sussidiarietà" delle intercettazioni [42].

Infine il termine "***prosecuzioni delle indagini***" viene sostituito con il termine "***svolgimento delle indagini***", consentendo il ricorso a questo mezzo di ricerca della prova fin dalla fase di avvio delle indagini preliminari [43].

In sintesi, ***un triplice affievolimento*** dei presupposti delle intercettazioni.

Indizi meno convincenti, spostamento all'indietro dell'istituto, abolizione del principio di sussidiarietà delle intercettazioni medesime.

Il predetto regime straordinario delle intercettazioni dipende necessariamente dalla nozione attribuita alla locuzione delitti criminalità organizzata, che, come detto sopra, non è tassativa.

Riguardo alle modalità applicative dell'istituto, quando le ***intercettazioni riguardano i reati di criminalità organizzata***, in primo luogo, il periodo iniziale di **durata** delle intercettazioni è di quaranta giorni (non quindici) e le **proroghe** hanno una durata più lunga (venti giorni anziché quindici) e possono essere disposte dal P.M. in via d'urgenza, salvo il dovere di osservanza della procedura di convalida del Gip [44], ciò al fine di permettere una continuità nell'ascolto.

Anche le **intercettazioni ambientali**, previste dal comma 2 dell'art. 266 c.p.p., subiscono notevoli deroghe quando vengono disposte nei procedimenti di criminalità organizzata. Le captazioni ambientali riguardano i dialoghi che svolgendosi tra persone simultaneamente presenti nello stesso luogo, non richiedono l'ausilio di strumenti tecnici per la trasmissione del suono tra i presenti. Il confine con le intercettazioni ordinarie, è dunque segnato dalla modalità dei *colloqui che si svolgono a viva voce*, anziché tramite telefono o computer.

Anche questo tipo di intercettazioni, rientrano nella disciplina prevista in generale dagli artt. 266-271 c.p.p., il dialogo deve essere *riservato*, di conseguenza è necessario che l'ascolto venga effettuato tramite particolari *strumenti meccanici o elettronici*, l'operazione si deve

[41] F. RUGGIERI, *Commento agli artt. 266-267*, inedito (originariamente destinato al *Commentario del nuovo codice di procedura penale*, diretto da E. AMODIO e O. DOMINIONI la cui pubblicazione è stata sospesa), p. 12 ss. del dattiloscritto citata da A. CAMON, *op. cit*., p. 82, nota 52.

[42] L''intercettazione deve essere necessaria, non però, meramente utile (Cass., sez. V, 11.7.1995 Bonacchi ed altri, in *ANPP*, 1995, p. 865 ove si legge che "*In tema di intercettazioni telefoniche, premesso che queste sono sempre da considerare come uno strumento di indagine di carattere eccezionale, in quanto incidente sul diritto, costituzionalmente garantito, di libertà e di segretezza delle comunicazioni (art. 15 Cost.), va poi ricordato che, anche quando trattasi di intercettazioni finalizzate ad indagini relative a delitti di criminalità organizzata, deve essere adeguatamente motivata la ritenuta sussistenza delle condizioni atte a legittimarle, quali indicate, in parziale deroga all'art. 267 c.p.p. dall'art. 13 comma 1 del. d.l. 13 maggio 1991 n. 152 conv. con modif. in l. 12 luglio 1991 n. 203; condizioni costituite dalla accertata preesistenza di 'sufficienti indizi' di reato e dalla parimenti accertata 'necessità' – da non confondere con la mera utilità – del ricorso allo strumento investigativo in questione ai fini della proficua conclusione delle indagini stesse. Detta motivazione, poi, non può consistere in mere citazioni o parafrasi apodittiche delle norme, tanto meno, limitarsi ad un generico richiamo ai contenuti, più o meno analitici, delle richieste inoltrate dagli investigatori, essendo invece onere del P.M., prima (in casi di urgenza) e del GIP dopo, in sede di convalida, esprimere una propria valutazione sulla presenza delle condizioni previste dalla legge; valutazione che, per le finalità di garanzia processuale alle quali è predisposta, non può certamente esaurirsi in una passiva e acritica ricezione delle indicazioni espresse da coloro che sono preposti alla materiale esecuzione delle indagini*".

[43] C. DI MARTINO-T. PROCACCIANTI, *Le intercettazioni telefoniche*, Padova, 2001, p. 119.

[44] C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 119. Tale potere di proroga del P.M. suscita dubbi di legittimità costituzionale in rapporto alla riserva di giurisdizione di cui all'art. 15, comma 2, Cost., il quale riserva al giudice il potere limitativo della segretezza delle comunicazioni.

svolgere all'*insaputa dei colloquianti* (o almeno di uno fra essi), infine l'*iniziativa* deve provenire da *un terzo* e non da chi partecipa al colloquio [45].

L'istituto costituisce una delle novità più vistose del codice odierno e ha una particolare capacità intrusiva ignota alle intercettazioni ordinarie.

L'art. 266, comma 2, c.p.p., autorizza l'intercettazione tra presenti per tutti i reati disciplinati nel comma 1, quindi per i reati per i quali e consentita l'intercettazione telefonica o informatica, con tutti profili problematici relativi alla lieve gravità di alcuni reati menzionati nel comma 1 e la maggiore insidiosità del mezzo in questione.

Tuttavia, il legislatore, con l'intento di tutelare la privacy almeno nel **domicilio domestico** ha, in tema di intercettazioni ambientali, operato una *summa divisio*, a seconda che *l'intercettazione si svolga o no in uno dei luoghi indicati dall'art. 614 c.p.*; stabilendo che nel primo caso, accanto ai presupposti ordinari richiesti dall'art. 267 c.p.p., debba anche sussistere il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

Si tratta di un limite discutibile, secondo taluno oltre date soglie il garantismo diventa feticcio, utile alle culture ed economie del delitto; altri, ha sostenuto che non è ben chiaro perché si debbano disegnare dei confini "*territoriali*" di maggiore o minore tutela del diritto alla segretezza sostenendo che, il dialogo riservato è tale indipendentemente dal luogo ove si svolge [46].

Una dottrina ha trovato ***un accettabile equilibrio***, affermando che il collegamento tra tutela della segretezza e del domicilio non è affatto arbitrario; esso trova la sua giustificazione razionale nei motivi che hanno portato il domicilio ad emergere come nozione autonoma, vale a dire la salvaguardia degli interessi che trascendono dalla protezione accordata al diritto di proprietà. Ciò ha determinato l'allargamento dell'antico "*privilegio della casa*", cioè l'interesse ad una sfera di inviolabile intimità nelle relazioni sociali. Giacché l'art. 266, comma 2, c.p.p. apre una breccia così vistosa nel diritto alla privacy delle persone, non più al sicuro nella propria abitazione, appare perfettamente razionale un precetto che contenga quella breccia nei margini più ristretti possibili [47].

Il legislatore del 1988 richiede, ***l'attualità del reato***, con l'espressione "*ivi si stia svolgendo l'attività criminosa*". Si tratta di locuzione conforme alla flagranza di reato; quindi l'inter-

[45] A. CAMON, *op. cit.*, p. 176. Problemi in tema di intercettazioni ambientali si presentarono nel 1975 quando un giudice di primo grado dichiarò inutilizzabile la registrazione di conversazione tra imputati detenuti all'insaputa di costoro (Ass. Pisa, 9 gennaio 1975, Baldisseri ed altri, in *Riv. it. dir. proc. pen.*, 1976, p. 1002, con nota di CERVETTI). Il giudice partiva dal presupposto che gli artt. 226-*bis* e 339 c.p.p. abrogato riguardavano soltanto le comunicazioni a distanza e che nessuna disposizione legislativa regolamentava le conversazioni tra persone presenti. Il giudice d'appello la pensò in modo radicalmente opposto, sostenendo che gli articoli su citati combinati con l'art. 623-*bis* c.p. (testo del 1975) che interpreta autenticamente le comunicazioni non telegrafiche o telefoniche, comprende anche qualunque altra trasmissione di suono effettuata con collegamento su filo o ad onde guidate. In tale ultima espressione, si è ritenuto rientrassero anche le onde acustiche prodotte dalla corde vocali (Ass. App. Firenze, 3 maggio 1976 Baldissieri ed altri, in *Riv. it. dir. proc. pen.*, 1997, p. 802 ss. con nota di SCAPARONE). Si verificò un grande scalpore, e pareva irragionevole estendere l'applicazione di una norma come l'art. 623-*bis* c.p., quindi norma sostanziale per risolvere problemi procedurali era giuridicamente inaccettabile una interpretazione di tale tenore. In concreto non era possibile effettuare intercettazioni ambientali, malgrado qualche ambiguità dei *verba legis*, l'argomento si traeva agevolmente dall'art. 15 Costituzione il quale impone una riserva espressa di legge per poter limitare i diritto costituzionalmente previsti. L'assenza di una specifica norma escludeva l'ammissibilità prima, e l'utilizzabilità poi, di siffatte intercettazioni (E. ZAPPALÀ, *Il principio di tassatività dei mezzi di prova nel processo penale*, Milano, 1982, p. 209, G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, p. 47 ss.).

[46] La prima espressione e di F. CORDERO, *sub artt. 266-267*, in ID., *Codice di procedura penale commentato*, cit., p. 308, F. CAPRIOLI, *op. cit.*, p. 172.

[47] A. CAMON, *op. cit.*, p. 183.

cettazione ambientale nei luoghi previsti dall'art. 614 c.p. è praticabile, a condizione che vi sia fondato motivo che nel luogo si stia commettendo uno qualsiasi dei reati menzionati nell'art. 266, comma 1, c.p.p. [48].

La norma và necessariamente interpretata in conformità al dettato del legislatore che non postula il concreto svolgimento del'attività, ma, invero, che con giudizio *ex ante* ragionevolmente si possa ritenere la sussistenza all'atto dell'emanazione del provvedimento che nel domicilio designato si stia svolgendo l'attività criminosa [49].

Quanto ai luoghi tutelati, si noti che luoghi di privata dimora sono: oltre l'abitazione, quei luoghi che assolvono attualmente e concretamente la funzione di proteggere la vita privata di coloro che li possiedono. Ne deriva che, non tutti i locali, dai quali il possessore abbia il diritto di escludere la persona a lui non gradita, possono considerarsi luoghi di privata dimora; in quanto, lo *ius excludendi alios* rilevante *ex* art. 614 c.p. non è fine a se stesso, ma serve a tutelare il diritto alla riservatezza nello svolgimento di alcune manifestazioni della vita privata della persona, che l'art. 14 Cost. garantisce proclamando l'inviolabilità del domicilio [50].

---

[48] A. GIARDA, *Codice di procedura penale. Commentario*, a cura di A. GIARDA, II, Milano, 1992 p. 13, G. GATTI, *Il controllo del GIP sull'attività di indagine del P.M.: incidenti probatori, intercettazioni telefoniche, misure cautelari reali*, Quaderni CSM, 1995, 81 p. 331.

[49] In questo senso vedi P. BRUNO, *Le intercettazioni di comunicazioni o conversazioni*, in *Dig. disc. pen*., II, Torino, 1993, p. 206 ss.; C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 61, A. CAMON, *op. cit*., p. 185. Come spesso accade nelle fattispecie processuali a discrezionalità vincolata, nell'elaborazione giurisprudenziale il rigore della disposizione è stato attenuato, non ritenendosi al più necessario che detta attualità risulti effettivamente verificata sancendosi, viceversa, la sufficienza che se ne potesse ragionevolmente ritenere la realizzazione dell'atto del decreto autorizzativo. Il tutto ovviamente attraverso un giudizio *ex ante* (Cass., sez. VI, 29 novembre 1999, Perre, in *Cass. pen.*, 2001, p. 565; Cass., sez. VI, 21 novembre 1997, Avvantaggiato, in *Mass. uff.*, *210316*; Cass., sez. I, 12 dicembre 1994, Manzi, in *Giust. pen.*, III, 1995, p. 601). La locuzione "*fondato motivo di ritenere*" enfatizza, forse, la struttura dell'atto che autorizza il controllo; comunque, la legittimità della prova raccolta non può non dipendere da come sono esplicitati gli indizi sulla probabile flagranza di reato. Difatti nell'ultima sentenza citata si legge "*L'art. 266 comma 2 c.p.p., nel richiedere, come condizione atta a legittimare le intercettazioni ambientali in luoghi di privata dimora, che vi sia fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa, non postula affatto che detta attività risulti, poi, essere stata effettivamente sussistente, essendo invece da considerare sufficiente, sulla base del testuale dettato normativo (oltre che della evidente 'ratio legis'), che dell'attività in questione potesse, con giudizio 'ex ante', ragionevolmente ritenersi la sussistenza all'atto dell'emanazione del provvedimento di autorizzazione all'effettuazione delle operazioni*".

[50] Sul tema si veda C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 61 ss. La giurisprudenza ha escluso che possa qualificarsi luogo di privata dimora il deposito di una società esercente il commercio di carni, al quale acceda un numero indiscriminato di persone, salvo che nelle ore di chiusura, quando cioè in esso il titolare può compiervi qualsiasi attività di indole privata (Cass., sez. I, 23 marzo 1994, Pulito, in *Giust. pen.*, III, 1994, p. 356; Cass., sez. I, 13 febbraio 1992, D'Ancona, in *Arch. nuova proc. pen*., 1992, p. 620). Viceversa, si è ritenuto che per luogo di privata dimora deve intendersi quello adibito ad esercizio di attività che ognuno ha diritto di svolgere liberamente e legittimamente, senza turbativa da parte di estranei e tale è anche il luogo di esercizio di attività commerciale (Cass., sez. II, 10 giugno 1998, Cedrangolo, in *Mass. uff*., 211142) e l'ufficio privato poiché chi ne dispone svolge in esso la sua attività lavorativa, che implica un aspetto dello svolgimento della vita individuale (Cass., sez. VI, 29 settembre 2003, Giliberti, in *Mass. uff*., 227835). Dai luoghi di privata dimora è stata esclusa la camera di un ospedale pubblico di cui il degente non ha disponibilità esclusiva (Cass., sez. I, 22 gennaio 1996, Porcaro, in *Cass. pen*., 1997, p. 1082); del pari, anche la cella del carcere è stata esclusa dai luoghi tutelati dall'art. 14 Cost., in quanto il detenuto non è titolare dello *ius excludendi alios* (Cass., sez. VI, 5 novembre 1999, Bembi, in *Cass. pen*., 2000, p. 3352; Cass., sez. I, 3 marzo 1997, Talese, in *Cass. pen*., 1998, p. 2402). Quanto all'abitacolo dell'autovettura, si registra un peculiare contrasto: infatti mentre per la Corte costituzionale lo stesso è tutelato *ex* art. 14 Cost. (C. cost., 31 marzo 1987, n. 88, in *Foro it.*, 1987, II, c. 414), la Corte di cassazione evidenzia un duplice orientamento realizzandosi con alcune decisioni un adeguamento al principio sancito dalla Corte costituzionale (Cass., sez. I, 29 gennaio 2001, Veneziano, in *Mass. uff*., 218042; Cass., sez. VI, 23 gennaio 2001, De Palma, in *Guida dir*., 2001, 20, p. 97) ed affermandosi con altre la contraria opinione (Cass., sez. I, 20 dicembre 2004, n. 2613, in *Mass. uff*., 230533; Cass., sez. IV, 23 aprile 2004, n. 26010, in *Mass. uff*.,

Nel caso di procedimenti relativi all'accertamento dei reati di ***criminalità organizzata*** – ed ancora una volta di minaccia col mezzo del telefono – il ***requisito della flagranza è stato cancellato***, è esplicitamente previsto che il regime delle intercettazioni ambientali da svolgersi nel domicilio e negli altri luoghi indicati dall'art. 614 c.p. possa avvenire anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa [51].

Un problema autonomo per la disciplina derogatoria prevista, si profila in relazione all'art. 266-*bis* c.p.p. che, ***disciplina le intercettazioni di comunicazione informatica o telematica***. La disposizione prevede l'intercettazione del "flusso di comunicazioni relativo a sistemi informatici o telematici" per gli stessi reati indicati dall'art. 266 c.p.p., nonché per "*quelli commessi mediante l'impiego di tecnologie informatiche o telematiche*" [52]. Non è chiarito se le predette intercettazioni possono essere disposte solo per i reati di cui all'art. 266 c.p.p. o per tutti quei reati commessi mediante l'impiego delle tecnologie informatiche o telematiche.

Dal punto di vista logico, per quanto concerne le deroghe riguardanti la criminalità organizzata, non ci sarebbe motivo per negare che la *ratio* della lotta alla criminalità organizzata giustifichi un'interpretazione estensiva del rinvio all'art. 266 c.p.p., operato dall'art. 13 d.l. 152 del 1991, che dunque andrebbe riferito anche dall'art. 266-*bis* c.p.p. D'altronde, è nei voti della legge 547 del 1993, cui si deve l'introduzione dell'art. 266-*bis* c.p.p., estenderne quanto più possibile le potenzialità applicative sia a scopo repressivo che a scopo preventivo.

Non si deve, tuttavia, dimenticare che, il citato d.l. n. 152/1991 pone delle norme speciali, sia perché deroga al sistema delineato dagli art. 266 ss. c.p.p., sia perché si riferisce unicamente a determinate categorie di reati e si colloca *extra codice*.

Forse tale disciplina può prestare il fianco a censure di legittimità costituzionale sotto il profilo dell'indeterminatezza dei casi di intercettazione; ma l'interprete non può assolvere

229974; Cass., sez. VI, 1 dicembre 2003, Cavataio, in *Cass. pen*., 2005, p. 1995). Segnalati disorientamenti conseguono ad un equivoco interpretativo di base: se, infatti, è agevole l'individuazione del concetto di abitazione, non altrettanto può dirsi per quello di "*privata dimora*" *ex* art. 614 c.p. L'art. 614 c.p. tutela "*ogni luogo di cui si disponga a titolo privato ma nel quale non necessariamente si svolgono attività domestiche*").

[51] Cfr. art. 13 del d.l. 13 maggio 1991, n. 152 (in *G.U.* 13 maggio, n. 110). Decreto convertito con modificazioni in legge 12 luglio 1991, n. 203 (in *G.U.* 12 luglio 1991, n. 162), successivamente modificato dall'art. 3-*bis*, comma 1, d.l. 8 giugno 1992, n. 306 come modificato dalla legge 7 agosto 1992, n. 356, in sede di conversione e successivamente dall'art. 23, comma 1, legge 1° marzo 2001, n. 63. L'applicazione di detto articolo è stata estesa dall'art. 3 del d.l. 374/2001 conv. con modifiche in legge 15 dicembre 2001, n. 438, in materia di terrorismo internazionale, e dall'art. 9, legge 11 agosto 2003, n. 228, in materia di tratta di persone.

[52] Articolo aggiunto dall'art. 11, legge 23 dicembre 1993, n. 547, che modifica ed integra le norme del codice penale e del codice di procedura penale in tema di criminalità informatica. Il problema interpretativo si incentra sulla portata da attribuire a tale ultima locuzione. Non è chiaro, infatti, se il generico riferimento ai "reati commessi mediante l'impiego di tecnologie informatiche o telematiche" abbia voluto richiamare solo i reati informatici introdotti dalla legge 23 dicembre 1993, n. 547 ovvero anche i reati comuni realizzati mediante l'impiego di tecnologie informatiche (il che consentirebbe l'intercettazione anche per ipotesi di reato non previste dall'art. 266). Tale considerazione, unita a quella secondo la quale tale tipo di intercettazione è stata introdotta con la stessa legge che ha coniato i "reati informatici", ha condotto parte della dottrina a propendere per un'interpretazione sistematica degli artt. 266 e 266-*bis* che riservi l'intercettazione informatica ai soli reati introdotti dalla legge 23 dicembre 1993, n. 547 (L. FILIPPI, *op. cit*., p. 83; L. UGOCCIONI, *Commento all'art. 11 legge 547/93*, in *Legisl. pen*., 1996, 1-2, p. 142). La conclusione, non sembra consentita alla luce del dato letterale del testo di legge. Ove non è richiesto che l'uso di tecnologie informatiche sia elemento costitutivo del reato ma solo che il reato sia commesso con tali strumenti. Pertanto rientrano nella previsione sia quei delitti che sono necessariamente posti in essere con l'ausilio di tecnologie informatiche o telematiche (cfr., ad es., art. 615-*ter* c.p.) sia reati a forma libera che solo occasionalmente siano commessi con mezzo del computer (A. CAMON, *op. cit*., p. 67).

funzioni legislative: pertanto non resta che auspicare un intervento legislativo che ridisegni la norma nell'alveo della costituzionalità [53].

Altresì, le intercettazioni telefoniche e ambientali citate, possono essere disposte, come sancito dall'art. 295 commi 3 e 3-*bis* c.p.p., in un caso particolare, diretto ad "***agevolare la ricerca del latitante***".

La norma inizialmente prevista solo per i reati *ex* art. 51, comma 3-*bis*, c.p.p. (mafiosi in senso stretto), oggi è stata estesa dal d.l. 18 ottobre 2001 n. 374 ai delitti con finalità di terrorismo [54].

Innanzi tutto è bene chiarire il significato della locuzione **latitante**; che si riferisce a colui che: *si è sottratto volontariamente alla custodia cautelare, agli arresti domiciliari, al divieto di espatrio, all'obbligo di dimora e ad un ordine con cui si dispone la carcerazione* (art. 296, comma 1, c.p.p.). Questo è il ***presupposto soggettivo*** della particolare disciplina delle intercettazioni di cui ci stiamo occupando [55].

La particolare figura di intercettazione per agevolare la ricerca dei latitanti, richiama l'applicazione delle disposizioni previste negli artt. 268, 269, 270, c.p.p. ove compatibili. La disciplina dell'istituto si esaurisce qui, questo richiamo è parso poco opportuno ed ha lasciato alla dottrina e alla giurisprudenza la risoluzione di problemi cruciali [56].

L'art. 295 c.p.p. fa riferimento agli artt. 266 e 267 c.p.p., quindi le intercettazioni in discorso possono essere disposte solo allorché lo stato di latitanza sia dichiarato nel corso del procedimento per uno dei reati indicati dallo stesso art. 266 c.p.p. [57], altri problemi interpretativi riguardano la durata delle intercettazioni [58] e l'utilizzabilità probatoria dei risultati [59].

Accordata dottrina ha ritenuto che, premesse le finalità diverse tra i due tipi di intercettazioni (quelle comuni e quelle per la ricerca dei latitanti), le seconde devono essere finalizzate unicamente a agevolare la ricerca; altrimenti nei confronti del latitante si consentirebbe una intercettazione generale mirata alla ricerca di elementi a carico [60]. La giurisprudenza ha tutta-

[53] C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 120, L. UGOCCIONI, *Commento all'art. 11 legge 547/93*, in *Legisl. pen*., 1996, 1-2, p. 143 ss.; L. FILIPPI, *op. cit*., p. 83; Cass., sez. V, 27 febbraio 2002, Bresciani; Cass., sez. un., 13 luglio 1998, Gallieri, in *Guida dir.*, 1998, 48, p. 60. Un intervento legislativo appare ancora più necessario solo laddove si ponga mente alla rilevanza che ha acquisito l'art. 266-*bis* nell'interpretazione della Corte di cassazione in ordine all'assoggettamento alla disciplina delle intercettazioni anche dell'attività di acquisizione dei dati esteriori delle comunicazioni.

[54] F.P. GIORDANO, *op. cit*., p. 365.

[55] C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 76.

[56] A. CAMON, *op. cit*., p. 54.

[57] G. CIANI, *Art. 295*, in *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, III, Torino, 1990, p. 190. Vengono esclusi quindi i reati di cui all'art. 266-*bis* c.p.p. sul punto vedi: L. FILIPPI, *op. cit*., p. 246.

[58] Nel senso dell'utilizzabilità V. GREVI, *Misure cautelari*, in G. CONSO-V. GREVI, *Compendio procedura penale*, Padova, 2003, p. 398. Nel senso inverso vedi G. ILLUMINATI, *Intercettazioni per la ricerca del latitante: quali garanzie?*, in *Dir. pen. proc*., 1996, p. 83, Tribunale Milano, sez. VII, 19 ottobre 1995, Craxi, in *Dir. pen. proc*., 1996, p. 82, con nota di ILLUMINATI.

[59] Sono favorevoli alla utilizzabilità probatoria AMATO, *Commento agli articoli 293, 295-296*, in *Commentario del nuovo codice di procedura penale*, diretto da E. AMODIO e O. DOMINIONI, III, p. II, Milano, 1990, p. 138; A. SPATARO, *Le intercettazioni telefoniche*, *problemi operativi e processuali*, cit., p. 154. Per la tesi che nega il valore probatorio vedi G. ILLUMINATI, *Intercettazioni per la ricerca del latitante: quali garanzie?*, cit., p. 84 ove si legge che "*le intercettazioni in parola sono dirette alla ricerca del latitante e non all'acquisizione di prove per la decisione finale*". Per un'approfondita analisi sul tema si rinvia a A. CAMON, *op. cit*., p. 53 ss.

[60] G. ILLUMINATI, *Intercettazioni per la ricerca del latitante: quali garanzie?*, cit., p. 84.

via confermato l'utilizzabilità quando le intercettazioni rispettano di fatto le garanzie previste dagli art. 266 e ss. [61].

Il legislatore muovendosi nell'ottica del doppio binario, ha aggiunto all'art. 295 c.p.p. il comma 3-bis. che dispone: nel caso in cui il latitante è ricercato in relazione a un delitto di criminalità organizzata o a un delitto commesso con finalità di terrorismo o di eversione dell'ordinamento costituzionale – per il quale la legge prevede la reclusione non inferiore nel minimo a cinque anni e nel massimo a dieci anni – o infine per il delitto di partecipazione a associazione sovversiva o a banda armata, il giudice o il P.M. possono disporre l'**intercettazione di comunicazione tra presenti**, cioè quelle ambientali [62].

Si tratta di una precisazione assolutamente necessaria, infatti, il comma 3, art. 295, c.p.p. non è sufficiente a legittimare anche le intercettazioni ambientali; perché esso pur richiamando l'art. 266 c.p.p. utilizza l'espressione intercettazioni di conversazione o comunicazioni telefoniche e di altre *forme di telecomunicazione*. Con tale ultima espressione si intende un richiamo che ricapitola, in chiave generale, i più dettagliati cenni alle conversazioni o comunicazioni telefoniche [63].

Riguardo alla ***disciplina relativa al domicilio sussistono perplessità***, infatti, taluno ritiene che anche in questo caso, le captazioni ambientali non incontrano il limite di cui all'art. 266, comma 2, c.p.p. (già derogato in via generale con riguardo ai procedimenti di criminalità organizzata) mentre, altri, ritengono che la deroga non sia prevista e pertanto l'intercettazione ambientale nel luogo di privata dimora incontra gli stessi limiti previsti dal comma 2 dell'art. 266 c.p.p. [64].

---

[61] La giurisprudenza ha risolto il problema nella prassi specificando come le risultanze delle intercettazioni disposte, ai sensi dell'art. 295, comma 3, c.p.p., al fine di agevolare le ricerche del latitante possano essere utilizzate anche ai fini probatori, quando risultano di fatto osservate le garanzie e le prescrizioni di cui agli artt. 266 ss. c.p.p. operando, in caso contrario, il regime dei divieti di utilizzazione dettato dall'art. 271 c.p.p., anche se questo non è richiamato. La giurisprudenza ha anche ritenuto utilizzabili dette intercettazioni non solo nel processo relativo al latitante, ma anche, in altri processi. Cass., sez. I, 12 luglio 1999, Siascia, in *Cass. pen*., 2000, p. 2324. Vedi anche in *Arch. nuova proc. pen*., 1999, p. 603. Nel senso che "*il disposto di cui all'art. 271 c.p.p., non richiamato, a differenza degli artt. 268, 269 e 270, dall'art. 295 comma 3, non può essere invocato come causa di inutilizzabilità delle intercettazioni effettuate ai sensi di detta ultima norma*" vedi Cass., sez. VI, 29 ottobre 2003, Bevilacqua, in *Arch. nuova proc. pen*., 2004, p. 222 in fattispecie relativa all'utilizzabilità del contenuto delle intercettazioni disposte per la cattura del latitante nel processo all'imputato di favoreggiamento personale del latitante. Peraltro, dato l'espresso richiamo all'art. 270 c.p.p. "*deve ritenersi che i risultati delle intercettazioni disposte per agevolare le ricerche del latitante siano utilizzabili ai fini probatori, anche nei confronti di soggetti diversi, nell'ambito di altro procedimento*" (Cass., sez. I, 9 dicembre 1999, Bolandin, in *Arch. nuova proc. pen*., 2000, p. 166). In argomento vedi di recente, Cass., sez. I, 28 gennaio 2003, Pasquino, in *Mass. uff*., 223175; nonché Cass., sez. I, 22 marzo 2005, D'Amico ed altri, in *Mass. uff*., 231502, la quale ha ribadito l'utilizzabilità a fini probatori, anche in procedimenti diversi, e ciò "*anche a prescindere dalla esatta individuazione, nei decreti autorizzativi, del* nomen juris *del reato astrattamente perseguibile*". Sul rilievo che l'intercettazione di conversazioni per la ricerca di un latitante è sottoposta solo "*ove possibile*" al rispetto delle regole previste dall'art. 268, si è precisato che l'utilizzo di impianti esterni alla Procura non richiede una particolare motivazione in relazione alle indilazionabili ragioni di urgenza "*in quanto la cattura di un latitante integra di per sé una eccezionale ragione di urgenza, con l'ulteriore conseguenza che i risultati di detta intercettazione possono essere utilizzati anche in procedimento diverso*" (Cass., sez. I, 4 novembre 2004, Galia ed altri, in *Mass. uff*., 229774).

[62] A.A. DALIA-M. FERRRAIOLI, *op. cit*., p. 326. Da notare che l'art. 1 della legge 14 febbraio 2006 n. 56 ha disposto che le intercettazioni per la ricerca del latitante per i procedimenti pendenti davanti alla Corte D'Assise vengano disposte dal presidente della Corte, come sancito dall'art. 295, comma 3-*ter* c.p.p.

[63] G. DI CHIARA, *sub art. 3-bis d.l. 8 giugno 1992 n. 306 (Antimafia)*, in *Legisl. pen.*, 1993, p. 59, nota 8.

[64] La prima tesi è sostenuta da V. GREVI, *Misure cautelari*, cit., p. 398. Mentre e di parere diametralmente opposto e sostiene che su tale punto le intercettazioni ambientali previste dall'art. 13 del d.l. n. 152 del 1991 e

Infine, altro strumento lesivo della privacy è rappresentato dalle ***intercettazioni preventive***, così definite perché volte ad acquisire notizie per la prevenzione di alcuni delitti [65].

Si definiscono preventive, quelle intercettazioni i cui risultati possono essere utilizzati esclusivamente ai fini della prosecuzione delle indagini e non ai fini processuali [66].

Il primo problema che si pone è la ***compatibilità con l'art. 15 della Costituzione*** di tali intercettazioni, in quanto l'attività di prevenzione dei reati mal si concilia con la previsione costituzionale dell'obbligatorio intervento dell'autorità giudiziaria, che sarebbe chiamata non già a vagliare la sussistenza di indizi di reità bensì ad avallare l'esistenza di un sospetto, trasformandosi da giudice in poliziotto [67].

Eppure, la Corte Costituzionale, con la sentenza 34 del 1973 ha consentito il sacrificio della segretezza delle comunicazioni per la necessità di "*prevenire e reprimere i reati*" aggiungendo che il potere di intercettare si ricollega a "*quel dovere di prevenzione e di scoperta degli illeciti penali che è compito istituzionale degli organi di polizia giudiziaria*". Pertanto, la stessa Corte, ha affermato che i diritti previsti dall'art. 15 Cost. possono essere limitati per l'esigenza di prevenire e reprimere i reati; così legittimando l'esistenza nel sistema di intercettazioni che non seguono la commissione del reato, ma lo precedono [68].

Sulla scia della pronuncia della Corte del 1973 sono state previste nell'ordinamento italiano **tre ipotesi di intercettazioni preventive**:

A) La prima contemplata dall'art. 226 disp. att. c.p.p. che ha mantenuto in vigore l'art. 226-*sexies* c.p.p. 1930 per le intercettazioni telefoniche previste dall'art. 1, comma 8, d.l. 6 settembre 1982, n. 629 convertito con modificazioni nella legge 12 ottobre 1982, n. 726 [69].

---

quelle disciplinate dall'art. 295 c.p.p., pur avendo il tratto comune di riguardare procedimenti relativi alla criminalità organizzata, operano in due ambiti ben diversi. G. DI CHIARA, *sub art. 3-bis d.l. 8 giugno 1992 n. 306 (Antimafia)*, cit., p. 61.

[65] A.A. DALIA-M. FERRAIOLI, *op. cit*., p. 516.

[66] G. GATTI, *op. cit*., p. 224.

[67] L. FILIPPI, *op. cit*., p. 255 ss.

[68] Sul punto vedi Corte cost., 6 aprile 1973, n. 34, in *Giur. cost*., 1973, p. 326 in motivazione con nota di GREVI. Nella sentenza si legge che "*È infondata, in riferimento agli art. 15 e 24 cost. e nei sensi di cui in motivazione, la questione di costituzionalità dell'art. 226, ultimo comma, c.p.p., per il quale per intercettare o impedire comunicazioni telefoniche o prendere cognizione gli ufficiali di polizia giudiziaria devono munirsi di autorizzazione dell'autorità giudiziaria più vicina, che la concede con decreto motivato la corte afferma che: a) in riferimento all'art. 15, dopo aver (sentito il dovere di) formulare l'auspicio che si realizzino opportuni interventi legislativi idonei ad attuare anche sul piano tecnico le condizioni, necessarie all'effettivo controllo diretto ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione, ha osservato che aa) il decreto di autorizzazione è sindacabile e la sua eventuale illegittimità può essere rilevata nel corso del giudizio, b) le risultanze delle intercettazioni sono coperte dal segreto, al quale sono tenuti gli ufficiali giudiziari e, nel corso dell'istruttoria, chiunque ne abbia preso conoscenza, ac) nel processo non può essere utilizzato se non il materiale rilevante per l'imputazione di cui si discute e, pertanto, viene garantita non solo la segretezza di tutte le comunicazioni telefoniche dell'imputato non rilevanti ai fini del processo, ma anche la segretezza delle comunicazioni non pertinenti al processo che terzi, allo stesso estranei, abbiano fatto attraverso l'apparecchio telefonico sottoposto a controllo di intercettazione ovvero in collegamento con questo; b) in riferimento all'art. 24 2° comma, ha precisato che il diritto di serbare il silenzio, riconosciuto all'imputato sottoposto all'interrogatorio, non ha ragione né possibilità di operare, nel caso delle dichiarazioni o ammissioni di responsabilità spontaneamente fatte da un sospettato o da un indiziato nel corso di una conversazione telefonica intercettata su autorizzazione dell'autorità giudiziaria in sede di indagini preliminari all'istruttoria*".

[69] La disposizione di riferimento, così come risultante dalla successiva modifica apportata dall'art. 1 della legge 15 novembre 1988, n. 486, riconosceva all'Alto Commissario per il coordinamento della lotta contro la delinquenza mafiosa *ogni altro potere attribuito all'autorità di pubblica sicurezza, ivi compreso il potere di intercettazione telefonica ex art. 226-sexies c.p.p. 1930*. Tuttavia a partire dal 1° gennaio 1993 con l'art. 2, comma

La disciplina dell'art. 226 disp. att. c.p.p. riguarda l'attività captativa, attiene a ***delitti di particolare allarme sociale,*** quali quelli previsti dagli artt. 51, comma 3-*bis* e 407, comma 2, lett. a), n. 4, c.p.p.

Il ***potere di richiedere*** le intercettazioni preventive è attribuito al Ministro dell'Interno o, su sua delega, ai vertici dei servizi centrali interforze, al questore e ai comandanti provinciali dei Carabinieri o della Guardia di Finanza. Il Ministro può, altresì, delegare il Direttore della Direzione investigativa antimafia limitatamente ai delitti di criminalità organizzata di stampo mafioso.

In ogni caso, la richiesta di intercettazione deve pervenire al *procuratore della Repubblica presso il Tribunale* del capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo o, nel caso in cui tale luogo non sia determinabile, al Procuratore presso il Tribunale del capoluogo del distretto ove siano emerse le esigenze di prevenzione; che provvede con decreto motivato [70].

Inoltre, quando le suddette intercettazioni siano ritenute necessarie per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale, esse possono essere disposte anche su iniziativa del direttore dei servizi informativi e di sicurezza, in quanto a ciò delegati dal presidente del Consiglio dei ministri, a seguito di autorizzazione del Procuratore generale della Corte d'appello del distretto individuato come sopra [71].

B) **La seconda ipotesi di intercettazione preventiva** è disciplinata dall'art. 16 della legge 13 settembre 1982, n. 646. Tale disposizione prevede che il Procuratore della Repubblica del luogo dove le operazioni devono essere eseguite possa autorizzare gli ufficiali di polizia giudiziaria ad intercettare comunicazioni o conversazioni, telefoniche o telegrafiche, o quelle indicate dall'art. 623-*bis* c.p. quando "*lo ritenga necessario al fine di controllare che le persone, nei cui confronti sia stata applicata una delle misure di prevenzione della sorveglianza speciale o del soggiorno obbligatorio non continuino a porre in essere comportamenti analoghi a quelli che hanno dato luogo all'applicazione della misura di prevenzione*" [72].

Le garanzie previste dall'art. 16 legge 13 settembre 1982, n. 646 riguardano l'osservanza

2-*quater*, d.l. 29 ottobre 1991, n. 345 (conv. con modificazioni in legge 30 dicembre 1991, n. 410) le competenze dell'Alto Commissario sono state attribuite al Ministro dell'interno, con potestà di delega ai prefetti ed al direttore della Direzione investigativa antimafia. Si tratta quindi di una nuova attribuzione di poteri che non permette di ritenere implicitamente abrogata l'ipotesi di intercettazione con l'eliminazione della figura dell'Alto Commissario, come pure si era sostenuto nel passato.G. SPANGHER, *La disciplina italiana delle intercettazioni di conversazioni o comunicazioni*, in *Arch. pen*., 1994, p. 9.

[70] Il procuratore così individuato è altresì competente ad autorizzare (sempre con decreto motivato) le eventuali proroghe (venti giorni) dell'originario termine (quaranta giorni massimi), nel permanere delle esigenze investigative che giustificano l'attività di prevenzione e lo ritenga necessario; dando chiaramente atto dei motivi nel decreto di proroga. L. PISTORELLI, *Intercettazioni preventive ad ampio raggio ma inutilizzabili nel procedimento penale*, in *Guida dir*., 2001, 42, p. 90; F. RUGGERI, *Art. 5 D.L. 18.10.2001 n. 374 (Terrorismo internazionale)*, in *Legisl. pen*., 2002, p. 793 ss.

[71] V. GREVI, *Le prove*, in G. CONSO-V. GREVI, *Compendio di procedura penale*, Padova, 2006, p. 372. La previsione è dovuta agli artt. 4 e 7-*bis*, d.l. 27 luglio 2005, n. 144 conv. con legge 31 giugno 2005, n. 155.

[72] Si tratta di un'attività di prevenzione mirata ai fini della possibilità di reiterare la misura sulla base di nuovi elementi emersi nel corso dell'intercettazione che, ingenera non poche perplessità, con riferimento alla delega di esecuzione agli ufficiali di polizia giudiziaria e per la genericità del presupposto; che non solo si lega ad una necessità indeterminata, ma addirittura, rimette ogni valutazione al riguardo insindacabilmente al Procuratore della Repubblica. R. GUERRINI-L. MAZZA, *Le misure di prevenzione profili sostanziali e processuali*, Padova, 1996, p. 252.

delle modalità previste dagli artt. 226-*ter* e 226-*quater*, commi 1-4, c.p.p. 1930 [73], l'obbligo di disporre la distruzione delle registrazioni stesse e di ogni loro trascrizione sia pure parziale da parte del Procuratore della Repubblica che ha autorizzato le intercettazioni e, l'inutilizzabilità processuale degli elementi acquisiti attraverso l'intercettazione preventiva che possono essere utilizzati esclusivamente per la prosecuzione delle indagini [74].

Il riferimento alle indagini può, e deve, riguardare solo le indagini relative al procedimento per l'applicazione di una misura di prevenzione.

C) **L'ultima ipotesi** di intercettazione per la prevenzione dei reati è disciplinata dall'art. 25-*ter* del d.l. 8 giugno 1992, n. 306 (convertito in legge 7 agosto 1992, n. 356), per cui su richiesta del Ministro dell'interno o per sua delega al direttore della Direzione investigativa antimafia, dei responsabili di livello centrale dei servizi centrali e interprovinciali di cui all'art. 12, d.l. 13 maggio 1991, n. 152 (convertito in legge 12 luglio 1991, n. 203) o del questore, il Procuratore della Repubblica presso il tribunale del capoluogo del distretto dove le operazioni devono essere eseguite, può autorizzare, con decreto motivato, l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici [75], nonché l'intercettazione di comunicazioni tra presenti anche se queste avvengono nei luoghi indicati dall'art. 614 c.p.

Le richieste di intercettazione, con il relativo decreto, devono intervenire quando le intercettazioni medesime siano necessarie per l'attività di prevenzione e di informazione in ordine ai delitti indicati nell'art. 51, comma 3-*bis* (delitti strettamente mafiosi) [76]. La durata delle operazioni non può superare quaranta giorni, ma può essere prorogata dal Procuratore della Repubblica con decreto motivato per periodi successivi di venti giorni, qualora permangano i presupposti indicati dal comma 1 dell'art. 25-*ter* in discorso; cioè quando le intercettazioni continuino ad essere "necessarie per l'attività di prevenzione ed informazione, in ordine ai delitti di cui all'art. 51 comma 3-*bis*".

---

[73] R. D'AJELLO, *Le intercettazioni di conversazioni e comunicazioni*, in *Riv. pen. ec.*, 1990, p. 113. Ritiene che il riferimento attualmente riguarda gli artt. 267, 268, commi 1-3, c.p.p., 89 disp. att. c.p.p.

[74] C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 83.

[75] Tale possibilità è stata introdotta con la novella del 1993, allorché il legislatore nell'ottica di ampliare gli strumenti di lotta alla criminalità organizzata, ha stabilito che le intercettazioni preventive disciplinate dall'art. 25-*ter* in discorso, possono riguardare anche il flusso di comunicazione relativo a sistemi informatici e telematici (art. 13, legge 23 dicembre 1993, n. 547). Precisando che la possibilità di ricorrere a tali intercettazioni non dipende dal fatto che i reati vadano commessi con tali strumenti telematici. La dizione relativi a sistemi informatici sembra sufficientemente ampia per comprendere qualsiasi tipo di comunicazione tra elaboratori di qualsiasi genere. Vedi L. UGOCCIONI, *sub. art. 13 legge 23 dicembre 1993 n. 547 (Criminalità informatica)*, in *Legisl. pen*., 1996, p. 148 e nello stesso senso, G. FUMU, *sub art. 266-266-bis*, in *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, III, Agg., Torino, 1998, p. 136, nota 18.

[76] Pur nel silenzio della legge, è da ritenere che *il decreto autorizzativo* debba essere motivato, solo in tal modo si eviterebbe un contrasto con l'art. 15 Cost. comma 2 anche perché non avrebbe senso, esigere la motivazione per il decreto di proroga e non esigerla per il decreto che dispone le intercettazioni. DI CHIARA, *Commento all'art. 25-ter d.l. 306/92*, in *Legisl. pen*., 1993, p. 256. Anche se l'autore afferma che la disciplina dell'art. 25-ter è problematica. Infatti i presupposti dello steso, costituiscono la fornace problematica dell'intero istituto. Basti pensare che la norma esigendo un decreto motivato, ammette che il Procuratore della Repubblica, dopo avere verificato che si versa in tema di uno dei reati di cui al comma 3-*bis* dell'art. 51 c.p.p. deve anche accertare la necessità di ricorrere alle intercettazioni. E poiché tale accertamento va compiuto in un momento in cui il procedimento penale non è ancora iniziato, il magistrato può avvalersi per esso non di elementi oggettivi, quali ad esempio indizi di reità a carico del soggetto controllato, ma soltanto di elementi di sospetto, indicati nella richiesta. La necessità di ricorrere alle intercettazioni è dunque un presupposto molto labile, che apre le strade ad abusi. Vedi ROSSI, *I presupposti delle intercettazioni telefoniche*, in *Riv. it. dir. proc. pen*., 1987, p. 608.

Su richiesta del Ministro dell'interno, o dei soggetti da lui delegati, il Procuratore della Repubblica può autorizzare che, le operazioni di intercettazione siano eseguite con impianti diversi da quelli esistenti presso la Procura della Repubblica. Non sono espressamente previste, né la registrazione né la verbalizzazione delle intercettazioni, che restano perciò prive di documentazione.

4. Conclusioni

Dalla breve analisi normativa e giurisprudenziale sopra specificata, si evince come per le indagati riguardanti delitti presumibilmente ascrivibili al *genus* della criminalità organizzata, il diritto alla riservatezza viene irrimediabilmente sacrificato per garantire la sicurezza collettiva.

Le garanzie riconosciute durante le indagini per ipotesi di reato "*meno gravi*" ed a carico di indagati "*meno pericolosi*", cedono il passo all'affievolimento in nome della sicurezza collettiva.

Presupposto per l'affievolimento delle garanzie e che il reato oggetto d'indagine appartenga alla categoria dei delitti di criminalità organizzata.

L'aspetto preoccupante è che, la diffusione dell'impiego legislativo della locuzione criminalità organizzata è divenuta proporzionale in modo inverso all'univocità della sua definizione; oggi siffatta locuzione è ampliamente diffusa pur non essendo chiaro il significato[77].

Come si è visto sopra non esiste un'univoca interpretazione della locuzione, dottrina e giurisprudenza manifestano nozioni diverse e spesso contrastanti.

Un chiarimento, e la ricerca di una certa forma di tassatività, pare necessario, poiché, la persona sottoposta alle indagini per una presunta ipotesi di reato di criminalità organizzata subisce un forte affievolimento delle proprie garanzie individuali costituzionalmente previste con un'evidente breccia nel diritto alla privacy.

È evidente che il pericolo della criminalità organizzata è grave e comporta spesso la tendenza ad applica una definizione "*aperta*" della locuzione, in primo luogo per coprire i diversi settori in cui le organizzazioni criminali si infiltrano e, in secondo luogo, per evitare di creare "*lacci e laccioli*" al sistema di contrasto.

Bisogna comunque essere consapevoli che la normativa di contrasto alla criminalità organizzata sacrifica il diritto alla privacy, spesso ledendo la riservatezza di cittadini che nulla c'entrano con l'associazione.

Riguardo alle deroghe, si è visto come la disciplina ordinaria delle intercettazioni cede il passo a presupposti diversi quando le indagini riguardano delitti di criminalità organizzata o di minaccia col mezzo del telefono.

Come detto, si verifica ***un triplice affievolimento*** dei presupposti delle intercettazioni: indizi meno convincenti di quelli richiesti in via ordinaria, spostamento all'indietro (cioè verso i primi passi delle indagini preliminari) dell'istituto, abolizione del principio di sussidiarietà delle intercettazioni medesime.

La *ratio* di queste modifiche è palese, nell'ambito mafioso è noto come la velocità di decisioni, la mobilità, la capacità di anticipare gli inquirenti o i clan avversari, lo svolgimento dei traffici in un contesto internazionale sono modalità operative essenziali per la sopravvi-

[77] Sul tema specifico vedi O. LUPACCHINI, *op. cit*., p. 178 ss.; E. FORTUNA-S. DRAGONE, *Le prove*, in E. FORTUNA *et al*., *Manuale del nuovo processo penale*, Padova, 1991, p. 394; C. TAORMINA, *op. cit*., c. 129 ss. nella prospettiva del raffronto fra la nozione criminologica ed il contenuto normativo della formula "criminalità organizzata", S. RINALDI, *Un dibattito sulla risposta istituzionale alla criminalità organizzata*, in *Dei delitti e delle pene*, 1992, II, p. 58 ss. nonché L. STORTONI, *Criminalità organizzata e legislazione di emergenza*, *ivi*, p. 37 ss.

venza delle organizzazioni stesse. Per questo motivo, i membri delle associazioni sono obbligati, nonostante i rischi, ad usare con frequenza i mezzi di comunicazione a distanza.

Inoltre, la forza di intimidazione di queste associazioni e la piaga del fenomeno omertoso, rendono talvolta malsicure le fonti di prova testimoniali; spingendo gli inquirenti, anche sotto questo profilo, a puntare molto sui c.d. atti a sorpresa.

È evidente che, l'applicabilità di un regime o dell'altro all'indagine in corso dipende necessariamente dalla nozione di criminalità organizzata, che, come detto sopra non è tassativa.

Il regime delle intercettazioni in teoria eccezionale, potrebbe essere usato come un passaporto; poiché molti delitti potrebbero essere presentati come di criminalità organizzata e poi sfociare in capi di imputazione totalmente differenti.

L'***evanescenza della locuzione***, porterebbe poi il rischio di divergenze interpretative tra giudice delle indagini preliminari (che autorizza le intercettazioni) e quello del dibattimento (che ne vaglia l'utilizzabilità); con due possibili epiloghi: il possibile azzeramento della prova qualora il secondo giudice ritenga che il reato per cui l'intercettazione è stata disposta non rientri tra quelli di criminalità organizzata [78], o, in alternativa, applicando principi già sanciti dalla giurisprudenza, la conferma dell'utilizzabilità delle intercettazioni disposte per reati inizialmente qualificati di criminalità organizzata ma successivamente riqualificati come non di criminalità organizzata [79].

Permane perplessità riguardo alla possibilità di adottare il regime speciale delle intercettazioni predette anche per il reato di minacce con il mezzo del telefono, che, invero, è chiaramente un reato minore per il quale non dovrebbe ragionevolmente sussistere una lesione così forte del diritto alla privacy.

Per quanto concerne la disciplina delle **intercettazioni ambientali,** pur apparendo *ictu oculi* la maggiore lesione delle privacy conseguente all'adozione di questo secondo mezzo di ricerca della prova, la disciplina è conformata essenzialmente su quella delle intercettazioni di comunicazioni telefoniche.

Invero, mentre queste ultime consentono la sorveglianza di un solo mezzo di comunicazione a distanza, l'ascolto ambientale ha un raggio d'azione onnicomprensivo e vi rientra tutto quanto viene detto in un determinato luogo. L'individuo viene sorpreso nel momento in cui è massima la sua fiducia nell'intimità e nella libertà del comunicare. Pertanto, è condivisibile la deduzione di chi ha sostenuto che, le intercettazioni ambientali più che limitare il diritto alla privacy lo sopprimono radicalmente [80].

L'unico limite volto a tutelare la privacy dalle intercettazioni ambientali pare quello riguardante l'ambiente domestico che tutela il domicilio da intrusioni esterne quando non vi sia fondato motivo di ritenere che all'interno si stia svolgendo l'attività criminosa.

Nel caso di procedimenti concernenti reati di *criminalità organizzata* – ed ancora una volta di minaccia col mezzo del telefono – il requisito della flagranza è stato cancellato.

Tale normativa è criticabile, soprattutto per i procedimenti volti ad accertare le minacce a

[78] A. CAMON, *op. cit*., p. 84.

[79] Sul punto, si veda: Cass. pen., sez. VI, 20 ottobre 2009, n. 50072, B. Ced, in *Cass. pen*., 2009, ove si legge che: "*Sono utilizzabili i risultati delle intercettazioni disposte in riferimento ad un titolo di reato per il quale le medesime sono consentite, anche quando al fatto venga successivamente attribuita una diversa qualificazione giuridica con la conseguente mutazione del titolo in quello di un reato per cui non sarebbe stato invece possibile autorizzare le operazioni di intercettazione*". Vedi anche: Cass. pen., n. 40036 del 2008; Cass. pen., n. 26763 del 2008; Cass. pen., n. 16665 del 2008; Cass. pen., n. 8380 del 2008; Cass. pen., sez. VI, 24 giugno 2005, n. 33751; Cass. pen., n. 19852 del 2009; Cass. pen., n. 5331 del 1994.

[80] F.M. IACOVIELLO, *Intercettazioni ambientali: l'audace intrusione di una norma tra garanzie costituzionali ed esigenze dell'etica sociale*, in *Cass. pen*., 1992, p. 1564 ss.

mezzo telefono, poiché ***il sistema si appiattisce*** e regola in modo identico i diversi tipi di intercettazione, questa soluzione sarebbe accettabile se intercettazioni telefoniche e ambientali violassero in modo identico la privacy, ma la lesione è indiscutibilmente maggiore quando si propende per le seconde.

Si è altresì chiarito come le intercettazioni telefoniche e ambientali possono essere utilizzati quasi in maniera illimitata per la **ricerca dei latitati** per gravi reati.

Il crescente fenomeno delle misure cautelari coercitive e la consapevolezza che alcuni importanti personaggi della criminalità organizzata, pur trovandosi con limiti alla libertà personale hanno comunque esercitato un ruolo chiave all'interno delle rispettive associazioni delinquenziali [81], hanno spinto il legislatore a irrobustire l'azione delle forze dell'ordine impiegate nella cattura dei latitanti.

Nessuna tutela alla riservatezza esiste per chi si sottrae volontariamente all'esecuzione della pena e si trova nello status di latitante per gravi reati; l'unica tutela dal punto di vista delle garanzie processuali riguarda la non utilizzabilità probatoria delle intercettazioni volte alla ricerca del latitante, anche se, sussistono contrasti giurisprudenziali sul punto [82].

Invero, anche se la dottrina ha affermato l'inutilizzabilità processuale dei risultati delle intercettazioni, detta tesi è stata più volte negata dalla giurisprudenza che ha posto in discussione tale limite di salvaguardia [83].

La giurisprudenza, nelle diverse pronunce sul tema, ha specificato che le risultanze delle intercettazioni disposte ai sensi dell'art. 295, comma 3, c.p.p. al fine di agevolare le ricerche del latitante, possano essere utilizzate ai fini probatori, quando risultano di fatto osservate le garanzie e le prescrizioni di cui agli artt. 266 e ss. c.p.p. [84].

---

[81] G. CIANI, *Sub art. 295 c.p.p.*, in *Commento al nuovo codice di procedura penale*, coordinato da M. CHIAVARIO, II, Agg., 1993, p. 122.

[82] G. ILLUMINATI, *Intercettazioni per la ricerca del latitante: quali garanzie?*, cit., p. 83; Trib. Milano, sez. VII, 19 ottobre 1995, Craxi, in *Dir. pen. proc*., 1996, p. 82 con nota di ILLUMINATI; Cass. pen., sez. I, 18 ottobre 2000, n. 5897, Mangia, in *Arch. nuova proc. pen*., 2001, p. 161.

[83] Cass., sez. I, 16 settembre 1999, Sciascia, in *Cass. pen*., 2000, p. 1309; Cass., sez. I, 16 settembre 1998, Bolandin, in *Dir. pen. proc*., 1999, p. 470; Trib. Milano, 19 ottobre 1995, Craxi, in *Guida dir*., 1995, 44, p. 102.

[84] Cass., sez. I, 12 luglio 1999, Siascia, in *Cass. pen*., 2000, p. 2324 ove si legge che "*Le risultanze delle intercettazioni disposte, ai sensi dell'art. 295, comma 3, c.p.p., al fine di agevolare le ricerche del latitante possono essere utilizzate anche a fini probatori quando risultino di fatto osservate le garanzie e le prescrizioni di cui agli art. 266 ss. c.p.p. operando, in caso contrario, nonostante la mancanza di un espresso richiamo, il regime dei divieti di utilizzazione dettato dall'art. 271 c.p.p.*", vedi *Arch. nuova proc. pen*., 1999, p. 603. Nel senso che "*il disposto di cui all'art. 271 c.p.p., non richiamato, a differenza degli artt. 268, 269 e 270, dall'art. 295 comma 3, non può essere invocato come causa di inutilizzabilità delle intercettazioni effettuate ai sensi di detta ultima norma*", vedi Cass., sez. VI, 29 ottobre 2003, Bevilacqua, in *Arch. nuova proc. pen*., 2004, p. 222 in fattispecie relativa all'utilizzabilità del contenuto delle intercettazioni disposte per la cattura del latitante nel processo all'imputato di favoreggiamento personale del latitante. Peraltro, dato l'espresso richiamo all'art. 270 c.p.p. "*deve ritenersi che i risultati delle intercettazioni disposte per agevolare le ricerche del latitante siano utilizzabili ai fini probatori, anche nei confronti di soggetti diversi, nell'ambito di altro procedimento*" (Cass., sez. I, 9 dicembre 1999, Bolandin, in *Arch. nuova proc. pen*., 2000, p. 166). In argomento vedi di recente, Cass., sez. I, 28 gennaio 2003, Pasquino, in *Mass. uff*., 223175; nonché Cass., sez. I, 22 marzo 2005, D'Amico ed altri, in *Mass. uff*., 231502, la quale ha ribadito l'utilizzabilità a fini probatori, anche in procedimenti diversi, e ciò "*anche a prescindere dalla esatta individuazione, nei decreti autorizzativi, del nomen juris del reato astrattamente perseguibile*". Da ultima si veda Cass. pen., sez. I, 7 giugno 2007, n. 24178, in *Guida dir*., 2007, 30, p. 67 ove si dispone che i risultati delle intercettazioni per la ricerca del latitante possono essere utilizzati in procedimenti diversi, stante l'espresso rinvio all'art. 270 c.p.p., e ciò senza applicare i divieti previsti dall'art. 271 c.p.p. in quanto non espressamente richiamato. Sul rilievo che l'intercettazione di conversazioni per la ricerca di un latitante è sottoposta solo "*ove possibile*" al rispetto delle regole previste dall'art. 268 c.p.p., si è precisato che l'utilizzo di impianti esterni alla Procura non richiede una particolare motivazione in relazione alle indilazionabili ragioni di ur-

Alcuni autori hanno ritenuto ricavabile dal sistema la regola secondo cui solo le intercettazioni per la prosecuzione delle indagini sono suscettibili di risultati utilizzabili a fini di prova. Del resto, se così non fosse, il decreto autorizzativo per la ricerca del latitante, ove strumentalizzato a fini di prova, sarebbe privo di motivazione in ordine all'assoluta indispensabilità della stessa ai fini della prosecuzione delle indagini. E ciò in contrasto, oltre che con l'art. 267 c.p.p., con l'art. 15 Cost. che impone un atto motivato dell'Autorità giudiziaria [85].

Altra, grave breccia nel diritto alla privacy, è ravvisabile nella disciplina sulle c.d. **intercettazioni preventive**.

Le intercettazioni preventive si caratterizzano per la ***forte connotazione extraprocessuale***; in forza della quale un qualsiasi ingresso surrettizio dei risultati delle intercettazioni preventive nei *materialia iudicii* darebbe luogo alla sanzione dell'inutilizzabilità; ma, in ogni caso, la garanzia processuale dell'inutilizzabilità non può in alcun modo tutelare il diritto alla segretezza delle comunicazioni e alla privacy dei cittadini da intrusioni nella vita privata.

È evidente la natura completamente diversa tra le intercettazioni preventive, finalizzata ad un uso di indagine, e le intercettazioni investigative ordinarie, che sono configurate come una prova irripetibile, pertanto acquisite al fascicolo del dibattimento.

Nella prassi spesso si procede a intercettazioni preventive e in seguito si attuano le intercettazioni ordinarie, assodato che, le intercettazioni preventive sono utilizzabili ai fini della fase antecedente all'esercizio dell'azione penale come valide notizie di reato sulla cui base iniziare un'attività di indagine, e, dunque, come indizi sufficienti al fine di disporre le intercettazioni telefoniche o ambientali, sempreché queste riguardino delitti di cui all'art. 51, comma 3 *bis*, c.p.p. [86].

Il rischio di lesione della garanzia della privacy nell'ambito delle intercettazioni preventive è ulteriormente acuito dai numerosi soggetti che hanno il ***potere di richiedere l'autorizzazione*** per lo svolgimento delle intercettazioni preventive, attribuito al Ministro dell'Interno o, su sua delega, ai vertici dei servizi centrali interforze, al questore e ai comandanti provinciali dei Carabinieri o della Guardia di Finanza, per i gravi delitti elencati nell'art. 407, comma 2, lett. a), n. 4 e 51, comma 3-*bis*, c.p.p.

Il Ministro può, altresì, delegare il Direttore della Direzione Investigativa Antimafia limitatamente ai delitti di criminalità organizzata di stampo mafioso specificati nell'art. 51, comma 3-*bis*, c.p.p.

Inoltre, quando le suddette intercettazioni siano ritenute indispensabili per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale, esse possono essere disposte anche su iniziativa del direttore dei servizi informativi e di sicurezza, AISE e AISI, in quanto a ciò delegati dal presidente del Consiglio dei ministri, a seguito di autorizzazione del Procuratore generale della Corte d'appello del distretto ove si trova il soggetto da intercettare o dove sorgono le esigenze di prevenzione [87].

---

genza "in quanto la cattura di un latitante integra di per sé una eccezionale ragione di urgenza, con l'ulteriore conseguenza che i risultati di detta intercettazione possono essere utilizzati anche in procedimento diverso" (Cass. pen., sez. I, 4 novembre 2004, Galia ed altri, in *Mass. uff.*, 229774).

[85] L. FILIPPI, *op. cit.*, p. 253; G. ILLUMINATI, *Intercettazioni per la ricerca del latitante quali garanzie?*, cit., p. 84.

[86] Cass. pen., sez. V, 18 agosto 1998, n. 4977, Nigro, in *Cass. pen.*, 1999, p. 2914 (s.m.), *Arch. nuova proc. pen.*, 1998, 828; Cass. pen., sez. V, 18 agosto 1998, n. 4977, Albano, in *Giust. pen.*, 1999, III, p. 279.

[87] V. GREVI, *Le prove*, cit., p. 372; P. TONINI, *Manuale di procedura penale*, X ed., Milano, 2009, p. 372. La previsione è dovuta agli artt. 4 e 7-*bis*, d.l. 27 luglio 2005, n. 144, conv. con legge 31 giugno 2005, n. 155.

Molteplici sono i soggetti che possono richiedere le intercettazioni *de qua* con possibili lesioni della riservatezza dei cittadini e poche, o quasi nulle, le garanzie individuali tutelate. La dottrina più sensibile ha opportunamente segnalato come la genericità del presupposto, costituito da semplice necessità di acquisire notizie concernenti la prevenzione di alcuni gravi reati (art. 226 disp. att. c.p.p., comma 1), vanifica la garanzia dell'atto motivato; quindi da tale accorto parere, pare proliferarsi un netto contrasto con l'art. 15 Cost. [88].

In tema di misure di prevenzione, da ricordare, che esistono intercettazioni preventive per i soggetti ai quali è stata applicata la misura della sorveglianza speciale o dell'obbligo di soggiorno, quindi, riguardanti le indagini relative al procedimento per l'applicazione di una misura di prevenzione. Ma, invero, è previsto che tra i destinatari dell'autorizzazione rientrino degli ufficiali della polizia giudiziaria, i quali, e ben noto, devono, anche di propria iniziativa, prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, etc. (art. 55 c.p.p.); in altri termini, intervenire a reato commesso. Mentre, è alla polizia di sicurezza che spetta il compito di prevenire i reati e, dunque, anche di controllare i sorvegliati speciali.

Anche in detta materia si paventa una lesione delle garanzie individuali, per via del riferimento della norma a indagini di polizia giudiziaria, dirette ad accertare i reati più che prevenirli.

Insomma, anche se inespresso, emerge in maniera abbastanza chiara la volontà di sottoporre le conversazioni di determinati soggetti, nei cui confronti sia stata formulata una prognosi di pericolosità, a sorveglianza generale, mediante intercettazioni sistematiche per raccogliere informazioni su eventuali reati di cui non si aveva precedentemente notizia. L'esistenza di tale potere si traduce in pratica, in impedimento all'uso del telefono e degli altri strumenti di comunicazione, con grave lesione della liberta e segretezza delle comunicazioni e al diritto alla privacy [89].

Da quanto detto, si evince come nell'ambio delle misure volte al contrato alla criminalità organizzata, specificatamente nella disciplina delle intercettazioni telefoniche, ambientali, per la ricerca del latitante e preventive, notevoli sono le divergenze interpretative e molteplici i rischi o, le concrete lesioni, del diritto alla riservatezza di cittadini che nulla c'entrano con le organizzazioni criminali.

È evidente che lo scopo del legislatore è quello di garantire la sicurezza collettiva, tuttavia, l'auspicio rimane che il diritto alla privacy e il diritto alla sicurezza coesistano, poiché, appare preoccupante che la legislazione emergenziale, prassi ormai consolidata del legislatore italiano, invade progressivamente gran parte dei settori del diritto con una temibile capacità di consolidamento a discapito delle garanzie individuali di tutti.

Infine, sia consentito, un accenno alle recenti iniziative in tema di intercettazioni e di normativa di contrasto alla criminalità organizzata.

Per quanto riguarda il contrasto alla criminalità organizzata rilevante è il d.l. 4 febbraio 2010, n. 4 (pubblicato in *G.U.* 3 aprile 2010, n. 78), concernente l'istituzione dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata.

Il piano attuativo del Governo è composto da diversi punti, tra i quali, rilevano, ai fini sopra evidenziati: la realizzazione di un codice delle leggi antimafia, volto a razionalizzare meglio la normativa di contrasto e ad attuare concretamente il *doppio binario*, con il rischio, pe-

[88] L. FILIPPI, *op. cit*., p. 258.

[89] G. ILLUMINATI, *sub art. 16 l. 13 settembre 1982 n. 646 (Norme Antimafia)*, in *Legisl. pen*., 1983, p. 322. Vedi anche C. DI MARTINO-T. PROCACCIANTI, *op. cit*., p. 85.

rò, evidente, di creare un *corpus* normativo repressivo che si allontana sempre più dalle garanzie individuali previste nel codice di rito [90].

Le regole "*derogatorie*", non più presenti nel codice di rito, non consentiranno di cogliere l'effettiva ragionevolezza e necessità delle singole disposizioni "*speciali*".

Per quanto concerne i progetti di riforma della disciplina sulle intercettazioni telefoniche, il recente disegno di legge proposto dal ministro Angelino Alfano e già approvato alla Camera l'11 giugno 2009, proseguendo nella politica del doppio binario, introduce per i reati di mafia e terrorismo (più precisamente, per i delitti elencati ai commi 3-*bis* e 3-*quater* dell'art. 51 c.p.p.) deroghe: non evidenti indizi di reato ma "*sufficienti indizi di reato*", termini più lunghi di efficacia dei provvedimenti autorizzativi (quaranta giorni in prima battuta, e venti per le proroghe), sostanziale assenza di limiti di durata, dato che, quest'ultimo coincide con i termini massimi dell'indagine preliminare, non necessità, per le cd. intercettazioni ambientali, di elementi che denuncino lo svolgimento contestuale dell'attività delittuosa, neppure nei luoghi di privata dimora [91].

Viene altresì risolto normativamente il problema dell'utilizzabilità dei risultanti delle intercettazioni a seguito della ***riqualificazione giuridica*** del fatto.

È previsto che i risultati delle intercettazioni non possono essere utilizzati qualora, nell'udienza preliminare o nel dibattimento, il fatto risulti diversamente qualificato e in relazione ad esso non sussistano i limiti di ammissibilità previsti dall'art. 266 c.p.p.

Lo stesso principio di inutilizzabilità dovrebbe valere anche per la riqualificazione di un fatto come non ascrivibile al *genus* del delitto di criminalità organizzata e per il quale, invece, siano state disposte intercettazioni usufruendo del regime derogatorio.

In conclusione, dal disegno di legge, si evince un sistema di deroghe alla disciplina ordinaria che rimane vincolato all'evanescente nozione di delitti di criminalità organizzata sancita dall'art. 53, comma 3 *bis* e 3-*quater* c.p.p.; con alcune opportune soluzioni rispetto al passato ma, con tanti nuovi interrogativi; il legislatore non ha colto l'occasione per applicare in detta materia nuovi criteri di marcata tassatività volti a meglio tutelare il diritto alla privacy dei cittadini.

L'auspicio è la ricerca di un giusto equilibrio che possa affinare e migliorare il doppio binario già esistente nell'ordinamento italiano ma che non perda di vista i diritti costituzionalmente garantiti.

I naturali interlocutori in quest'opera di ricerca di punti di equilibrio sono: il legislatore che ha la responsabilità di formulare le regole che cristallizzano questi bilanciamenti; la corte costituzionale, che ha il compito di tutelare i diritti fondamentali dell'individuo anche contro la volontà della maggioranza precipitata nella legge e, infine, i giudici ordinari, ai quali spetta il compito di concretizzare la volontà legislativa nel singolo caso, riempiendo di contenuto la norma, compito particolarmente delicato e importante quando la norma è connotata da un elevato grado di vaghezza.

Il diritto penale è potere giuridicamente regolato: potere, cioè, che si dispiega attraverso un tasso di elevata formalizzazione; che vede la partecipazione di più attori istituzionali in tutte le decisioni che concernono i diritti fondamentali dell'individuo; che contempla meccani-

[90] Sul punto si veda *Altalex*, quotidiano di informazione giuridica, n. 2824, 7 aprile 2010, sul sito *www.altalex.com*.

[91] Per maggiori approfondimenti sul disegno di legge presentato dal Ministro Angelino Alfano, approvato dalla Camera dei Deputati l'11 giugno 2009, n. 1611, F. RUGGIERI, *Il disegno di legge governativo sulle intercettazioni: poche note positive e molte perplessità*, in *Cass. pen*., 2008, 6, p. 2239.

L. GUGLIELMO, *Disegno di legge Intercettazioni*, pubblicata scheda sul disegno di legge sul sito Magistratura Democratica, 16 febbraio 2010, *http://magistraturademocratica.it/node/2278*.

smi di controllo e di revisione di quelle stesse decisioni; che consente sempre all'individuo di essere ascoltato, e di far valere la propria versione dei fatti; e che vincola l'autorità giurisdizionale a dar conto analiticamente, al metro di standard probatori diversamente modulati nel corso del giudizio, delle ragioni del provvedimento limitativo dei diritti dell'individuo.

La dottrina penalistica deve difendere il ruolo del sistema penale quale strumento di contrasto anche rispetto alla criminalità organizzata, contro tutte le spinte che vorrebbero invece affidarne l'intera responsabilità – sotto la parola d'ordine della 'guerra' – al potere esecutivo. Ciò in quanto il sistema penale rappresenta ancora il migliore strumento a nostra disposizione per minimizzare i rischi di abusi e il rispetto delle garanzie individuali [92].

Tuttavia, la sfida criminale che ci aspetta è estremamente seria ed esige di essere combattuta con strumenti incisivi anche a costo di tollerare la limitazione di taluni diritti e talune garanzie, nel bilanciamento con le antinomiche ragioni della sicurezza.

Compito della dottrina penalistica dovrà, allora, essere quello di raccogliere la sfida, e di rendersi disponibile a cooperare con gli attori del diritto penale – legislatori e giudici – nella faticosa opera di bilanciamento tra sicurezza e diritti.

Questo si è fatto per quanto riguarda la criminalità organizzata di tipo mafioso e si dovrà procedere in tal senso anche per il crimine organizzato di natura terroristica o eversiva. Si dovranno sempre rispettare le garanzie individuali di qualsiasi indagato e limitarle solo se necessario, nei modi e nei termini previsti dalla legge, con delle norme tassative, con il controllo dell'autorità giudiziaria e nel rispetto della Carta costituzionale; concedendo all'indagato – imputato la possibilità di raccogliere elementi di prova a proprio favore, difendersi provando la propria innocenza, proponendo istanze di vario tipo e chiedendo il riesame della sua posizione, nonché proponendo appello avverso decisioni errate, in concreto, esercitando tutti i diritti e facoltà che solo il diritto penale sostanziale e processuale offrono nel rispetto del principio di parità delle armi.

[92] F. VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. e proc. pen.*, 2006, 2, p. 648.

CAPITOLO 8

La riforma dei reati di danneggiamento informatico ad opera della legge n. 48 del 2008

di *Claudia Pecorella*

SOMMARIO: 1. Premessa. – 2. Le diverse figure di danneggiamento informatico introdotte nel codice penale dalla legge n. 547 del 1993 e le esigenze di riforma. – 3. Il deludente intervento del legislatore del 2008.

1. Premessa

La ratifica della Convenzione di Budapest sul *Cybercrime* rappresentava per il legislatore italiano una buona occasione per intervenire sulla normativa in materia di reati informatici, introdotta nel nostro ordinamento con la legge n. 547 del 1993. Nei quindici anni trascorsi dall'entrata in vigore di quella legge erano emersi profili di inadeguatezza e di ambiguità di alcune delle disposizioni inserite nel codice penale per la repressione delle nuove forme di aggressione rese possibili dall'informatica: era il caso, soprattutto, della *frode informatica* (art. 640-*ter* c.p.) e dell'*accesso abusivo a un sistema informatico* (art. 615-*ter* c.p.), sui quali la giurisprudenza aveva avuto più spesso occasione di pronunciarsi, pervenendo a interpretazioni divergenti e talvolta poco compatibili con la *ratio* sottostante alla loro introduzione nel nostro sistema penale [1].

Meno problematiche apparivano le diverse ipotesi di *danneggiamento informatico* presenti nel codice penale, oggetto di scarsissima applicazione giurisprudenziale alla luce, quantomeno, della giurisprudenza edita. Tuttavia, anche rispetto a quelle disposizioni sembravano opportune alcune modifiche e soprattutto era avvertita l'esigenza di una maggiore uniformità, sul piano della formulazione legislativa, nell'individuazione degli eventi lesivi che esse erano dirette a reprimere.

Alle aggressioni all'integrità dei dati e dei sistemi informatici il legislatore del 1993 aveva dedicato particolare attenzione, non limitandosi a recepire le indicazioni contenute nella Raccomandazione del Consiglio d'Europa sulla criminalità informatica del 1989 e quelle ulteriori emerse, nel corso dei primi anni '90, nei colloqui preparatori del XV Congresso internazionale dell'AIDP – che aveva tra i suoi temi anche la criminalità informatica –, ma rivolgendo anche lo sguardo a quelle figure tradizionali di reato che, pur dirette alla tutela di beni diversi dal patrimonio, si erano rivelate nella prassi altrettanto utili nella repressione del danneggiamento informatico, tanto che appariva opportuno sancirne in modo espresso e chiaro il nuovo ambito di operatività. Mi riferisco al delitto di esercizio arbitrario delle proprie ragioni con

[1] A questo proposito, rinvio al testo della relazione svolta alla Conferenza internazionale sul tema "*Computer crimes e cyber crimes*: offese globali, risposte globali. Aspetti sostanziali e processuali del diritto penale dell'informatica in dimensione europea e internazionale" (Verona, 26-27 ottobre 2007), in corso di pubblicazione negli Atti.

violenza sulle cose (art. 392 c.p.) e di attentato ad impianti di pubblica utilità (art. 420 c.p.).

Le nuove disposizioni sui reati informatici erano state disseminate all'*interno del codice penale*, in base ad una scelta condivisibile del legislatore del 1993 che, sulla falsariga di quanto suggerito dal Consiglio d'Europa – che metteva in guardia dal pericolo di una *overcriminalization* delle condotte di abuso dell'informatica –, si era limitato a colmare i vuoti di tutela, derivanti dalla impossibilità o difficoltà di ricorrere alle fattispecie tradizionali allorquando il fatto si fosse realizzato servendosi di un elaboratore elettronico (era il caso, ad esempio, della truffa) o avesse riguardato beni informatici immateriali, come i dati e i programmi (non assimilabili alle "cose mobili altrui" ai fini proprio del danneggiamento). Quella scelta ha condizionato anche la *collocazione sistematica* delle nuove figure di reato all'interno del codice penale: appropriato è stato considerato il loro inserimento in prossimità delle fattispecie tradizionali che erano risultate non applicabili o applicabili solo con difficoltà e a certe condizioni alle diverse manifestazioni del nuovo fenomeno criminale. Una soluzione che rende evidente come attraverso la tecnologia informatica si siano solo rese possibili nuove modalità di aggressione a beni già oggetto di tutela nell'ordinamento (il patrimonio, la fede pubblica, la riservatezza individuale etc.) e che dovrebbe facilitare l'interprete nella ricostruzione degli specifici obiettivi di tutela delle nuove norme incriminatrici. Sotto questo profilo, per fortuna, la legge n. 48 del 2008 non ha attuato alcun capovolgimento di prospettiva, anche se, proprio con riguardo ai delitti di danneggiamento, si è (inspiegabilmente) spostata all'interno dei delitti contro il patrimonio la figura dell'attentato a sistemi informatici di pubblica utilità (art. 420 c.p.) e si è invece persa l'occasione per correggere l'impropria collocazione della disposizione sulla diffusione di programmi virus (art. 615-*quinquies* c.p.) tra i delitti contro l'inviolabilità del domicilio.

2. Le diverse figure di danneggiamento informatico introdotte nel codice penale dalla legge 547/1993 e le esigenze di riforma

Uno sguardo più da vicino all'intervento in tema di danneggiamento informatico, realizzato con la legge n. 547 del 1993, mi pare necessario per poter cogliere il senso complessivo della riforma attuata con la legge n. 48 del 2008.

a) Recependo le indicazioni del Consiglio d'Europa, era stata innanzitutto inserita all'interno dei delitti contro il patrimonio una figura "generale" di *danneggiamento di sistemi informatici e telematici* (art. 635-*bis* c.p.) che, ricalcando pressoché pedissequamente quella tradizionale (art. 635 c.p.), reprimeva le aggressioni all'integrità e alla funzionalità tanto della componente materiale (il 'sistema informatico') quanto di quella immateriale, rappresentata da "programmi, informazioni o dati altrui"[2]. Si era invece rinunciato all'introduzione di un'ulteriore fattispecie di "sabotaggio informatico" che, stando alla Raccomandazione del 1989, avrebbe dovuto reprimere condotte di danneggiamento di dati e programmi, o di ingerenza in un sistema informatico, che fossero accompagnate dall'*intenzione* di "ostacolare il funzionamento di un sistema informatico o di un sistema di telecomunicazione". A questo proposito, è stata verosimilmente ritenuta sufficiente la tutela assicurata ai "sistemi informatici" (oltreché ai dati e ai programmi) con l'introduzione del nuovo art. 635-*bis* c.p. e con l'am-

[2] Prima della sua sostituzione ad opera della legge n. 48 del 2008, l'art. 635-*bis* c.p. disponeva: "*Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni*".

pliamento dell'art. 420 c.p., avente ad oggetto sistemi informatici *di pubblica utilità*[3].

Anteriormente all'entrata in vigore della legge n. 547 del 1993, la giurisprudenza aveva ritenuto applicabile la figura tradizionale del danneggiamento di *cose* altrui (art. 635 c.p.) all'illegittima cancellazione di un programma, in considerazione della "inservibilità" del sistema informatico che ne era derivata[4]. Coerentemente con quella soluzione, l'unica pronuncia edita sul reato di danneggiamento informatico, successivamente introdotto nel codice penale, si è limitata a ribadire la punibilità della cancellazione di dati dalla memoria di un *computer* ai sensi dell'art. 635 c.p., pervenendo peraltro ad escludere l'operatività retroattiva della disposizione speciale, contenuta nell'art. 635-*bis* c.p., per la sanzione più grave in essa prevista[5]. Per il danneggiamento informatico era, infatti, prevista la stessa pena (reclusione da sei mesi a tre anni) originariamente contemplata per il danneggiamento aggravato di cose ai sensi del secondo comma dell'art. 635 c.p.: una soluzione non del tutto comprensibile – perché "la dimensione informatica di un delitto non deve essere considerata in quanto tale una circostanza aggravante del delitto stesso"[6] – e diventata ancora più problematica da quando, con il d.lgs. n. 274 del 2000, il delitto tradizionale di danneggiamento è stato devoluto alla competenza penale del giudice di pace, alla quale è estranea l'applicazione della pena detentiva.

A parte questo profilo, la nuova fattispecie di danneggiamento informatico risultava, da un lato, inutilmente e pericolosamente ampia nell'espressa menzione delle "informazioni" (accanto ai dati e ai programmi) tra i beni suscettibili di aggressione – perché si prestava a far rientrare nella più grave figura delineata dall'art. 635-*bis* c.p. il "danneggiamento" di informazioni non ancora (o non più) codificate in dati, ma contenute su un supporto materiale, di tipo tradizionale, come un semplice foglio di carta – e dall'altro lato, eccessivamente delimitata nel richiedere che i dati e i programmi oggetto di danneggiamento informatico fossero "altrui". Non solo valevano anche qui le ragioni che, con riferimento alla fattispecie tradizionale di danneggiamento, avevano evidenziato la necessità di tutelare anche il titolare di un diritto di godimento su beni altrui, proprio nei confronti di condotte aggressive poste in essere dal proprietario del bene, ma appariva insuperabile la difficoltà di attribuire un diritto di proprietà su cose incorporee come i dati informatici e del tutto inadeguata una soluzione interpretativa che identificasse sempre e comunque nel proprietario del supporto, sul quale i dati fossero stati registrati, la persona avente diritto di disporre dei dati stessi[7].

Con riguardo infine alle circostanze aggravanti contemplate nel secondo comma dell'art. 635-*bis* c.p., a parte l'inapplicabilità di gran parte di quelle contenute nel comma 2 dell'art. 635 c.p. al quale veniva fatto rinvio, particolarmente ambigua risultava quella consistente nell'*abuso della "qualità di operatore di sistema"*, per le incertezze interpretative cui dava luo-

[3] Nella sua originaria formulazione, l'art. 420 c.p., sotto la rubrica "Attentato a impianti di pubblica utilità", prevedeva che la pena della reclusione da uno a quattro anni, comminata nel primo comma per *i fatti diretti a danneggiare o distruggere* impianti di pubblica utilità, fosse applicabile anche nel caso in cui l'attentato avesse ad oggetto "sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti". Il terzo e ultimo comma dell'art. 420 c.p. prevedeva poi una pena più severa (la reclusione da tre a otto anni) per l'ipotesi in cui dal fatto fosse derivata "la distruzione o il danneggiamento (…) del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione anche parziale del funzionamento (…) del sistema".

[4] Cfr. Pret. Torino, 23 ottobre 1989, Vincenti, in *Foro it.*, 1990, II, c. 462 ss. con nota di R. CASO; App. Torino, 29 novembre 1990, Vincenti, *ivi*, 1991, II, c. 228.

[5] Cfr. Cass., sez. un., 9 ottobre 1996, Carpanelli, in *Cass. pen.*, 1997, 2428 ss. con nota di G. TOMEI.

[6] Così COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS, *La criminalité informatique – Rapport final*, Strasbourg, 1990, p. 23.

[7] Cfr., in proposito, C. PECORELLA, *Il diritto penale dell'informatica*, rist. con aggiornamento, Padova, 2006, p. 204 ss.

go; incertezze che erano destinate, tra l'altro, a riproporsi nei confronti di tutte le figure di reato informatico per le quali tale aggravante era pure prevista [8]. Controverso era risultato il significato della locuzione "operatore di sistema", non corrispondente ad alcuna figura professionale specifica nel campo dell'informatica, e quindi identificabile vuoi con l'amministratore *di sistema*, per i particolari poteri sull'elaboratore che ad esso competono – secondo la tesi più restrittiva e più condivisibile – vuoi con l'*operatore* al terminale, che di regola è sprovvisto di alcun potere operativo sul sistema propriamente detto [9].

b) Sollecitata in ambito internazionale, ad opera questa volta del XV Congresso dell'AIDP, è stata anche l'introduzione nel codice penale della disposizione che reprime la *diffusione di programmi diretti a danneggiare o interrompere un sistema informatico* (art. 615-*quinquies* c.p.) [10]. Nonostante l'impropria collocazione sistematica, quella figura di reato mirava a rafforzare la tutela dell'integrità e della funzionalità di dati e sistemi informatici, attraverso l'incriminazione di condotte pericolose (la diffusione, la comunicazione o la consegna di un programma "avente per scopo o per effetto il danneggiamento" di un sistema o dei suoi dati), in quanto prodromiche alla possibile realizzazione di un danneggiamento informatico da parte di chi fosse venuto in possesso di un programma avente quelle caratteristiche. La "forte" anticipazione della tutela realizzata attraverso l'art. 615-*quinquies* c.p. poteva ritenersi legittima, alla luce del principio di proporzione, per l'importanza che assumono nella nostra vita privata e pubblica l'integrità e la funzionalità dei sistemi informatici e dei dati che essi gestiscono.

Tralasciando le perplessità sollevate dalla dottrina sulla mancata previsione di un dolo specifico di danno all'interno della fattispecie, che avrebbe rimosso ogni dubbio sulla liceità della consegna di un programma *virus* ad un esperto informatico ai fini della individuazione di un possibile antidoto [11], il profilo davvero problematico del reato in esame mi pare fosse quello del rapporto con il danneggiamento informatico (art. 635-*bis* c.p.), che sarebbe stato integrato tutte le volte in cui il programma illecitamente diffuso o consegnato ad altri fosse stato poi effettivamente utilizzato da chi ne era venuto illecitamente in possesso. Più precisamente, sarebbe stata necessaria una coincidenza tra i fatti puniti, in via anticipata, attraverso l'art. 615-*quinquies* c.p. e quelli sanzionati, più gravemente e in uno stadio successivo, da tutte le altre disposizioni che, in aggiunta all'art. 635-*bis* c.p., consideravano il danneggiamento dei sistemi informatici e delle loro componenti immateriali come elemento costitutivo o circostanza aggravante di un diverso reato.

[8] Cfr. artt. 640-*ter* (frode informatica), 615-*ter* (Accesso abusivo a un sistema informatico) e 615-*quater* (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici), 617-*quater* (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche), 617-*quinquies* (Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche) e 617-*sexies* (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche) c.p.

[9] Per le diverse interpretazioni, cfr. C. PECORELLA, *Commento all'art. 615-ter*, in E. DOLCINI-G. MARINUCCI (a cura di), *Codice penale commentato*, III ed., Milano, 2011; in giurisprudenza, per la configurabilità dell'aggravante in capo all'impiegato di banca, abilitato all'uso del terminale per registrare le quotidiane operazioni di cassa, cfr. M.M. ALMA-C. PERRONI, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997, p. 504 ss.

[10] Anche su questa disposizione, come si vedrà, è intervenuto il legislatore del 2008; nella sua versione originaria, l'art. 615-*quinquies* c.p. prevedeva la pena della reclusione fino a due anni e della multa fino a 10.329 euro per "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento".

[11] A ben vedere, tuttavia, all'estromissione di queste condotte dall'ambito di applicazione dell'art. 615-*quinquies* c.p. si sarebbe potuto (e dovuto) già pervenire sul piano interpretativo, considerando rilevanti solo condotte tipicamente pericolose per il bene protetto (quali certo non possono essere considerate quelle menzionate).

A questo riguardo, poco comprensibile appariva, all'interno dell'art. 615-*quinquies* c.p., il riferimento alla "interruzione, totale o parziale" e alla "alterazione" del funzionamento del sistema, tra gli scopi o gli effetti possibili del programma oggetto di illecita diffusione, come eventi ulteriori rispetto al più generico "danneggiamento". A quest'ultimo erano, infatti, riconducibili tutti gli eventi dannosi dai quali poteva derivare una responsabilità per il reato previsto nell'art. 635-*bis* c.p., e quindi anche l'inservibilità totale o parziale del sistema o dei suoi dati, che tra quegli eventi era contemplata e che era destinata a realizzarsi ogniqualvolta il funzionamento del sistema fosse stato "interrotto" o "alterato".

Le inaccettabili conseguenze che potevano derivare da quella inopportuna duplicazione di concetti tra le due disposizioni (e più in generale, tra le diverse disposizioni in materia di danneggiamento informatico) si possono cogliere nella sentenza della Corte d'appello di Bologna sul caso Vierika, che costituisce uno dei due casi soltanto di diffusione di programmi "infetti" sui quali la giurisprudenza ha avuto occasione di pronunciarsi [12]. Dopo aver escluso che, nel caso specifico sottoposto al loro esame, l'abbassamento del livello di sicurezza impostato dall'utente per la selezione delle informazioni reperibili in Rete – che costituiva un effetto del programma Vierika – potesse qualificarsi come "danneggiamento del sistema" (ai sensi, in particolare, dell'art. 615-*ter*, comma 2, n. 3, c.p., per il quale in primo grado l'imputato era stato altresì condannato), i giudici bolognesi hanno ritenuto realizzata un'ipotesi di "alterazione" del funzionamento del sistema, rilevante (esclusivamente) ai sensi dell'art. 615-*quinquies* c.p. [13]. A tal fine si è precisato che "alterare" il funzionamento di un sistema equivale a "manipolarlo in modo che compia azioni non volute dall'utente, ovvero modificarne i parametri di funzionamento, anche secondo opzioni e possibilità previste nel programma stesso, contro la volontà dell'utilizzatore". Attraverso quella interpretazione – che presuppone una sostanziale coincidenza tra la (mera) modifica del funzionamento del sistema informatico e la (diversa e più grave) "alterazione" di esso –, si era compromesso quel rapporto, che ritengo necessario, tra la norma che punisce la condotta prodromica (la diffusione di un programma diretto a danneggiare) e tutte quelle che sanzionano i suoi eventuali sviluppi successivi (la verificazione del danno temuto). L'alterazione del funzionamento del sistema, non comportando un vero e proprio danneggiamento del sistema, in base alla valutazione dei giudici del caso in esame, non sarebbe stata punibile ad alcun titolo in base alle diverse disposizioni in materia di danneggiamento informatico, che quel particolare evento (dannoso?) non menzionano; attraverso l'art. 615-*quinquies* c.p. si sarebbe potuto dunque punire una condotta "pericolosa" che, se fosse stata portata a conseguenze ulteriori, non avrebbe cagionato un danno penalmente rilevante.

c) Vanno infine ricordate due diverse fattispecie di reato che erano state ampliate dal legislatore del 1993 in corrispondenza con la nuova figura generale di danneggiamento informatico, contestualmente inserita nel codice penale. Si trattava, in particolare, del delitto di *esercizio arbitrario delle proprie ragioni con violenza sulle cose* (art. 392 c.p.) e dell'*attentato a impianti di pubblica utilità* (art. 420 c.p.), che erano stati oggetto di applicazione giurisprudenziale proprio in casi di danneggiamento informatico, come prima ho ricordato.

Rispetto al primo, si era ampliata la nozione di violenza sulle cose attraverso, tra l'altro, il

[12] In un altro caso, il *fumus* di questo reato era stato ravvisato nella comunicazione di un *dialer* che, per sostituire il sistema di connessione in uso con un altro a prezzo maggiorato, aveva provocato per un brevissimo lasso di tempo l'interruzione della connessione alla Rete del sistema informatico: cfr. Trib. La Spezia, 23 settembre 2004, in *Giur. merito*, 2005, 3, p. 615.

[13] La sentenza della Corte d'Appello di Bologna sul caso Vierika è reperibile sul sito *www.penale.it*; per quella di primo grado, cfr. Trib. Bologna, 21 luglio 2005, in *Corr. merito*, 2006, p. 759 ss. con nota di F. D'ARCANGELO.

riferimento alla "alterazione, modificazione o cancellazione di un *programma informatico*". A questo riguardo mi limito a segnalare che, se proprio rispetto ad un caso di cancellazione di un programma informatico si era posto in passato il problema dell'applicabilità del reato di esercizio arbitrario delle proprie ragioni con violenza sulle cose (non essendo configurabile nel caso concreto il danneggiamento, perché l'autore era proprietario del programma) [14], sarebbe stato opportuno che anche il danneggiamento dei *dati* fosse ricompreso nell'ambito della definizione di violenza sulle cose, diretta per di più ad operare "agli effetti della legge penale".

Per quanto riguarda, invece, il secondo, si era chiarito che anche i sistemi informatici (e non solo gli impianti) dovessero essere "di pubblica utilità" perché l'aggressione a essi rivolta potesse integrare il reato in esame e risultare offensiva del bene tutelato (l'ordine pubblico), e si era estesa la punibilità alle condotte aventi ad oggetto "dati, *informazioni* o programmi" contenuti in quei sistemi o "ad essi pertinenti". Un corrispondente ampliamento aveva subito l'ultimo comma dell'articolo in esame, che prevedeva un aggravamento della pena per l'ipotesi in cui si verificasse la "distruzione o il danneggiamento" del sistema o dei suoi dati e programmi, ovvero la "interruzione anche parziale del funzionamento" del sistema. Si riproponevano quindi le stesse perplessità già segnalate sull'espressa menzione delle "informazioni" tra i beni suscettibili di aggressione e sulla "inspiegabile difformità di linguaggio" [15] nell'indicazione degli eventi dannosi al cui verificarsi conseguiva l'aggravamento della sanzione.

In conclusione, si può affermare che le disposizioni sul danneggiamento informatico inserite nel codice penale con la legge n. 547 del 1993 non si segnalassero all'attenzione del legislatore per la necessità di urgenti modifiche (diversamente da quelle sulla frode informatica e sull'accesso abusivo), anche alla luce della scarsa applicazione giurisprudenziale che esse avevano ricevuto. L'occasione offerta dall'attuazione della Convenzione di Budapest ben si prestava, tuttavia, ad un intervento di "correzione" di alcuni aspetti specifici di singole disposizioni, per assicurarne in futuro un'applicazione coerente con gli obiettivi di tutela perseguiti: alludo all'ampliamento della nozione di violenza sulle cose contenuta nel terzo comma dell'art. 392 c.p., alla eliminazione delle "informazioni" tra i beni suscettibili di danneggiamento informatico e all'ampliamento della tutela apprestata dall'art. 635-*bis* c.p. ai beni informatici nei confronti delle aggressioni realizzate (eventualmente anche dal proprietario, laddove un diritto di proprietà sia configurabile) in violazione di un diritto altrui. Più in generale, mi sembrava necessario intervenire sulla formulazione delle diverse disposizioni, per assicurare un miglior coordinamento tra loro e, rispetto all'aggravante dell'abuso della qualità di operatore di sistema, per dare indicazioni univoche alla giurisprudenza sulla *ratio* di quella maggiore punibilità.

3. Il deludente intervento del legislatore del 2008

Niente (o quasi) di quello che ci si poteva aspettare è stato realizzato con la legge n. 48 del 2008, che ha moltiplicato le figure di danneggiamento informatico, rendendo autonome le fattispecie, rispettivamente, di *danneggiamento di dati e programmi* (art. 635-*bis* c.p.) e di *danneggiamento di sistemi informatici* (art. 635-*quater* c.p.) – come suggerito dalla Conven-

[14] Cfr. Trib. Torino, 12 dicembre 1983, Basile, in *Giur. it.*, 1984, II, c. 352 ss. con nota di A. FIGONE.

[15] Così F. MANTOVANI, *Diritto penale. Parte speciale I, Delitti contro la persona*, Padova, 2005, p. 504, per il quale quella difformità, frutto di una sorta di "logorrea legislativa", comprometterebbe "il necessario ordine sistematico" delle disposizioni in esame.

zione di Budapest – e affiancando a ciascuna di esse una corrispondente ipotesi speciale, caratterizzata dalla *pubblica utilità dei dati e dei programmi* (art. 635-*ter* c.p.) e *dei sistemi* (art. 635-*quinquies* c.p.), nonché dall'anticipazione della tutela penale secondo il modello del delitto di attentato proprio dell'art. 420 c.p., che è stato, infatti, abrogato in quella sua parte.

Non si tratta tuttavia di una mera risistemazione di norme già contemplate nell'ordinamento: il legislatore ha proceduto anche a una loro riformulazione, che purtroppo, se non ha evitato la riproposizione di quegli stessi aspetti problematici prima evidenziati, ha finito col rendere particolarmente complesse fattispecie di reato che nella loro versione originaria erano certamente più chiare e altrettanto (se non maggiormente) ampie nella ricomprensione dei fatti di danneggiamento informatico ritenuti meritevoli di sanzione penale.

Sul piano sanzionatorio, la distinzione introdotta, tra danneggiamento di dati e danneggiamento di sistemi, ha comportato per quest'ultima ipotesi un inasprimento della pena, perché dalla reclusione da 6 mesi a 3 anni – prevista dall'originario art. 635-*bis* c.p. per il danneggiamento informatico e oggi solo per quello rivolto alla componente logica –, si è pervenuti alla reclusione da 1 a 5 anni. Invariata è rimasta invece, rispetto a quella in precedenza comminata nell'art. 420 c.p., la pena per le due ipotesi di attentato, nei confronti delle quali nessun diverso disvalore è attribuito alla circostanza che sia l'intero sistema informatico di pubblica utilità a essere coinvolto dall'aggressione anziché solo i suoi dati o programmi: una soluzione che poteva essere ragionevole quando anche il danneggiamento dei dati e dei sistemi era sottoposto ad un medesimo trattamento sanzionatorio, ma che genera oggi disarmonie nel sistema, per l'indubbia maggiore gravità che viene ad essere attribuita al danneggiamento di *dati* di pubblica utilità rispetto all'ipotesi generale (anticipazione della rilevanza penale alla soglia dell'attentato e contestuale inasprimento del minimo e del massimo edittale, oltreché perseguibilità d'ufficio), anziché al danneggiamento di *sistemi* di pubblica utilità che, pur in presenza della stessa anticipazione della tutela, viene punito con una sanzione uguale nel minimo e addirittura *inferiore* nel massimo, rispetto a quella contemplata per la figura base dall'art. 635-*quater* c.p.

Va anche segnalata l'estensione ai delitti di attentato a dati e sistemi di pubblica utilità delle stesse circostanze aggravanti previste per le altre ipotesi di danneggiamento informatico: al riguardo, se meritevole di apprezzamento è la razionalizzazione del rinvio alle circostanze previste dal secondo comma dell'art. 635 c.p. – oggi limitato a quella dell'uso di violenza alla persona o di minaccia –, non si può certo salutare con favore il più esteso impiego di quella consistente nell'abuso della qualità di operatore di sistema, per quella sua intrinseca ambiguità, cui ho in precedenza accennato e alla quale il legislatore del 2008 non ha posto rimedio.

Venendo poi alla formulazione delle nuove fattispecie, si può notare che la figura base di danneggiamento di dati e programmi (art. 635-*bis* c.p.) riproduce per lo più il testo dell'art. 4 della Convenzione sul *Cybercrime*: l'ipotesi della "inservibilità totale o parziale" dei dati e dei programmi che, sulla falsariga della fattispecie tradizionale, era inserita nell'originario art. 635-*bis* c.p., è stata sostituita con le diverse ipotesi della "cancellazione, alterazione e soppressione" degli stessi. Un'operazione che, se da un lato ha aggiunto eventi dannosi *già ricompresi* nella norma (cancellare o sopprimere dati e programmi corrisponde, in termini più appropriati, a quella che veniva e viene ancora indicata come loro "distruzione"), dall'altro lato rischia di sollevare problemi sulla consistenza della "alterazione", alla luce della (ben lata) interpretazione di questo termine, accolta dalla Corte d'appello di Bologna nel caso Vierika prima ricordato. Con una vena di ottimismo si può tuttavia sperare che proprio la presenza di questa ipotesi all'interno di una disposizione volta a reprimere il danneggiamento dei dati, e la sua equiparazione, nella descrizione del fatto tipico, ad altre ipotesi di indubbia connotazione lesiva induca la giurisprudenza ad un'interpretazione filologicamente corretta di quel termine, che ne colga la differenza rispetto alla mera "modificazione".

Più problematica è forse la scomparsa dalla fattispecie dell'ipotesi della "inservibilità", che si prestava a ricomprendere tutte quelle forme di danneggiamento informatico che non comportano né una cancellazione né un deterioramento dei dati e dei programmi, ma ne compromettono la funzionalità: è il caso, ad esempio, di quegli interventi sui dati che li rendono inaccessibili al legittimo utente del sistema, come l'introduzione di una chiave d'accesso prima inesistente. Oggi quelle condotte sono rilevanti ai sensi del più grave reato di danneggiamento di sistemi, ove determinino l'inservibilità del sistema stesso e sempreché si realizzino con una di quelle modalità richieste dall'art. 635-*quater* c.p. per la punibilità del fatto: la causazione ai dati o ai programmi di uno degli eventi indicati dall'art. 635-*bis* c.p., ovvero "l'introduzione o la trasmissione di dati, informazioni e programmi". Solo a queste condizioni – che solo l'esperienza applicativa potrà chiarire se esaustive o meno – risulta oggi penalmente rilevante la "distruzione, il danneggiamento o l'inservibilità totale o parziale" del sistema, così come il fatto di aver ostacolato gravemente il suo funzionamento; di sicuro può dirsi che il danneggiamento (ivi compresa la distruzione) di un sistema informatico, che non sia causato da un intervento sulla sua componente logica, non ricadrà nell'art. 635-*quater* c.p., ma sarà punibile in base alla disposizione, molto meno grave, sul danneggiamento di cose (art. 635 c.p.), con la quale concorrerà quella sul danneggiamento dei dati e dei programmi (art. 635-*bis* c.p.), ogniqualvolta questi ultimi siano indirettamente coinvolti [16].

Il danneggiamento dei *sistemi informatici* ha perso dunque quella connotazione di reato causale puro che aveva l'originario art. 635-*bis* c.p. e che ancora possiedono l'art. 635 c.p. e il nuovo art. 635-*bis* c.p.: a questo risultato si è pervenuti, più o meno consapevolmente, nell'intento di rendere la normativa italiana sul punto il più aderente possibile alle indicazioni contenute nell'art. 5 della Convenzione sul *Cybercrime*, che caratterizza il reato di *System interference* proprio nella causazione senza diritto di "un serio ostacolo al funzionamento di un sistema informatico, *attraverso* l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati".

Non posso tuttavia non rilevare che l'allineamento alle indicazioni della Convenzione è mancato proprio in quelle parti che avrebbero consentito di risolvere alcuni dei difetti della nostra normativa originaria: alludo all'espressa menzione del danneggiamento di "informazioni" – che sarebbe scomparsa, a favore di un generico riferimento ai "dati", senz'altro comprensivo dei dati che formano un programma informatico – e al requisito della "altruità" di dati, programmi e sistemi informatici, che sarebbe stato sostituito da una clausola di illiceità espressa, equivalente all'espressione inglese *without right* utilizzata dalla Convenzione.

Qualche considerazione infine sulle modifiche che hanno riguardato l'art. 615-*quinquies* c.p. e che hanno trasformato sensibilmente la fattispecie originaria, trasferendo sul piano dell'elemento soggettivo quei caratteri di oggettiva pericolosità che prima dovevano possedere i programmi oggetto di diffusione illecita. In base alla sua nuova formulazione, la norma punisce un ampio spettro di condotte, aventi ad oggetto programmi informatici, dispositivi o apparecchiature, non altrimenti qualificati, la cui pericolosità, rispetto alla possibile futura realizzazione di un danneggiamento informatico, deriva soltanto dallo *scopo* perseguito dall'agente. È solo il dolo specifico di danno, il cui oggetto viene dettagliatamente indicato dalla legge (e ricomprende il danneggiamento del sistema o dei suoi dati, così come la volontà di favorire l'interruzione o l'alterazione del funzionamento del sistema), che rende punibili delle condotte di per sé neutre, consistenti nel diffondere o mettere in qualsiasi modo a disposizione

[16] Alla stessa conclusione si deve pervenire rispetto alla corrispondente figura del danneggiamento di sistemi informatici *di pubblica utilità* (art. 635-*quinquies* c.p.), che risulta integrata quando "il fatto di cui all'art. 635-*quater*" è diretto a cagionare uno degli eventi dannosi menzionati in questa disposizione.

di altri quegli strumenti, ovvero nel procurarsene in vario modo la disponibilità (producendoli, riproducendoli o importandoli).

Per sottrarre l'art. 615-*quinquies* c.p. a una censura d'illegittimità costituzionale è indispensabile un'interpretazione costituzionalmente orientata che ne circoscriva l'applicazione alle sole condotte oggettivamente idonee (oltreché soggettivamente dirette) a realizzare uno degli scopi perseguiti dall'agente, in considerazione delle particolari caratteristiche o qualità dello strumento che hanno ad oggetto [17]. Certo è che l'introduzione di una disposizione siffatta non risultava imposta dalla Convenzione di Budapest, che all'art. 6 indica come meritevole di sanzione penale la condotta di chi, senza diritto, "produce, vende, si procura per l'uso, importa, distribuisce o altrimenti rende disponibile ad altri: a) un dispositivo, compreso un programma informatico, *progettato o predisposto essenzialmente per la commissione*" *di uno dei reati indicati* (oltre al danneggiamento di dati e di sistemi, l'accesso abusivo e l'intercettazione di comunicazioni informatiche), avendo l'intenzione che sia utilizzato proprio per la loro commissione. Per adeguare a quelle indicazioni la fattispecie originariamente contemplata nell'art. 615-*quinquies* c.p. sarebbe stato sufficiente ampliare l'elencazione delle condotte pericolose e soprattutto estenderne l'oggetto a quei dispositivi, diversi e ulteriori rispetto al programma informatico, aventi quella specifica funzionalità indicata dalla Convenzione.

Quanto all'anticipazione della tutela penale così realizzata – e che comunque si sarebbe realizzata, recependo le indicazioni della Convenzione – si deve tornare a fare i conti con il principio di proporzione, che se non risultava calpestato dall'incriminazione di condotte di diffusione di uno strumento pericoloso, come un programma *virus* o similare, non altrettanto pacificamente appare rispettato con l'incriminazione di condotte ancora più lontane dall'offesa, come quella di chi *produce* un siffatto programma o un dispositivo avente analoghe funzioni, sia pure *allo scopo di* realizzare un danneggiamento informatico.

[17] Cfr., in proposito, L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 708 ss.

CAPITOLO 9

L'elemento soggettivo nei reati informatici: le categorie dogmatiche in una terra di confine

di *Marco Grotto*

1. Premessa

Affrontare le tematiche del "diritto dell'informatica" è l'occasione per riflettere su alcune categorie generali del diritto penale.

Una normativa così specifica, qual è quella in tema di reati informatici, e, soprattutto, la necessità di dare regolamentazione giuridica ad un mondo sempre più "virtuale" e sempre meno "reale" sottopongono gli istituti della parte generale del diritto penale a tensioni (quando non a "torsioni") interpretative ed applicative. A dimostrazione di questo assunto intendo proporre tre esempi: due di matrice giurisprudenziale (caso 1 e caso 2) ed un terzo, duplice (caso 3), relativo alla formulazione impressa dal legislatore a due norme incriminatrici.

2. Caso 1. Basta la colpa cosciente per ritenere provato il dolo eventuale?

Come noto, il codice penale italiano contiene una definizione dei concetti generali di "dolo" e "colpa". Parimenti, secondo una dottrina oramai indiscussa ed una giurisprudenza quanto mai consolidata, rappresentazione e volontà sussistono non solo quando il reo agisce con la precipua finalità di cagionare l'evento che poi si verifica (dolo intenzionale) oppure con la certezza che, pur volendo raggiungere un diverso scopo, la verificazione dell'evento è passaggio imprescindibile (dolo diretto), ma anche quando la volizione sia, per così dire, attenuata a livello di "accettazione del rischio". Ed, anzi, proprio questa fortunata locuzione è richiamata da buona parte della manualistica, al fine di distinguere tra la forma meno partecipata di dolo – il dolo eventuale – e la manifestazione più intensa di colpa – la colpa cosciente [1].

[1] Nella dottrina italiana, tra la vastissima bibliografia, v. G. DELITALA, *Dolo eventuale e colpa cosciente*, in ID., *Diritto penale. Raccolta degli scritti*, I, Milano, 1976, p. 431 ss.; G.A. DE FRANCESCO, *Dolo eventuale e*

Brevemente: se l'agente si rappresenta, come probabile conseguenza della sua azione o omissione, quell'evento da cui la legge fa dipendere l'esistenza del reato e, ciononostante, egli decide di agire, se ne fa derivare che l'"accettazione del rischio" equivale, in sostanza, alla sua volizione. Al contrario, risponderà a titolo di colpa chi, pur rappresentandosi l'evento, confidi, sbagliando, nel fatto che esso non avrà a realizzarsi [2].

Questa distinzione, che – come detto – gode di ottimo credito presso la dottrina, è stata sposata in più di un'occasione anche dalla giurisprudenza [3].

È noto quali e quante siano le problematiche applicative in tema di colpa cosciente/dolo eventuale (es.: contagio da HIV [4], morte o lesioni cagionate da chi si mette alla guida in stato di ebbrezza [5] o da chi lancia di sassi dal cavalcavia [6]). Anche "il mondo dell'informatica" non si sottrae a questo destino, così come i casi proposti dimostrano.

2.1. La sentenza del Giudice per l'udienza preliminare presso il Tribunale di Palermo del 21 aprile 2009

Il GUP presso il Tribunale di Palermo [7], in sede di giudizio abbreviato, s'è occupato di dare veste giuridica ad una situazione sicuramente nota al comune utente informatico, quotidiano destinatario di c.d. *e-mail spam*, ma, a quanto consta, piuttosto rara ad incontrarsi nei repertori giurisprudenziali [8].

Il caso è presto riassunto. Tizio, in cerca di lavoro, riceve, da un ignaro mittente, un'*e-*

colpa cosciente, in *Riv. it. dir. proc. pen.*, 1988, p. 113 ss.; G. LICCI, *Dolo eventuale*, in *Riv. it. dir. proc. pen.*, 1990, p. 1498 ss.; S. PROSDOCIMI, *Dolus eventualis. Il dolo eventuale nella struttura delle fattispecie penali*, Milano, 1993; S. CANESTRARI, *Dolo eventuale e colpa cosciente. Ai confini tra dolo e colpa nella struttura delle tipologie delittuose*, Milano, 1999; L. EUSEBI, *Appunti sul confine fra dolo e colpa nella teoria del reato*, in *Riv. it. dir. proc. pen.*, 2000, p. 1072 ss.; P. VENENZIANI, *Dolo eventuale e colpa cosciente*, in *Studium iuris*, 2000, p. 70 ss.; S. CANESTRARI, *La definizione legale del dolo: il problema del dolo eventualis*, in *Riv. it. dir. proc. pen.*, 2001, p. 906 ss.; F. CURI, *Tertium datur. Dal common law al civil law per una scomposizione tripartita dell'elemento soggettivo*, Milano, 2003.

[2] V., nella manualistica, F. ANTOLISEI, *Manuale di diritto penale. Parte generale*, XVI ed., Milano, 2003, p. 354 ss.; G. FIANDACA-E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2008, p. 330; F. MANTOVANI, *Diritto penale*, V ed., Padova, 2007, p. 325; T. PADOVANI, *Diritto penale*, VII ed., Milano, 2004, p. 191; M. ROMANO, *Commentario sistematico del codice penale*, III ed., Milano, 2004, p. 410. Da ultimo, v. anche S. CANESTRARI-L. CORNACCHIA-G. DE SIMONE, *Manuale di diritto penale. Parte generale*, Torino, 2007, p. 394 ss.

[3] Basti il riferimento a Cass., sez. fer., 24 luglio 2008 (dep. 31 ottobre 2008), n. 40878, in *Cass. pen.*, 2009, p. 4264 ss. con nota di richiami.

[4] Tra i casi più recenti, v. Cass., sez. V, 17 settembre 2008 (dep. 1 dicembre 2008), n. 44712, in *Cass. pen.*, 2009, p. 4721 ss. ed in *Dir. pen. proc.*, 2009, p. 308 s.

[5] *Incidente mortale provocato da guida spericolata: colpa cosciente o dolo eventuale?* Cass., sez. IV, 24 marzo 2010 (u.p. 18 febbraio 2010), n. 11222, in *Dir. pen. proc.*, 2010, p. 544 s.

[6] V. Cass., sez. I, 25 gennaio 2005, n. 5436, in *Riv. giur. polizia*, 2005, p. 344.

[7] GUP Palermo, 21 aprile 2009, in *De Jure*.

[8] Per i precedenti, v. GUP Milano, 28 luglio 2006, in *Dir. Internet*, 2007, p. 62 ss., con nota di G. VACIAGO-M.T. GIORDANO, *La qualificazione giuridica del phishing in una delle sue prime applicazioni giurisprudenziali*; GUP Milano, 15 ottobre 2007, in *Dir. inf.*, 2009, p. 76 ss.; Trib. Milano, 29 ottobre 2008, in *Corr. merito*, 2009, p. 285 ss. con nota di F. AGNINO, *Computer crime e fattispecie penali internazionali: quando il phishing integra il delitto di truffa*. Convincente nell'escludere che il *phishing* possa essere ricondotto al delitto di cui all'art. 640 c.p., R. FLOR, *Phising, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, p. 899 ss. (che rimane un contributo di riferimento, nonostante scritti successivi dello stesso A. sul medesimo argomento).

mail con la quale gli viene richiesto di mettere a disposizione il proprio conto corrente per alcune transazioni bancarie, da e verso l'estero. Lusingato dalla possibilità di un facile guadagno, questa persona permette ad una società spagnola di accreditare sul proprio conto corrente una certa somma, che egli provvede poi ad inviare ad una cittadina di nazionalità russa, trattenendo per sé l'8%.

Dubitando della legalità del *proprio* comportamento, Tizio si reca presso il più vicino comando dei Carabinieri ed espone l'accaduto. Ironia della sorte, a suo carico viene aperto un procedimento penale per riciclaggio (art. 648 *bis* c.p.).

La difesa, a questo punto, parrebbe fin troppo facile: è evidente che Tizio potrà anche aver tenuto una condotta tipica ai sensi dell'art. 648 *bis* c.p.; certo è che egli era ignaro della provenienza illecita delle somme transitate dalla Spagna al suo conto corrente e da questo nelle mani di un cittadino straniero. Prova ne sia che il procedimento penale a suo carico è scaturito proprio da una richiesta di informazioni alla PG in ordine alla legittimità o meno del comportamento tenuto.

Ma ecco la parte interessante della sentenza: premessa la sicura compatibilità tra l'elemento soggettivo del dolo eventuale ed il delitto di riciclaggio[9], il GUP motiva ritenendo che "*il contenuto e la forma dell'e-mail, le condizioni del contratto ed in particolare la richiesta del numero del conto corrente, non potevano indurre Tizio a ritenere che la proposta contrattuale avesse una dignità giuridica e non celasse un'operazione dai connotati illeciti»*. Reputa, infatti, il giudice "*che un uomo di normale esperienza (tale è Tizio), leggendo frasi [sgrammaticate quali quelle contenute nel messaggio e-mail], non poteva in alcun modo – diversamente da quanto sostenuto dalla difesa – firmare il contratto di lavoro, inviando peraltro tutte le informazioni in ordine al proprio conto corrente*". Ed ancora: "*va sottolineato che, come già rilevato, già nella fase della conclusione del contratto erano emersi elementi (il contenuto delle clausole contrattuali, i numerosi errori di grammatica, il linguaggio del tutto atecnico) che dovevano indurre [Tizio] a ritenere che l'operazione posta in essere dalla [società spagnola] non poteva in alcun modo essere ricondotta negli schemi legali tipici di un contratto di lavoro. Poteva e doveva inoltre essere immediatamente rilevato dalle condizioni contrattuali che non esisteva alcuna prestazione lavorativa richiesta [a Tizio], ma il vero scopo della società proponente era quello di acquisire la disponibilità del conto [a lui] intestato*".

Su questi elementi e su questo ragionamento in termini di puro rimprovero all'agente concreto per non essersi uniformato all'agente modello, si basa la sentenza di condanna per il reato di cui all'art. 648-*bis* c.p., emessa dal tribunale palermitano.

2.2. La sentenza del Tribunale di Milano n. 1972 del 2010 nel caso Google/ViviDown

Anche nella oramai notissima sentenza meneghina[10] compare un analogo *modus rationandi*, che diventa, evidentemente, *modus argomentandi*. In particolare, il giudice di primo grado, ritenendo di dover escludere una responsabilità di Google ai sensi dell'art. 40 cpv. c.p.[11], si sofferma sul profilo della responsabilità penale *ex* art. 167 d.lgs. n. 196 del 2003, il quale racchiude la sanzione penale per l'illecito trattamento dei dati personali.

[9] Di lì a poco, le sezioni unite riterranno altresì la compatibilità tra dolo eventuale e reato di ricettazione (art. 648 c.p.): v. Cass., sez. un., sent. 26 novembre 2009, dep. 30 marzo 2010.

[10] Trib. Milano, 24 febbraio 2010, n. 1972, in *Foro it.*, 2010, II, c. 279.

[11] *Contra*, F. SGUBBI, *Parere pro veritate sulla fondatezza delle imputazioni elevate dalla Procura della Repubblica di Milano nel processo "Vivi Down"*, in *Dir. inf.*, 2009, p. 745 ss.

La fattispecie punisce chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di una serie di disposizioni di legge, richiamate dalla medesima norma incriminatrice, e sempre che dal fatto derivi un nocumento [12].

Il problema che il Tribunale si è trovato ad affrontare può riassumersi come segue. Ammesso [13] (invero, è difficile sostenere il contrario) che tanto l'*upload* quanto il mantenimento sul *server*, a disposizione degli utenti, di un *file* video, avente i noti contenuti, integra un'attività di trattamento di dati personali [14], per di più sensibili [15], ed ammesso pure che il predetto trattamento sia avvenuto in assenza di consenso [16], la condotta di Google, oltre ad essere tipica, può dirsi anche colpevole? Ovvero, accertato che il mantenimento *on line* dall'8-10 settembre 2006 al 7 novembre di un filmato girato e pubblicato senza il consenso dell'interessato rappresenta un fatto tipico ai sensi dell'art. 167 TU, si può ritenere che detto comportamento sia stato oggetto di rappresentazione e volizione? Una rappresentazione e volizione della quale – non va dimenticato – dovrebbero essere portatori i vertici di Google.

Il Tribunale di Milano conclude ritenendo provato anche l'elemento soggettivo (tanto nel profilo di dolo generico quanto in quello di dolo specifico), ma con argomentazioni che mi lasciano perplesso.

Vale la pena riportare alcuni passaggi della motivazione.

"*Quanto ai fatti di questo procedimento, non sarebbe stato ragionevole pensare quantomeno ad un controllo sui video maggiormente visualizzati, o che rivestivano i primi posti nelle diverse sezioni di Google Video …? Ma un elemento macroscopico viene volontariamente sottaciuto da tutti: neppure un'analisi testuale in relazione ai titoli dei video era stata prevista! Questa semplice operazione avrebbe consentito di bloccare automaticamente ed immediatamente in ingresso (ai fini di una successiva verifica manuale più dettagliata, che in questo caso avrebbe confermato l'analisi preliminare) un video che – come quello in esame – era*

[12] Sul problematico inquadramento dogmatico del requisito del "nocumento", v. F.D. BUSNELLI-C.M. BIANCA (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, Padova, 2007. Favorevole all'impostazione giurisprudenziale (v., *ex multis*, Cass., sez. III, 17 novembre 2004 e sez. III, 26 marzo 2004, in *Foro it.*, 2006, II, c. 46, con nota di M. CHIAROLLA, *Trattamento dei dati personali su Internet ed illecito penale*) in termini di condizione obiettiva di punibilità, A. MANNA, *Codice della privacy: nuove garanzie per i cittadini nel testo unico in materia di protezione dei dati personali (commento al d.leg. 30 giugno 2003 n. 196)*, in *Dir. pen. proc.*, 2004, p. 15 ss.

[13] V. p. 90 s. della sentenza (testo dattiloscritto).

[14] Ai sensi dell'art. 4 del d.lgs. n. 196 del 2003, per "trattamento" deve intendersi "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*", mentre è "dato personale" "*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*". Nessun dubbio, quindi, che la pubblicazione *on line* di un filmato che rappresenta una persona riconoscibile integri un "trattamento" quanto meno di quel particolare "dato personale" che è l'immagine.

[15] Sempre l'art. 4 cit. definisce "dati sensibili" "*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché 'i dati personali idonei a rivelare lo stato di salute e la vita sessuale'*" (virgolette aggiunte).

[16] L'art. 167 d.lgs. n. 196 del 2003 sanziona, tra l'altro, la violazione dell'art. 23 del TU, il quale prescrive che "*il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato*". Nel caso concreto, tuttavia, sembra più congruo il richiamo che l'art. 167 cit. fa all'art. 26 del TU, che contiene alcune "rafforzate" "*garanzie per i dati sensibili*".

stato ignobilmente titolato … Eppure certo non si potrà dire che Google, che ha sviluppato il motore di ricerca per eccellenza, non possa vantare tale "know how" in materia …"[17].

Dopo di che, alcune argomentazioni "intermedie"[18] sono dedicate alla affermazione del principio che, anche nel caso di un *host provider* (mero intermediario di traffico), "*esiste … un obbligo non di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi, ai terzi che questi dati consegnano*". Come a dire: indipendentemente dal dovere (di cui si nega l'esistenza) di controllare i contenuti veicolati in rete, qualsiasi ISP ha il dovere (giuridico) di informare gli utenti degli obblighi di legge in materia di trattamento dei dati personali.

Da questo punto di vista, il comportamento tenuto da Google viene ritenuto censurabile in ragione del fatto che le informazioni sugli obblighi derivanti dal rispetto della normativa sul trattamento dei dati personali erano "celate" all'interno delle "condizioni generali di servizio". Tale contegno, "*improntato ad esigenze di minimalismo contrattuale*", denoterebbe – secondo il giudice – una "*scarsa volontà comunicativa … L'informativa sulla privacy, visualizzabile per l'utente dalla pagina iniziale del servizio Google Video in sede di attivazione del relativo "account" al fine di porre in essere il caricamento dei files da parte dell'utente medesimo, era del tutto carente, o comunque talmente "nascosta" nelle condizioni generali di contratto da risultare assolutamente inefficace per i fini previsti dalla legge*".

Ribadito quindi che esiste un obbligo generale di informare l'utente della necessità che, anche nel *web*, il trattamento dei dati personali avvenga con modalità conformi a quelle previste dalla legge e stigmatizzato il comportamento di Google, in particolare, e di chiunque altro, in generale, "anneghi" avvertimenti di siffatto contenuto tra le spesso illeggibili clausole contrattuali, ecco le conclusioni del Tribunale[19]: "*l'esistenza di tutti questi "indici rilevatori" di tipo fattuale e documentale dimostra, a parere di chi scrive, una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela; non solo, ma anche dell'interesse economico ricollegabile a tale accettazione del rischio e della chiara consapevolezza di quest'ultimo*".

Detto diversamente: Google, nel momento in cui ha preferito una politica di *low-profile* in tema di *privacy*, ha "accettato il rischio" di compiere un illecito trattamento di dati personali.

2.3. Considerazioni sulle modalità di accertamento dell'elemento soggettivo

Le difficoltà dell'accertamento dell'elemento soggettivo sono note e da tempo la dottrina ha sviluppato riflessioni metodologiche, oltre che dogmatiche, in materia. Sul fronte applicativo, le corti, di merito o di legittimità, si confrontano con la necessità di dover ricavare la prova del dolo o della colpa da alcuni indici fattuali. È, quindi, il fatto *hic et nunc* considerato, la sua specifica caratterizzazione che permette di "ricostruire" l'atteggiamento interiore del soggetto[20].

Colpa (cosciente) e dolo (eventuale) in molte occasioni vengono qualificati come stati soggettivi contigui, l'uno vicino all'altro, tant'è che per distinguerli si sono proposte numero-

[17] V. p. 80 ss. della sentenza (testo dattiloscritto).

[18] V. p. 92 s. della sentenza (testo dattiloscritto).

[19] V. p. 98 della sentenza (testo dattiloscritto).

[20] Accenna specificamente al problema il manuale di S. CANESTRARI-L. CORNACCHIA-G. DE SIMONE, *op. cit*., p. 397 s.

se e diverse soluzioni. Tra le tante – come accennato – quella che gode di maggior credito è la c.d. teoria dell'accettazione del rischio.

Senza intervenire *funditus* nel dibattito – non sarebbe, d'altronde, questa la sede opportuna –, ritengo vadano segnalati almeno due aspetti.

2.3.1. Primo problema

Per prima cosa, va ribadito che, anche nella forma "eventuale", si ha dolo solo nel caso in cui – come chiaramente scandisce l'art. 43 c.p. – l'evento dannoso o pericolo è "preveduto" e "voluto" dall'agente [21]. Considerato che l'elemento della "previsione dell'evento" può essere caratteristica anche della colpa (art. 61, n. 3, c.p.), se ne ricava che è la componente volitiva che caratterizza il dolo, anche eventuale.

Nelle sentenze che si sono portate all'attenzione del lettore, la motivazione in punto di elemento soggettivo ha le cadenze di un'argomentazione in tema di responsabilità squisitamente colposa più che responsabilità dolosa. La componente volitiva, che deve pur sempre caratterizzare l'accettazione del rischio (tant'è che agire, nonostante la previsione dell'evento ed accettando il rischio della sua verificazione, equivale a volere l'evento stesso), viene desunta dal non essersi resi conto, come sarebbe stato in grado di fare chiunque (*rectius*: l'agente modello), che l'*e-mail* contenente un'offerta di lavoro era fasulla e dal non essersi adoperato, come dovrebbe fare qualsiasi ISP diligente, per rendere evidenti gli obblighi di legge in materia di trattamento dei dati personali.

Il salto logico è evidente: non aver fatto quel che un *homo eiusdem condicionis* (nel primo caso) *et professionis* (nel secondo caso) avrebbe fatto è indice, anzi, *rectius*, "prova" dell'accettazione del rischio e quindi di volizione dell'evento [22].

Nonostante le difficoltà probatorie [23], ritengo che la tendenza debba essere oggetto di censura. Diversamente, le derive in termini di "presunzione" dell'elemento soggettivo dal contesto oggettivo risulteranno sempre meno fronteggiabili. Detta impostazione ha, infatti, già contaminato diversi contesti: il danno da prodotto [24]; la responsabilità di amministratori e sindaci nelle società di capitale [25]; la riferibilità dei reati scopo ai vertici dell'associazione [26]; la responsabilità medica [27].

[21] Così anche S. CANESTRARI, *Dolo eventuale e colpa cosciente*, cit., p. 70 ss.

[22] Anche le impostazioni più spiccatamente tipologiche, pur rintracciando nel dolo eventuale una base oggettiva di rischio doloso (che deve essere di tale natura per cui la possibilità di "correre quel rischio" non verrebbe seriamente presa in considerazione da alcun *homo eiusdem condicionis et professionis*), non rinunciano al profilo psicologico della rappresentazione e della volizione (sebbene nella forma degradata dell'accettazione del rischio). Il pensiero va a S. CANESTRARI, *Dolo eventuale e colpa cosciente*, cit., *passim*.

[23] Si è osservato che il punto centrale della problematica del dolo non è da ricercare sul piano concettuale, bensì su quello processuale: C. PIERGALLINI, *Danno da prodotto e responsabilità penale. Profili dogmatici e politico-criminali*, Milano, 2004, p. 377, nota 37, con richiami bibliografici.

[24] C. PIERGALLINI, *op. cit.*, p. 390 s.

[25] Per una sintesi, v. E. M. AMBROSETTI-E. MEZZETTI-M. RONCO, *Diritto penale dell'impresa*, Bologna, 2008, p. 74 ss. Recentemente, v. F. CENTONZE, *Controlli societari e responsabilità penale*, Milano, 2009.

[26] Basti il richiamo a Corte d'Assise d'Appello di Perugia, 17 novembre 2002, in *Foro it.*, 2003, II, c. 335 (poi riformata da Cass., sez. un., 30 ottobre 2003, in *Foro it.*, 2004, II, c. 161).

[27] V. F. PALAZZO, *Responsabilità medica, "disagio" professionale e riforme penali*, in *Dir. pen. proc.*, 2009, p. 1061 ss.

2.3.2. Secondo problema

Quale evento o, meglio, quale comportamento è stato oggetto di rappresentazione e volizione (ovvero di accettazione)?

Nel tentativo di ricostruire la dogmatica del dolo, una parte della dottrina ha rimarcato la necessità che, ad essere oggetto di rappresentazione, sia il fatto tipico nella sua interezza così come *hic et nunc* verificatosi. Basti, ad esempio, ripensare alle letture ora critiche ora "correttive" dell'art. 82, comma 1, c.p., puntualmente orientate a stigmatizzare la scelta legislativa di equiparare il fatto effettivamente realizzato (ma non voluto) a quello voluto (ma non realizzato)[28].

È specialmente il secondo dei casi proposti che offre le maggiori sollecitazioni sul punto. Ammesso che non aver fornito quelle avvertenze che, invece, si sarebbero dovute fornire (o che un avveduto ISP-modello avrebbe fornito), significhi "accettazione del rischio", qual è il rischio oggetto di accettazione? Ovvero, qual è, in questo caso, l'oggetto del dolo eventuale?

La lettera dell'art. 43 c.p. riferisce la previsione e la volizione all'"evento", ma è stato presto chiarito che, se, *ex* art. 47 c.p., l'errore sul fatto esclude il dolo, oggetto del dolo non potrà che essere lo stesso fatto tipico. E per "fatto" – si è detto prima – deve intendersi quell'insieme di condotta, nesso causale ed evento venuti concretamente ad esistenza.

Così, rapportato all'art. 167 del d.lgs. n. 196 del 2003, questo ragionamento induce a ritenere che oggetto di dolo eventuale può essere, al più, il trattamento, *hic et nunc* attuato (il mantenimento *on line*, dall'8-10 settembre 2006 al 7 novembre, del noto filmato) e caratterizzato dalla violazione di una o più delle norme richiamate dalla fattispecie incriminatrice.

Il ragionamento, proposto dalla sentenza del Tribunale di Milano, sembra, invece, condurre ad altre, diverse conclusioni. Affermare – come s'è fatto – che la mancata adozione di una corretta *policy* aziendale in termini di *privacy* può integrare un'accettazione del rischio di violare le norme richiamate dall'art. 167 del TU significa, in sostanza, individuare l'oggetto di rappresentazione e volizione non nella singola, concreta violazione, bensì in qualsivoglia violazione da chiunque compiuta. Portando alle estreme conseguenze questo ragionamento, se ne ricava che, ad adottare un'informativa minimale in tema di trattamento dei dati personali, si accetta il rischio che un *qualsiasi* utente usi lo spazio *web*, che gli è messo a disposizione, per compiere *qualsiasi* reato in danno di *qualsiasi* persona.

Il che, invero, oltre a configgere con una ricostruzione dell'oggetto del dolo in termini di condotta ed evento "concreti", vanifica gli sforzi "contenitivi" in punto di responsabilità *ex* art. 40, comma 2, c.p. La posizione dell'ISP, infatti, è stata paragonata a quella degli agenti di polizia: tanto l'uno quanto l'altro, anche ad ammettere che abbiano un obbligo di controllo, non possono – per svariati motivi, che qui non v'è spazio per riproporre – essere chiamati a rispondere di qualsiasi reato da chiunque compiuto sol perché, intervenendo tempestivamente, l'avrebbero evitato. Tale condivisibile conclusione pare dovrebbe ritenersi, nella sostanza, rimessa in discussione a sposare una ricostruzione del dolo eventuale come accettazione del rischio del verificarsi di qualsiasi tipo di evento (o reato) in danno di qualsiasi bene giuridico.

[28] Per tutti, G. FIANDACA-E. MUSCO, *op. cit*., p. 383 ss.

3. Caso 2. Elemento soggettivo e tipicità nel concorso di persone

3.1. La vicenda della c.d. baia dei pirati

La recente giurisprudenza in tema di crimini informatici offre un altro interessantissimo spunto di riflessione con riferimento alle tematiche del dolo e, più nello specifico, del suo atteggiarsi nel concorso di persone.

Come noto, su iniziativa della procura locale, il Tribunale di Bergamo si è dovuto occupare, anche in Italia, dell'assai insidioso problema della c.d. baia dei pirati (o *pirate bay*)[29]. Ai gestori, stranieri, del famoso *torrent tracker*, è stata contestata la violazione dell'art. 110 c.p. (con riferimento al quale di veda *infra*) e dell'art. 171-*ter* della legge sul diritto d'autore, n. 633 del 1941 (nel prosieguo, per brevità, anche "LdA"). La norma, nella sua assai articola formulazione, sanziona (anche) chi, agendo a fini di lucro ed in violazione dell'art. 16 LdA, comunica al pubblico, immettendola in un sistema di reti telematiche, un'opera dell'ingegno protetta dal diritto d'autore o anche solo parte di essa (art. 171-*ter*, comma 2, lett. a *bis*, LdA).

Il GIP, nell'accogliere la richiesta di sequestro avanzata dal PM, ha svolto alcune interessanti osservazioni, utili ai fini della riflessione che si vuole proporre in questa sede.

Egli, in particolare, ha sottolineato come "*in conformità ad una tendenza ormai consolidata, il materiale coperto da diritto di autore non viene diffuso attraverso la pubblicazione su un 'server' (come avviene per gli ordinari siti 'internet') e quindi su un sistema informatico fisso, stabile ... Nel caso in esame, al contrario, il materiale destinato alla diffusione non è concentrato su un 'server' fisso, ma rimane sugli apparati informatici dei singoli utenti, che scambiano direttamente dati, interagendo 'da pari a pari' (donde la definizione di circuito "peer-to-peer")*". Ne segue che, in questo sistema "di pari", i *server* non servono (più) per archiviare il materiale oggetto di scambio, bensì hanno la "*funzione di gestire le connessioni tra gli utenti e l'indicizzazione dei 'file'. È indispensabile, infatti, che l'utente interessato al prelievo o allo scambio di particolari dati sia in grado di sapere se, dove ed in quale misura possa reperirli nel momento in cui si connette alla rete mondiale (accertamento precluso agli ordinari strumenti di ricerca, che non sono in grado di documentare e localizzare il contenuto dei singoli computer)*".

Esattamente questo era lo scopo del sito/*torrent tracker* denominato *www.thepiratebay.org*. Nelle parole del GIP: "*tale è ... la funzione del sito "internet" www.thepiratebayy.org, che non conserva – sui 'server' che lo ospitano – i "file" che interessano ai suoi utenti e non li mette a disposizione di questi ultimi in modo diretto ed immediato, ma svolge una funzione di 'smistamento' (tecnicamente 'tracking' o tracciamento). Il sito, in pratica, definisce e fornisce un complesso codice alfanumerico di collegamento ('torrent') univoco per ciascun singolo 'file' ... Grazie a questa univoca codificazione, gli utenti che accedono alle pagine di 'The Pirate Bay' sono posti in condizione di interagire, instaurando collegamenti e scambi sulla base di quel comune dato identificativo, che consente la convergenza di domanda e offerta*".

[29] Con decreto dell'1 agosto 2008, il giudice per le indagini preliminari presso il Tribunale di Bergamo, visti gli artt. 321 e ss. c.p.p., ha disposto il sequestro preventivo del sito *ww.thepiratebay.org*, disponendo altresì che i fornitori di servizi *internet* e, segnatamente, i provider operanti sul territorio dello Stato italiano inibiscano agli rispettivi utenti – anche e mente degli artt. 14 e 15 dal d.lgs. n. 70 del 2003 – l'accesso: all'indirizzo *www. thepiratebay.org*; ai relativi *alias* e nomi di dominio presenti e futuri, rinvianti al sito medesimo; all'indirizzo IP statico 83.140.176.146, che al momento risulta associato ai predetti nomi di dominio ed ad ogni ulteriore indirizzo IP statico associato ai nomi stessi nell'attualità e in futuro.

Già nel primo provvedimento cautelare, tuttavia, emerge quell'errore di fondo in cui, a mio parere, incorrerà anche la Suprema Corte[30]. Infatti, l'inquadramento giuridico appare non in linea con la puntuale descrizione del funzionamento del sito/*torrent tracker* e del funzionamento dei sistemi di scambio di *file* c.d. *peer to peer*. Secondo il GIP bergamasco, "*la gestione del sito stesso può ... ricondursi, al paradigma delittuoso ex art. 171 ter con specifico riferimento alle previsioni del comma 2, lettera a bis), di tale previsione incriminatrice. Ed invero può ritenersi che gli odierni indagati, in concorso tra loro e con terzi attualmente ignoti, in violazione dell'articolo 16 della l. 633/1941 ed a fini di lucro, abbiano comunicato e tuttora comunichino al pubblico opere dell'ingegno protette dal diritto d'autore, immettendo le opere stesse sulla rete "internet" attraverso il sito identificato ... www.thepiratebay.org*".

La Corte di Cassazione, chiamata a pronunciarsi sulla legittimità del provvedimento del Tribunale del riesame[31] in tema di sequestro preventivo del sito *internet www.thepirate bay.org* nonché di altri *alias* o *mirrow*, si è espressa nei termini che seguono.

"*Innanzi tutto va affermato che correttamente l'impugnata ordinanza del tribunale di Bergamo ha ritenuto sussistere, quale presupposto del sequestro preventivo, il 'fumus commissi delicti' consistente nel trasferimento, a mezzo della rete 'internet', di 'file' aventi il contenuto di opere coperte da diritto d'autore in violazione del diritto esclusivo di comunicazione al pubblico di tali opere. La particolare tecnologia informatica di condivisione di "file" tra utenti della rete "internet" (c.d. 'file sharing') e l'utilizzo di protocolli di trasferimento dei "file" direttamente tra utenti (c.d. 'peer to peer') per la diffusione in rete di opere coperte da diritto d'autore ... non escludono la configurabilità del reato ...*".

Gli ermellini proseguono sottolineando – come ha fatto il giudice di merito – che la caratteristica della condivisione di *file* (c.d. *file sharing*) e dei protocolli di trasferimento dei *file*, del tipo *peer to peer*, è quella di aver decentrato presso gli utenti (c.d. *client*) – i quali effettuano solitamente le operazioni di *downloading* – anche l'attività di "invio" dei *file* (c.d. *uploading*) contenenti l'opera protetta dalla normativa sul diritto d'autore. Pertanto – si insiste in motivazione – la "diffusione" dell'opera coperta da diritto d'autore non avviene dal centro (il sito *web*) verso la periferia (che riceve il *downloading*), ma da un utente che effettua l'*uploading* agli altri utenti che lo ricevono; quindi da "pari a pari" (*peer to peer*), non essendoci un centro (il sito *web*; il *server*) che possiede l'opera e che la trasferisca "in periferia", agli utenti che accedono al sito. L'opera è, invece, "in periferia", presso gli utenti stessi, e da questi è trasferita – e quindi diffusa – ad altri utenti.

Anche la Corte di Cassazione, quindi, si preoccupa, prima di tutto, di descrivere in modo preciso e compiuto il funzionamento delle reti *peer to peer*.

Subito dopo è affrontato, in due *steps*, il problema giuridico.

Prima di tutto, considerato che a carico dei gestori del sito incriminato pende un'imputazione per concorso nell'altrui reato, la Corte si premura di precisare che "*il reato di diffusione dell'opera, senza averne diritto, mediante la rete 'internet' è commesso innanzi tutto da chi fa l''uploading', reato previsto, rispettivamente, dalla LdA, art. 171, comma 1, lett. a bis), se c'è la messa a disposizione dell'opera in rete "a qualsiasi scopo e in qualsiasi forma", ma non a scopo di lucro, ovvero dall'art. 171 ter, comma 2, lett. a bis), se c'è la comunicazione dell'opera in rete a fine di lucro*". Ed è esattamente questa seconda la fattispecie per la quale si procede, "*essendosi ravvisato – da parte dei giudici di merito – il fine di lucro negli introiti delle inserzioni pubblicitarie a pagamento*".

[30] Cass., sez. III, 29 settembre 2009, n. 49437, in *Foro it.*, 2010, II, c. 136. La Suprema Corte ha annullato la sentenza del Trib. di Bergamo, 3 ottobre 2008, in *Rep. Foro it.*, 2008, voce *Diritti d'autore*, n. 204.

[31] Il Tribunale del riesame di Bergamo, con ordinanza del 24 settembre 2008, a mente dell'art. 324 c.p.p., ha annullato il sequestro preventivo disposto dal giudice per le indagini preliminari.

Quanto al gestore del sito, poi, vanno distinte due situazioni. La prima è quella del sito *web* che si limita a mettere a disposizione il protocollo di comunicazione (quale quello *peer to peer*) per consentire la condivisione dei *file* contenenti l'opera coperta da diritto d'autore ed il loro trasferimento tra utenti. In questo caso – ritiene la Corte – il titolare del sito sarebbe estraneo al reato. La seconda situazione è quella del caso di specie, ove il gestore del sito "*fa qualcosa di più*", ovvero si occupa anche di indicizzare le informazioni che gli provengono dagli utenti, che sono tutti potenziali autori di *uploading*. In questo modo, le informazioni contenute nel sito (ovvero, le chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), permettono agli utenti di "orientarsi", chiedendo il *download* di una certa opera piuttosto che di un'altra. Ed è proprio in ragione di questo elaborare e rendere disponibili nel sito, a mezzo di un motore di ricerca o con delle liste indicizzate, le chiavi di accesso alle opere protette che il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. "*Ed allora è vero che lo scambio dei file avviene da utente ad utente ("peer to peer"), ma l'attività del sito "web" (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò, e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone ex art. 110 c.p. ... In altre parole la tecnologia 'peer to peer' decentra sì l''uploading' (la diffusione in rete dell'opera), ma non ha anche l'effetto, per così dire, di decentrare l'illegalità della diffusione dell'opera coperta da diritto d'autore senza averne diritto. Rimane comunque un apporto del centro (ossia del titolare del sito "web") a ciò che fa la periferia (gli utenti del servizio informatico che, utilizzando quanto reso disponibile nel sito 'web', scaricano l'opera protetta dal diritto d'autore), apporto che, nel nostro ordinamento giuridico, consente l'imputazione a titolo di concorso nel reato previsto dal cit. art. 171 ter, comma 2, lett. a bis*".

3.2. Considerazioni sul ruolo dell'elemento soggettivo nel concorso di persone

Il fatto oggetto di contestazione appare quanto mai chiaro: i gestori del sito *www.thepiratebay.org* hanno messo a disposizione degli utenti un c.d. *torrent tracker* (in termini più semplici: un motore di ricerca per i *file torrent*) che consente agli utenti di individuare in quale macchina, connessa in rete, si trova il *file* il cui *download* si desidera. Come precisato dal GIP di Bergamo e come rimarcato anche dalla Corte di Cassazione, la duttilità del sistema di *download* attraverso i *file torrent* consiste nel fatto che, fisicamente, i dati informatici sono e rimangono memorizzati sui PC dei singoli utenti e non vengono, invece (come accadeva con i sistemi precedenti di condivisione, quali, ad esempio, *Napster*), ad essere situati sul *server* (che, nel caso di specie, ospita il sito *www.thepiratebay.org*), il quale funge da mero tramite di uno scambio "tra pari". A ciò va aggiunto anche il fatto che l'utente effettua il *download* non del *file* intero, bensì di segmenti (meno "pesanti") dello stesso.

Se questa è la situazione, ne segue che, la condotta di "immissione in un sistema di reti telematiche di un'opera dell'ingegno protetta dal diritto d'autore", sanzionata (con la reclusione da uno a quattro anni e con la multa da € 2.582,00 ad € 15.493,00) dall'art. 171-*ter*, comma 2, lett. a *bis* LdA, è posta in essere dal singolo utente, che mette in condivisione i *file* del proprio PC. Al contrario, sarebbe errato ritenere che analoga condotta ponga in essere il gestore del *torrent tracker*, il quale null'altro fa se non fornire, alla macchina che si connette ad un certo sito, le istruzioni informatiche per ritrovare, nelle altre macchine collegate, il *file* di interesse. Quest'ultimo, infatti, non compie alcuna operazione di "comunicazione al pubblico" di opere protette dal diritto d'autore, né si rende colpevole della "immissione" di predette opere nei sistemi di reti telematiche.

Se questo è vero, se ne deve concludere che il comportamento dei gestori del sito *www.thepiratebay.org* non può considerarsi tipico ai sensi dell'art. 171-*ter* LdA. Tuttavia – come evidenziato sin dalla formulazione del capo di imputazione –, ritengono i giudici che si sono pronunciati sul caso, che chi gestisce un *server* che ha la precipua funzione di "facilitare" gli utenti nel *download* di opere protette dal diritto d'autore, potrà essere agevolmente chiamato a rispondere ai sensi dell'art. 110 c.p. In questo contesto, la sua condotta, pur non riconducibile, di per sé, alla fattispecie incriminatrice contenuta nella LdA, diventa tipica in quanto avente un contenuto che, materialmente ed univocamente, è agevolatore rispetto alla commissione di quello specifico reato [32].

Tale conclusione viene ad essere non completamente condivisibile sol ponendo attenzione all'elemento soggettivo di fattispecie. L'art. 171-*ter* LdA, tanto al comma 1 quanto al comma 2, lett. a *bis*, sanziona esclusivamente chi agisce "a fini di lucro" [33]. L'elemento del dolo specifico, specialmente nel settore della tutela penale del diritto d'autore, non può essere sottovalutato: se non altro perché uno dei tratti distintivi tra l'art. 171-*bis* e l'art. 171 *ter* LdA è rappresentato proprio dall'alternativa "fine di profitto"/"fine di lucro" e perché, in molteplici occasioni, il legislatore è intervenuto su questo aspetto [34].

Tanto nelle pronunce di merito quanto in quella di legittimità, la ricostruzione del dolo specifico in capo ai gestori del sito incriminato è affrontata in modo piuttosto agevole: la vendita di spazi pubblicitari sul sito *www.thepiratebay.org* è prova del fatto che gli indagati hanno agito a fine di lucro. Conclusione, questa, che si può anche condividere.

Tuttavia, a questo punto, c'è qualcosa che sfugge. I gestori del *torrent tracker* sono chiamati a rispondere per aver favorito la comunicazione al pubblico, mediante immissione in rete, di opere protette dal diritto d'autore, così concorrendo con i singoli utenti, che a quel sito si sono collegati, alla realizzazione del reato di cui all'art. 171-*ter* LdA. Il comportamento dei gestori del sito, di per sé atipico, acquista tipicità in virtù dell'art. 110 c.p.; mentre ad essere tipico sarebbe il comportamento degli utenti alla ricerca di *file* da "scaricare". Ma ecco l'"inghippo": i primi agiscono con il dolo specifico del "fine di lucro", mentre i secondi è verosimile agiscano o con dolo generico o, al più, con il dolo specifico del "fine di profitto", intendendosi, per tale, anche il risparmio di spesa.

Di qui il salto logico: nella vicenda bergamasca l'imputazione è, per così dire, "composita": da un lato, il fatto tipico è posto in essere dai singoli utenti, mentre la condotta agevolatrice dei gestori del sito da atipica *diventa* tipica grazie all'art. 110 c.p.; dall'altro, il dolo specifico di profitto è proprio di chi concorre (con comportamento atipico) nell'altrui reato, ma non anche di chi quel reato materialmente commette. Come a dire: gli utenti pongono in essere la condotta ed il gestore del sito "mette" il dolo specifico che manca per aversi il reato perfetto.

[32] Sulla funzione dell'art. 110 c.p. quale "clausola generale", che rende punibili fatti che non lo sarebbero ai sensi della fattispecie di parte speciale, v. L. RISICATO, *Combinazione ed interferenza di forme di manifestazione del reato. Contributo ad una teoria delle clausole generali di incriminazione suppletiva*, Milano, 2001, p. 61 ss.

[33] Sul punto, anche per i richiami giurisprudenziali, v. M. MORRA, *I reati in materia di diritto d'autore. Le fattispecie incriminatrici e le altre disposizioni penali*, Milano, 2008, p. 81 ss. In argomento, D. TERRACINA, *La tutela penale del diritto d'autore e dei diritti connessi*, Torino, 2006.

[34] Con riferimento al comma 1 dell'art. 171-*ter* LdA, le parole "*a fini di lucro*" sono state dapprima sostituite dalle parole "*per trarne profitto*" dall'art. 1, comma 2, d.l. n. 72 del 2004, conv., con modificazioni, nella legge n. 128 del 2004. L'art. 3, comma 3-*quinquies* del d.l. n. 7 del 2005, conv., con modificazioni, nella legge n. 43 del 2005, ha poi sostituito le parole "*per trarne profitto*" con le attuali "*a fine di lucro*". Anche la lett. a *bis* del comma 2 dell'art. 171-*ter* LdA è stata oggetto di novella nel 2005: le originarie parole "*per trarne profitto*" sono state sostituite dalle attuali "*a fini di lucro*" dall'art. 3, comma 3-*quinquies* del d. l. n. 7 del 2005 cit.

Contrariamente a quanto affermato, la condotta dei gestori del sito *www.thepiratebay.org* non integra – a mio avviso – un concorso nel reato di cui all'art. 171-*ter*, comma 2, lett. a *bis* LdA, bensì, al più, un concorso nel diverso reato previsto dell'art. 171, comma 1, lett. a *bis* LdA. L'accertamento della finalità di lucro, che anima il gestore del *torrent tracker* è superflua in un caso come quello descritto, perché egli non pone in essere un fatto tipico ai sensi dell'art 171-*ter*, né concorre con altri che tengano quel contengo ("comunicare al pubblico opere protette *con finalità di lucro*"). Tutto quello che si può contestare al gestore del sito è, semmai, il concorso nel meno grave reato di cui all'art. 171 LdA (per il quale vale anche la causa di estinzione di cui al comma 2).

Il caso in esame è particolarmente interessante anche ai fini di una rilettura delle problematiche in tema di concorso di persone: la conclusione cui si è giunti presuppone, infatti, una visione dei contributi concorsuali in termini di accessorietà (il comportamento dell'*ISP* è penalmente rilevante perché, seppur atipico, è accessorio rispetto alla condotta, *in se* avente rilievo penale, posta in essere dall'utente). L'impostazione suggerita dalla Cassazione sembra invece più vicina alla teorica della fattispecie plurisoggettiva (eventuale o differenziata), con ciò esponendosi alle critiche sopra formulate, oltre che a quelle generalmente mosse alla predette impostazioni [35].

4. Caso 3. Scelte legislative (improprie) e ruolo del dolo specifico

4.1. La frode del certificatore (art. 640-*quinquies* c.p.)

La legge n. 48 del 2008, che ha ratificato e dato attuazione alla Convenzione Cybercrime, ha introdotto, all'interno del codice penale, alcune nuove figure di reato. Tra queste rappresenta un fattore di novità la "frode informatica del soggetto che presta servizi di certificazione di firma elettronica", ora prevista all'art. 640-*quinquies* c.p.: "*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*" [36].

[35] In sintesi, v. G. FIANDACA-E. MUSCO, *op. cit*., p. 491 ss.

[36] L'inserimento dell'art. 640-*quinquies* si deve all'art. 5, legge 18 marzo 2008, n. 48. Per un primo commento ai profili di diritto penale sostanziale della legge n. 48 del 2008, si vedano: G. AMATO, *Contrasto specifico all'abuso di dispositivi*, in *Guida dir.*, 2008, 16, p. 58, ID., *Danneggiamento perseguibile a querela*, in *Guida dir.*, 2008, 16, p. 60; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 700; ID., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet*, 2008, p. 437; F. RESTA, *Un intervento incisivo nella sostanza*, in *Guida al dir.*, 2008, 16, p.54; P. SCOGNAMIGLIO, *Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48*, Napoli, 2008. Un elenco dei Paesi che hanno ratificato la Convenzione Cybercrime può essere reperito su *www.coe.int/cybercrime*. Sul ruolo del Consiglio d'Europa e sull'importanza della convenzione di Budapest, v. *ex multis*: P. DAMINI-S. DELSIGNORE, *XVI Congresso dell'associazione internazionale di diritto penale (Budapest, 5-11 settembre 1999)*, in *Indice pen.*, 2000, p. 337 ss.; G. ILARDA-G. MARULLO (a cura di), *Cybercrime: conferenza internazionale. La convenzione del consiglio d'Europa sulla criminalità informatica*, Milano, 2004; L. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, p. 189 ss.; C. SARZANA DI SANT'IPPOLITO, *Sicurezza informatica e lotta alla cybercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislative*, in *Dir. Internet*, 2005, 5, p. 437 ss.

La novella legislativa costituisce l'occasione per svolgere alcune riflessioni sugli attuali orientamenti della politica criminale [37].

La *rubrica legis* e la collocazione sistematica della nuova fattispecie impongono di verificare quanto sia "truffaldino" il comportamento del certificatore qualificato descritto all'art. 640-*quinquies* c.p. e se questo suo contegno mantenga un qualche denominatore comune con il "tradizionale" reato di truffa (art. 640 c.p.).

Secondo un'opinione piuttosto condivisa si ha truffa quando: *i*) sono posti in essere artifici o raggiri; *ii*) essi portano ad un'induzione in errore della vittima; *iii*) la vittima compie un atto di disposizione patrimoniale; *iv*) dall'atto di disposizione patrimoniale deriva il duplice evento di ingiusto profitto con altrui danno [38].

Una condotta sì articolata e complessa non era, evidentemente, in grado di reggere il confronto con i tempi e, soprattutto, con l'avvento della tecnologica informatica. Infatti, già nel 1993 (con la legge n. 547) è stato introdotto nel codice penale l'art. 640 *ter* c.p. [39].

Nella truffa "tradizionale" il reo ha quale referente una persona fisica ed è proprio questo che gli permette di farle credere che esiste ciò che non esiste o che non esiste ciò che esiste. Scopo del truffatore è colorare di verosimiglianza quella che in realtà è una rappresentazione distorta della realtà: una *mise en scene*. Quando il "reo" diventa "operatore" e la "vittima" diventa un "sistema informatico", la conservazione dell'esposto schematismo non è più possibile né auspicabile: solo un uomo (e non anche una macchina) può credere reale ciò che tale non è ed essere così tratto in errore.

---

[37] In argomento, sia permesso il rimando a M. GROTTO, *Reati informatici e Convenzione Cybercrime. Oltre la "Truffa" e la "Frode informatica": la "Frode del certificatore"*, in *Dir. inf.*, 2009, p. 139 ss.

[38] In realtà la formulazione della norma è più sintetica ("*Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro*"). Questa sorta di quadripartizione, però, è pressoché unanimemente condivisa da dottrina e giurisprudenza. Tra la vasta letteratura si vedano A. CRESPI, *Il comportamento fraudolento e l'incusso timore di un pericolo immaginario*, in *Riv. it. dir. proc. pen.*, 1963, p. 154 ss; G. FIANDACA, *Frode valutaria e truffa in danno dello Stato*, in *Foro it.*, 1981, II, c. 431; G. LA CUTE, voce *Truffa (dir. vig.)*, in *Enc. dir.*, Milano, 1992, p. 243; M. MANTOVANI, *Dolo, truffa, annullabilità del contratto (Nota a Cass., 10 dicembre 1986, n. 7322, Tanesini c. Mazzei)*, in *Nuova giur. civ.*, 1987, I, p. 271; G. MARINI, voce *Truffa*, in *Dig. pen.*, XIV, Torino, 1999, p. 353; G. PECORELLA, voce *Patrimonio (delitti contro)*, in *Noviss. Dig., Agg.*, XII, Torino, 1965, p. 643; C. PEDRAZZI, *La promessa del soggetto passivo come evento nei delitti contro il patrimonio*, in *Riv. it. dir. proc. pen.*, 1952, p. 384; ID., *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, *passim*; U. PIOLETTI, voce *Truffa*, in *Novis. Dig.*, *App.*, VII, Torino, 1987, p. 907; G. SAMMARCO, voce *Truffa*, in *Enci. giur. Treccani*, XXXI, Roma, 1994; M. ZANOTTI, *La truffa*, Milano, 1993, *passim*; tra i commentari, basti il richiamo a M.T. VASCIAVEO, *Art. 640*, in G. MARINUCCI-E. DOLCINI (a cura di), *Codice penale commentato*, Milano, 2006, p. 4602 ss.

[39] Il reato di "frode informatica" è stato introdotto all'art. 640 *ter* c.p. dalla legge 23 dicembre 1993, n. 547. L'intervento novellistico ha tratto origine della Raccomandazione del Consiglio d'Europa n. R (89) 9 del 1989 (pubblicata in *Riv. trim. dir. pen. ec.*, 1992, p. 377 ss. in appendice al contributo di V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*; specificamente, in argomento: CONSEIL DE L'EUROPE, *La criminalité informatique. Raccomandation n. R (89) 9 sur la criminalité en relation avec l'ordinateur et rapport final du Comité européen pour les problèmes criminels*, Strasbourg, 1990). L'interesse per le attività riconducibili alla frode informatica non manca nemmeno nella Convenzione Cybercrime, il cui art. 8, rubricato "*Computer-related fraud*" recita: "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without righzt, the causing of a loss of property to another person by: || a) any input, alteration, deletion or suppression of computer data; || b) any interference with the functioning of a computer system, || with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person*". Anche negli atti parlamentari che descrivono l'*iter* di recepimento della Convenzione sono specificamente richiamate le iniziative di stampo europeo: si veda la relazione al d.d.l. n. 2807 presentata alla Camera il 19 giugno 2007.

Prendendo atto di questo inconfutabile dato fattuale, il legislatore del 1993, nel formulare la fattispecie dell'art. 640-*ter* c.p., ha ben ritenuto di abbandonare il riferimento ad "artifici o raggiri" e di concentrare l'attenzione sulle condotte di "alterazione di un sistema informatico o telematico" ovvero di "intervento senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti".

Se nel 1993 si è ritenuto di mantenere una certa continuità tra la struttura della truffa e quella della frode informatica, ciò non è accaduto nel 2008. La fattispecie di cui all'art. 640-*quinquies* c.p. sanziona un comportamento che, apparentemente, nulla ha a che vedere con l'evento di illecito profitto e altrui danno, che gli artt. 640 e 640-*ter* c.p. vogliono realizzato per il tramite di condotte subdole, ora ricadenti sulla vittima ora sulla macchina.

La condotta tipica, originariamente concepita, in sede di presentazione del disegno di legge, come "violazione degli obblighi indicati all'art. 32 del c.d. Codice dell'Amministrazione digitale", è diventata "violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato"; il duplice evento di danno e profitto è scomparso; il dolo da generico è diventato specifico; il reato da comune è diventato proprio.

L'interrogativo se, con l'eliminazione del riferimento all'art. 32 d.lgs. n. 82 del 2005, si sia o meno ampliato il novero di comportamenti aventi rilevanza penale, è presto risolto. Nonostante il Codice dell'Amministrazione Digitale riservi numerose norme alla figura del certificatore qualificato (dall'art. 26 all'art. 37), è solo l'art. 32 che, allo stato, elenca gli *obblighi di legge* che egli deve rispettare nel momento in cui provvede al *rilascio* del certificato qualificato.

Il passaggio dalla formulazione iniziale del d.d.l. a quella definitiva della legge n. 48 del 2008 non sembra quindi produrre modifiche di particolare rilievo. Anzi, il venir meno del riferimento espresso all'art. 32 del d.lgs. n. 82 del 2005 rappresenta un esempio di positivo superamento della tecnica meramente sanzionatoria che, seppur criticata dalla dottrina con ricchezza di argomentazioni, riesce spesso a sedurre il legislatore. Peccato, però, che si sia rinunciato ad una descrizione più puntuale e precisa delle condotte penalmente rilevanti, così condannando l'art. 640-*quinquies* c.p. ad una certa indeterminatezza.

Il duplice evento di danno e di profitto circoscrive non poco la rilevanza penale delle condotte di cui agli artt. 640 e 640 *ter* c.p. Ciò non accade con riguardo all'art. 640 *quinquies* c.p., che, semplicemente, sanziona "*il soggetto che presta servizi di certificazione di firma elettronica, il quale ... viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato*". Così, mentre l'art. 640 c.p. e l'art. 640-*ter* c.p. hanno una formulazione speculare per quanto riguarda l'evento e l'elemento soggettivo, l'art. 640-*quinquies* c.p. (nel testo che è entrato in vigore) innova completamente: scompare l'evento di danno ed al dolo generico viene sostituito il dolo specifico.

Ed eccoci quindi al *punctum dolens*: quale ruolo è stato riservato dal legislatore della riforma all'elemento soggettivo? Qual è la conseguenza del fatto che nell'art. 640-*quinquies* c.p. il dolo specifico sia "caricato" di un danno che, negli artt. 640 e 640-*ter* c.p., fa parte del fatto tipico?

Nel caso *de quo* il fatto tipico non adempie completamente alla funzione che gli sarebbe propria, di puntualizzazione del *discrimen* tra ciò che è lecito è ciò che è penalmente vietato (e sanzionato): s'è già evidenziato come la condotta tipica risulti, almeno in parte, indeterminata e s'è già messa il luce la necessità di circoscrivere il richiamo all'art. 32 del d.lgs. n. 82 del 2005 a quei precetti che, se violati, portano al rilascio di un certificato sprovvisto di quell'affidabilità che dovrebbe caratterizzarlo. Ne consegue che il fine di profitto "o" danno viene ad assumere una portata selettiva più che significativa.

L'elemento soggettivo, quindi, *i*) è criterio per distinguere, tra le violazioni del d.lgs. n. 82 del 2005, quelle che hanno *anche* rilievo penale da quelle che, invece, hanno solo portata

civilistico-amministrativa e *ii*) è l'unico elemento che colora di patrimonialità la fattispecie[40].

Ricostruire ed interpretare il delitto di frode del certificatore leggendo la condotta base *separatamente* dalla finalità specifica indicata dalla norma, porterebbe ad una sovrapposizione tra responsabilità penale e responsabilità civile: la violazione degli obblighi del certificatore, indicati dall'art. 32 del Codice dell'Amministrazione Digitale, assume, infatti, uguale rilevanza *oggettiva* tanto nell'un settore quanto nell'altro. È la stessa struttura del delitto che impone di non prescindere, nella descrizione *del fatto*, dal dolo specifico.

Nell'art. 640-*quinquies* c.p. il legislatore richiede che un certo fine *soggettivo* sorregga una condotta *oggettiva*, la quale viene così ad essere considerata *strumentale* rispetto a quello. Quel che rileva, e che si sanziona, è l'uso di un certo strumento per ottenere un determinato fine: l'azione nel suo complesso va ricostruita avendo ben presente lo scopo per il quale il soggetto si vale di un certo mezzo.

4.2. La diffusione di programmi virus (art. 615-*quinquies* c.p.)

Un caso simile a quello che s'è pocanzi descritto riguarda l'art. 615-*quinquies* c.p. Prima della riforma attuata nel 2008, con la legge di ratifica della Convenzione di Budapest del 2001, la norma sanzionava chi "*diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento*".

Successivamente, non è chiaro se con uno scopo preciso di anticipazione della tutela, il legislatore ha ritenuto che l'articolo abbisognasse di un qualche "ritocco". Il risultato non è dei migliori.

Il fatto tipico che ne è risultato consiste nel "procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri" oggetti di uso quanto mai comune nella vita quotidiana, ovvero "*apparecchiature, dispositivi o programmi informatici*"[41].

La mancanza di un qualsiasi disvalore d'azione è dato quanto mai evidente. Il che è in contrasto con un diritto penale "del fatto" (art. 25, comma 2, Cost.) prima ancora che con un'impostazione costituzionalmente orientata della materia sanzionatoria. La sanzione penale (reclusione fino a due anni e multa fino ad € 10.329,00) consegue, infatti, ad una condotta (intesa quale fatto tipico) *ictu oculi* in tutto e per tutto lecita, qual è la "produzione, riproduzione, importazione, diffusione, comunicazione, consegna" di un qualsiasi *software*.

Com'è accaduto per l'art. 640-*quinquies* c.p., anche in questo caso l'intero disvalore del fatto tipico è "caricato" sull'elemento soggettivo, ovvero sul dolo specifico di "danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti" ovvero di "favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento" dei predetti sistemi informatici o telematici. La sanzione penale "si regge", quindi, sull'elemento soggettivo del dolo specifico, il quale, peraltro, risulta particolarmente articolato nella sua formulazione.

Prima di tutto, vengono in rilievo due diverse finalità:

[40] *Amplius*, v. M. GROTTO, *Reati informatici e Convenzione Cybercrime*, cit., p. 151 ss.

[41] Per un primo commento, v. G. CORASANITI-G.C. LUCENTE, *Cybercrime, responsabilità degli enti, prova digitale*, Padova, 2009, p. 120 ss.

1. lo scopo di "danneggiamento illecito".

Il requisito di illiceità speciale è, forse, superfluo, considerando che la sistematica dei reati informatici non contempla un danneggiamento che possa dirsi "lecito". Tanto negli artt. 635-*bis*, *ter*, *quater* e *quinquies* c.p., quanto negli artt. 392 e 615-*ter*, comma 2, n. 3, c.p. – dove, in termini diversi, si richiamano ora condotte espressive di una *vis* bruta, quali quelle di "distruzione, deterioramento, cancellazione, alterazione, soppressione" (art. 635-*bis* c.p.), ora condotte meno "invasive", quali quelle di "alterazione, modificazione, cancellazione" o di "impedito o turbato funzionamento" (art. 392 c.p.) – non si è sentita la necessità di precisare che il "danneggiamento" deve essere anche "illecito". Forse perché si è, giustamente, dato per scontato che la distruzione della *res* propria (con tale aggettivo intendendosi richiamare non solo il diritto di proprietà, ma anche la situazione di titolarità giuridica che importi un potere dispositivo sulla cosa), fin tanto che non reca danno o, quanto meno, pericolo alla collettività (v. art. 423, comma 2, c.p.), sia una legittima espressione del diritto di proprietà, sancito in Costituzione (art. 42, comma 2, Cost.) ed articolatamente disciplinato nel codice civile (artt. 832 e ss. c.c.). Né, d'altra parte, sarebbe congruo prevedere una sanzione penale per chi distrugge un *res* sì altrui, ma col diritto di farlo.

Nel caso dell'art. 615-*quinquies*, invece, non basta che chi produce, riproduce, diffonde, comunica, consegna o mette a disposizione programmi lo faccia con fine di danneggiamento, ma è necessario che egli agisca per un fine di danneggiamento "illecito". Come a dire che chi diffonde, ad esempio, un *virus* deve voler agire per danneggiare gli altrui sistemi informatici, ma deve anche rappresentarsi che quella sua finalità è illegittima;

2. lo scopo di "favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento di un sistema informatico o telematico".

Francamente non comprendo perché si è scelto di punire chi agisce con lo scopo di "favorire l'interruzione" e, non semplicemente, chi agisce con lo scopo di "interrompere" il funzionamento del sistema informatico. L'impiego del verbo "favorire" fa pensare ad una situazione di "concorso di cause" (o "di persone"): si favorisce un processo già in atto o che, sebbene non *in fieri*, lo diverrà in ragione di altre cause. Con il che sembra quasi che il dolo specifico racchiuda in sé un dolo generico, visto che la "finalità di favorire" lascia presupporre che l'agente debba quanto meno rappresentarsi il processo di danneggiamento "favorito".

Ma non è tutto, perché così come accade per la condotta, anche il dolo specifico ha un suo "oggetto materiale":

1. un sistema informatico;
2. un sistema telematico;
3. informazioni, contenute o pertinenti un sistema informatico (o telematico);
4. dati, contenuti o pertinenti un sistema informatico (o telematico);
5. programmi, contenuti o pertinenti un sistema informatico (o telematico).

Così "sezionato", il dolo specifico di fattispecie risulta in tutta la sua complessità. E la situazione è ancor più delicata sol che si ponga mente al fatto che tutti questi elementi da un lato dovrebbero stare, almeno secondo l'impostazione teorica tradizionale, solo "nella testa di chi agisce", mentre, dall'altro, sono il solo *discrimen* tra il giuridicamente lecito ed il penalmente sanzionato.

4.3. Il tentativo di una lettura "correttiva": il ruolo tipizzante del dolo specifico

Il fatto che nell'ordinamento siano contemplate fattispecie quali l'art. 640-*quinquies* e l'art. 615-*quinquies* c.p. rende quanto mai opportuno il recupero di un'impostazione dogmatica che, così come oramai si ammette (più o meno) pacificamente per la colpa, valorizzi il carattere "doloso" del fatto già sul piano della tipicità.

Il reato a dolo specifico si caratterizza per il *rapporto di mezzo a fine* che lega la condotta *oggettivamente descritta* con un determinato scopo dell'agente, solo *soggettivamente espresso*. Nei reati a dolo specifico il legislatore richiede che un determinato *fine soggettivo* sorregga una *condotta oggettiva*, la quale viene dunque considerata strumentale rispetto al primo.

Il fine dell'azione non soltanto forma oggetto di rappresentazione da parte dell'agente, ma ha anche efficacia causale (sia pure non esclusiva) sull'azione esterna, configurandola come *esecutiva* di un'unica, globale volontà d'agire: porre in essere il comportamento strumentale oggettivamente descritto dalla norma deve costituire già la parziale realizzazione del fine, in quanto momento necessario al suo pieno verificarsi. "*Solo* se sussiste questa connessione condizionante con il contenuto finalistico determinato dalla legge, la stessa condotta o fatto-base "oggettivi" possono dirsi anche *tipici*" [42].

Se inteso quale specificazione del solo elemento soggettivo, il fine dell'agente si trova esposto al rischio di essere accertato dopo il fatto tipico e dopo il dolo generico. Al contrario, se riconosciuto quale elemento costitutivo della tipicità, l'accertamento del fine specifico implicherà la previa prova del nesso teleologico già nel momento dell'accertamento della condotta, attraverso la presenza di dati che, ulteriori rispetto al comportamento materiale (tipizzato), ne dimostrino la caratteristica strumentalità, necessaria ad integrare il fatto tipico. E tale accertamento dovrà, logicamente, precedere quello dei presupposti d'imputazione soggettiva del fatto all'agente.

Nei reati a dolo specifico, il legislatore intende quindi dare espresso rilievo normativo all'interesse dell'agente per la cui soddisfazione sarebbe oggettivamente necessario il realizzarsi del risultato o l'esplicarsi delle attività ulteriori, indicati dalla fattispecie come contenuto del fine tipico.

La strumentalità del comportamento alla soddisfazione del predetto interesse di parte, perseguito dall'agente, costituisce un dato sintomatico del contenuto *oggettivamente lesivo* che il fatto ha rispetto al bene giuridico tutelato. In altri termini, nel fatto di reato viene tipizzato uno specifico "conflitto intersoggettivo di interessi": da un lato quello che anima l'agente; dall'altro quello dell'ordinamento alla protezione del bene giuridico. Ed è proprio per perseguire il proprio interesse che l'agente lede, *strumentalmente*, l'interesse della vittima: sinteticamente, offende il bene giuridico [43]. Quanto al fatto che – come noto – per aversi reato non è necessario che il reo realizzi compiutamente il fine che lo spinge all'azione, esso è conseguenza naturale della circostanza che non solo il *raggiungimento materiale*, ma anche il mero *perseguimento* di un certo interesse di parte, mediante una determinata azione esterna, può realizzare *oggettivamente* lo specifico conflitto intersoggettivo di interessi rilevante per il diritto penale. In tale prospettiva è quanto mai evidente come lo scopo perseguito dall'agente non possa ridursi a dato meramente interiore, dovendo al contrario la proiezione finalistica riflettersi anche all'esterno, quale dato reale ed oggettivamente apprezzabile. Breve: l'interesse di

[42] L. PICOTTI, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, p. 502. L'intera opera dell'A. è dedicata ad argomentare l'impostazione anche qui proposta e già suggerita anche in M. GROTTO, *op. cit.*, p. 155 ss.

[43] L. PICOTTI, *Il dolo specifico*, cit., p. 508.

parte deve sussistere *oggettivamente* per poter entrare *realmente* in conflitto con il bene o interesse tutelato, anche se poi la consumazione del reato prescinde dalla materiale, effettiva *realizzazione* del risultato finale.

Il fine specifico, proprio perché esprime la direzione finalistica che viene impressa al comportamento dell'agente, "non può confondersi con il dolo in genere, ma ne puntualizza, piuttosto, l'*oggetto*".

CAPITOLO 10

L'unità virtuale del diritto penale dell'informatica

di *Francesca Romana Fulvi*

1. Premessa

È noto che l'emergere di nuove forme di criminalità connesse alla progressiva diffusione delle tecnologie informatiche e all'impiego sempre più frequente ed esteso del *computer*, in diversi ambiti di attività, ha portato ad unificare una serie di comportamenti illeciti sotto la dizione di "crimini informatici".

Dottrina e giurisprudenza qualificano "informatici" tutti i reati realizzati attraverso l'utilizzo di un *personal computer*, di sistemi informatici o telematici, oppure commessi in danno del predetto elaboratore o del sistema elettronico, ovvero in danno di programmi, informazioni, dati ivi contenuti, che costituiscono, dunque, l'oggetto materiale della condotta criminosa [1].

All'interno della categoria dei *computer's crimes* si suole ricomprendere sia gli "illeciti eventualmente informatici" sia i "reati necessariamente informatici" [2].

I primi sono quelli rispetto ai quali l'utilizzazione delle summenzionate tecnologie informatiche ha solo ampliato l'ambito delle possibili forme di realizzazione di reati già previsti e sanzionati dall'ordinamento, i quali possono essere posti in essere anche senza ricorrere all'impiego di strumenti informatici e telematici [3]. Tra questi rientrano, sicuramente, i c.d. reati cibernetici, ovvero commessi in Rete [4].

[1] Per un approfondimento delle problematiche emerse a seguito del tentativo di definire la categoria dei reati informatici si rinvia a F. MUCCIARELLI, voce *Computer (disciplina giuridica del)*, in *Dig. disc. pen.*, Torino, 1988, p. 373; C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 1 ss.; D. PETRINI, *La responsabilità penale per i reati*, Napoli, 2004, p. 24 ss., il quale evidenzia che da un lato in dottrina sono state proposte opzioni troppo ampie e generali, che "*se consentivano di ricomprendere ogni sorta di comportamento offensivo legato all'uso del computer, finivano per perdere qualsiasi utile valenza classificatoria*", dall'altro si è posto l'accento soprattutto sul nuovo mezzo di aggressione utilizzato dai criminali informatici, limitando, di conseguenza, gli interventi del legislatore a semplici modifiche di fattispecie preesistenti.

[2] Sulla distinzione cfr. S. AMORE-V. STANCA-S. STARO, *I crimini informatici*, Camerino, 2006.

[3] Un esempio di reato eventualmente informatico può essere rinvenuto nel furto commesso avvalendosi delle tecnologie informatiche: si applicherà, infatti, l'art. 624 c.p. anche nell'ipotesi in cui la sottrazione e l'impossessamento della cosa mobile altrui sia avvenuta senza il ricorso agli strumenti informatici o telematici. Per una disamina dei possibili impieghi delle tecnologie informatiche da parte delle associazioni illecite per realizzare reati "comuni" cfr. V. MILITELLO, *Informatica e criminalità organizzata*, in *Riv. trim. dir. pen. econ.*, 1990, p. 81 ss.

[4] Un esempio di reato cibernetico è costituito dalla diffamazione realizzata mediante *Internet*, in cui la propalazione dell'offesa si realizza attraverso l'utilizzo di strumenti informatici o telematici, e punita, come l'ipotesi

I secondi sono quegli illeciti a cui sono applicabili solo fattispecie di reato specificamente "informatiche", cioè formulate dal legislatore per perseguire nuove forme di criminalità che coinvolgono direttamente sistemi informatici o telematici [5].

2. Nascita del diritto penale dell'informatica

Il c.d. diritto penale dell'informatica è costituito da un insieme eterogeneo e non coordinato di norme, dislocate in luoghi diversi del codice penale ed in leggi speciali complementari [6], e formatosi in modo alluvionale e disorganico sotto la spinta dell'esigenza di predisporre strumenti di tutela *ad hoc* contro le nuove aggressioni perpetrate attraverso l'impiego della tecnologia informatica e di adempiere gli obblighi assunti in sede comunitaria e internazionale [7].

In occasione del primo significativo intervento del 1993 [8], infatti, il legislatore nazionale non ha inserito i reati informatici all'interno del tessuto normativo seguendo un disegno organico e sistematico [9], in modo da ridurre al minimo le ipotesi di contraddittorietà o di duplica-

base, ai sensi dell'art. 595 c.p. I reati cibernetici, infatti, sono una categoria aperta, che ricomprende sia fattispecie che prevedono specificamente, tra i loro elementi costitutivi, il riferimento a mezzi e/o oggetti "informatici", sia le incriminazioni offensive di beni giuridici "tradizionali" se riferibili, in via interpretativa, a condotte realizzate servendosi di *Internet* e della tecnologia delle telecomunicazioni. *Internet*, infatti, essendo una rete "globale" accessibile a tutti gli utenti e garantendone l'anonimato, costituisce un mezzo attivo di realizzazione dei comportamenti illeciti, e non solo l'oggetto delle stesse (L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, pp. 28 e 58 ss.). Sulle possibili esplicazioni delle condotte di reato in Rete o, in generale, attraverso l'utilizzo delle tecnologie informatiche e telematiche si rinvia anche a F. MANTOVANI, *Diritto penale. Parte Speciale. Delitti contro la persona*, I, Padova, 2005, p. 481 ss.; C. PECORELLA, *op. cit.*, p. 28 ss.; F. RUGGIERO, *Ciberspazio e diritto penale: il problema del bene giuridico*, in *Riv. pen.*, 2001, 3, p. 218.

[5] L'evoluzione della civiltà tecnologica e la progressiva diffusione delle tecnologie informatiche e telematiche, infatti, hanno comportato la necessità di prevedere nuove ipotesi di reato in precedenza neppure ipotizzabili. Giova specificare, però, che nei reati necessariamente informatici il mezzo impiegato può anche non essere informatico (nel danneggiamento, ad es., si può procedere alla cancellazione dei dati anche attraverso mezzi meccanici), ma l'oggetto materiale della condotta deve essere sempre un *personal computer* o un sistema informatico o telematico, ovvero programmi, informazioni, dati in essi contenuti (cfr. D. PETRINI, *op. cit.*, p. 29). Sono reati informatici in senso stretto, ad es., la truffa realizzata con l'alterazione di un sistema informatico o telematico o frode informatica (art. 640 *ter* c.p.) e l'accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.).

[6] Ad esempio, nel codice penale compare il reato di frode informatica (art. 640-*ter* c.p.) tra i delitti contro il patrimonio e sono distribuite tra i delitti contro l'inviolabilità del domicilio e contro l'inviolabilità dei segreti le altre fattispecie introdotte *ex novo* nel 1993, che forse avrebbero meritato una collocazione autonoma. Altre fattispecie compaiono invece in leggi speciali: i reati di indebito utilizzo di carte di credito o bancomat (legge n. 197 del 1991) e quelli contenuti nella legge sul diritto d'autore (legge n. 633 del 1941), nei decreti legislativi sulla protezione dei dati personali (d.lgs. n. 196 del 2003) e sul commercio elettronico (d.lgs. n. 70 del 2003). Sulla *ratio* della collocazione topografica dei reati informatici cfr. L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 30 ss.

[7] In questo senso L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 22 ss.

[8] Legge 23 dicembre 1993, n. 547, pubblicata in *G.U.* 30 dicembre 1993, n. 305. Anteriormente alla legge n. 547 del 1993 il legislatore aveva predisposto una tutela frammentata ed occasionale, derivante da situazioni contingenti o dall'esigenza di ottemperare obblighi assunti in seno alla Comunità Europea. Per un'analisi degli interventi normativi antecedenti e successivi all'emanazione della legge n. 547 del 1993 si rinvia a L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 26 ss., il quale evidenzia il passaggio, con la novella legislativa del 1993, dalla fase dei *computer-crime* a quella del *cyber-crime*; Id., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, 2, p. 189 ss.

[9] Ciò che caratterizza, infatti, un sistema giuridico armonico (ovvero organizzato sistematicamente) è la distinzione delle categorie di tutela, la loro graduazione, la riduzione al minimo della probabilità di duplicazione o

zione dei precetti e quelle di lacune di previsione. Infatti, invece di emanare un'autonoma legge speciale *ad hoc* o di inserire gli illeciti in un distinto e specifico titolo del codice penale [10], si è preferito da un lato, modificare alcune tradizionali incriminazioni codicistiche al fine di renderle idonee a ricomprendere le condotte proprie della fenomenologia informatica [11], dall'altro, aggiungere all'interno dei diversi titoli dedicati ai delitti contro il patrimonio, l'inviolabilità dei segreti, ecc. delle fattispecie incriminatrici di nuovo conio [12] strutturate sul modello di altre già esistenti sulle quali si innestano come una sorta di peculiare estensione [13].

Tale scelta legislativa può essere compresa solo alla luce della considerazione che in un primo momento i *computer crimes* non sono stati percepiti come una originale e specifica ca-

di contraddittorietà dei precetti. Per un'approfondita analisi si rinvia alla diffusa ricostruzione operata da: F. MODUGNO, voce *Ordinamento giuridico*, in *Enc. dir*., XXX, Milano, 1980, p. 678 ss., che espone tutti gli aspetti della riflessione della dottrina sull'ordinamento giuridico.

[10] Nella relazione d'accompagnamento al d.d.l. n. 2773 (in *Documenti Giustizia*, 1991, p. 145), infatti, si afferma che la particolarità della materia non ha costituito una ragione sufficiente per giustificare una trattazione autonoma degli illeciti informatici in una legge speciale o in un apposito titolo. Si è sostenuto, infatti, che tale opzione legislativa avrebbe confinato "*la materia del diritto penale dell'informatica in un ambito non centrale dell'ordinamento penale, senza riuscire comunque ad esaurirne la disciplina*" (L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 44, il quale analizza anche i modelli e le fonti ispiratrici dei reati informatici, p. 30 ss). Le scelte normative operate dagli altri Stati comunitari sono state differenti: il legislatore portoghese, ad es., ha emanato una legge speciale (legge 17 agosto 1991, n. 109), quello francese ha preferito inserire un nuovo e specifico titolo all'interno del codice penale, volto a prevedere e a punire solo le infrazioni "essenziali" (dapprima con la legge del 5 gennaio 1988 n. 88/19, che ha introdotto il capo III, nel titolo II del libro III del *code pénal* "*Di certi illeciti in materia informatica*", poi con il nuovo *code pénal*, entrato in vigore il 1994, che al capo III, titolo II del libro III disciplina "*Lesione del sistema di elaborazione automatizzata di dati*"), quello tedesco, similmente a quello italiano, ha seguito il c.d. metodo evolutivo, collocando sistematicamente le nuove fattispecie incriminatrici accanto alle corrispondenti fattispecie tradizionali (seconda legge per la lotta alla criminalità economica 2. WiKG del 15 maggio 1986, modificato dallo *Strafrechtsanderungsgesetz zur Bekampfung der Computerkriminalitat* (BGBI, 1786), promulgato dal Parlamento tedesco l'11 giugno 2007). In merito cfr. V. FROSINI, voce *Telematica ed informatica giuridica*, in *Enc. dir.*, XLIV, Varese, 1992, p. 80; D. PETRINI, *op. cit.*, pp. 23 e 41 ss.; L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 44 ss.

[11] Si pensi, ad esempio, all'art. 491-*bis* c.p., rubricato "*Documenti informatici*", volto alla protezione della c.d. fede pubblica documentale, poiché estende la tutela prevista dalle norme del capo III del Titolo VII del libro II del c.p. al documento informatico privato o pubblico; agli artt. 616, 621, 623-*bis* c.p., rubricati "*Violazione, sottrazione e soppressione di corrispondenza*", "*Rivelazione del contenuto di documenti segreti*" e "*Altre comunicazioni e conversazioni*", che ampliano la tutela contenuta nelle relative fattispecie ricomprendendo anche la corrispondenza informatica o telematica, il documento informatico e qualunque altra trasmissione a distanza di suoni, immagini o altri dati.

[12] In questo senso F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, p. 2329. Si pensi, ad es., all'art. 640-*ter*, c.p., rubricato "*Frode informatica*", modellata sul paradigma della truffa comune di cui all'art. 640 c.p. e volto alla tutela del patrimonio. Nella frode informatica il legislatore, per descrivere adeguatamente le truffe commesse con l'ausilio del *computer*, ha sostituito gli artifici o raggiri attraverso i quali l'agente consegue un indebito profitto per sé o per altri con altrui danno, con l'alterazione delle funzioni di un sistema informatico o telematico o con l'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi ivi contenuti, prescindendo dall'induzione in errore di un soggetto fisico. La volontà della vittima, infatti, è viziata dall'aggiramento o dalla manipolazione delle procedure e dei meccanismi decisionali (automatizzati per il ricorso all'informatica) su cui faceva legittimo affidamento. La manipolazione o l'azione abusiva interrompe la corrispondenza tra il risultato della condotta della vittima e la sua reale e genuina volontà, seppur mediata dal sistema automatizzato. Per un'analisi dei riflessi sul piano giuridico della sostituzione del processo decisionale reale della mente di una persona con il trattamento dei dati affidato all'elaboratore si rinvia a L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 44 ss.

[13] Per un dettagliato esame delle tecniche di formulazione normativa utilizzate dal legislatore in riferimento ai reati informatici si veda L. PICOTTI, *Internet e diritto penale*, cit., p. 191 ss.; ID., *Sistematica dei reati informatici*, cit., p. 48 ss.

tegoria di illeciti, ma come nuove forme di aggressione, caratterizzate dal mezzo [14] o dall'oggetto materiale, a beni giuridici e a interessi tradizionali (patrimonio, fede pubblica, integrità dei segreti, diritto d'autore, ecc.) già oggetto di tutela [15].

Il diritto penale dell'informatica, pertanto, sarebbe un modo di dire al quale non corrisponde un impianto normativo organico e sistematico, le cui sparse membra dovrebbero trovare una ricomposizione soltanto per la costanza del mezzo di realizzazione degli illeciti.

Tuttavia, insistere sul mezzo mette in discussione la distinzione tra reati cibernetici in senso stretto o proprio e reati cibernetici relativi ai contenuti o in senso improprio e l'uniformità. Inoltre, la constatata mancata individuazione di una categoria dai contenuti omogenei ha portato alcuni autori a interrogarsi sull'esistenza di un diritto penale dell'Informatica [16], quale sotto-sistema del diritto penale comune, avente per oggetto di tutela un particolare e nuovo aspetto della realtà: la realtà virtuale [17].

---

[14] Al riguardo P. SCOGNAMIGLIO, *Criminalità informatica*, Napoli, 2008, p. 293, rileva che la scelta legislativa di inserire delle nuove figure di reato all'interno del codice penale "*riflette indubbiamente la consapevolezza che non si trattava d'introdurre fattispecie che tutelassero nuovi beni giuridici, ma di introdurre delle tutele contro nuove forme di aggressione, portate cioè con modalità nuove, a beni in larga parte già penalmente rilevanti e tutelati con norme codicistiche*". Nello stesso senso F. RUGGIERO, *op. cit.*, p. 218. In senso critico, invece, si rinvia a D. PETRINI, *op. cit.*, p. 25, il quale evidenzia come la limitazione della "*novità al mezzo di aggressione riconduceva le (mai negate) esigenze di riforma a modesti interventi di aggiustamento nei confronti di fattispecie già esistenti*". Per la trattazione in generale dei reati caratterizzati dal mezzo di aggressione si rinvia a S. FIORE, *Ratio della tutela e oggetto di aggressione nella sistematica dei reati di falso*, Napoli, 2000, p. 19, secondo il quale "*il criterio del bene giuridico tutelato non può essere esaustivo dell'organizzazione sistematica, risultando spesso affiancato ed integrato da altri criteri (in particolare quello fondato sulle modalità di aggressione), che tuttavia sarebbero solo sussidiari, nel senso che si muovono sempre all'interno del criterio principale, vale a dire quello del bene giuridico tutelato*".

[15] In questo senso la relazione d'accompagnamento al d.d.l. n. 2773 e, in dottrina, cfr. G. PICA, *La disciplina penale degli illeciti in materia di tecnologie informatiche*, in *Riv. pen. ec.*, 1995, p. 404. I primi commentatori hanno giudicato positivamente la scelta sia di collocare entro il codice la repressione delle nuove patologie della fenomenologia informatica a fronte della tendenza ad espandere, in modo incontrollato, la legislazione penale speciale, sia di non dare autonomia sistematica alla nuova normativa. In generale, sulle motivazioni che giustificano la scelta di modificare il codice penale F. RUGGIERO, *op. cit.*, p. 218. In senso critico cfr. F. BERGHELLA-R. BLAIOTTA, *op. cit.*, p. 2330, i quali osservano anche che il legislatore, per soddisfare un'esigenza di coerenza sistematica ha "*peccato di artificiosità*" e che sul pano lessicale "*l'attaccamento rituale alle formule tradizionali ha talora nuociuto alla messa a fuoco di tratti originali della nuova fenomenologia*".

[16] Tra gli autori che si sono maggiormente occupati della materia si consideri C. PECORELLA, *op. cit.*; G. PICA, voce *Reati informatici e telematici*, in *Dig. disc. pen.*, Agg., Torino, 2000, p. 521; L. PICOTTI, voce *Reati informatici*, in *Enc. giur. Treccani*, Agg., VIII, Roma, 2000, pp. 1-33; ID., *Sistematica dei reati informatici*, cit.; Id., *Internet e diritto penale*, cit., p. 189 ss., il quale rileva che l'ordinamento italiano, a partire dagli anni '90 si è dotato di un articolato "diritto penale dell'informatica", "*sovrabbondante di incriminazioni e con livelli sanzionatori piuttosto severi, ma privo di un organico disegno sistematico, che alla prova dei fatti non ha dimostrato di saper garantire un livello adeguato di prevenzione e controllo*». L'autore, ancora, ritiene che "*il quadro complessivo non può dirsi soddisfacente, di fronte alla perenne evoluzione della tecnologia, da un lato, ed alla sempre più accelerata internalizzazione e globalizzazione dei rapporti economici, politici, sociali – e quindi anche giuridici – dall'altro, emblematicamente sintetizzate dall'estensione di quelli che si svolgono in Internet*"; C. SARZANA DI SANT'IPPOLITO, *Note sul diritto penale dell'informatica*, in *Giust. pen.*, 1994, I, p. 21 ss., il quale individua il diritto penale dell'informatica quale sottospecie del diritto dell'informatica. Giova specificare che il diritto dell'informatica deve essere distinto dall'informatica giuridica, la quale ha ad oggetto la funzionalità pratica attribuita all'informatica come strumento ausiliario operante nell'ambito del diritto (ad es. le ricerca automatica di dati legislativi o giurisprudenziali, la creazione di archivi bibliografici, l'automazione delle procedure giudiziarie, ecc.). Sulla predetta distinzione cfr. anche V. FROSINI, *La criminalità informatica*, in *Dir. inf.*, 1997, p. 488.

[17] Cfr. F.R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *Dir. pen. proc.*, 2009, 5, p. 639 ss. nel quale si evidenzia che il diritto penale dell'informatica è un diritto giovane, sia

3. Identificazione di un sottosistema autonomo

La ragione che giustifica [18] l'introduzione di nuove norme – soprattutto nelle ipotesi in cui già sussistono delle disposizioni che potrebbero essere applicate, pur con qualche sforzo interpretativo – deve essere la necessità di tutela di nuovi beni giuridici specifici o di un nuovo bene giuridico di categoria [19], che poi si specifica nei vari profili costitutivi delle singole norme incriminatici. Pertanto, le nuove norme che incriminano i reati informatici postulano un bene giuridico di categoria che fondi l'unitarietà e la ragion d'essere dei reati informatici e consenta di autonomizzarli rispetto ai reati, non commessi con il mezzo informatico, che offendono beni preesistenti: la fede pubblica, l'ordine pubblico, il patrimonio, la proprietà intellettuale, la riservatezza. Infatti, la sottolineatura del mezzo di aggressione non supera due obiezioni: la prima, che esso è sempre uguale in tutti i casi, quale che sia il bene preesistente volta a volta aggredito, dimostrando così la ridondanza del mezzo rispetto al supposto bene finale esclusivo; la seconda, che se il mezzo fosse soltanto tale, e cioè modalità della condotta, la sua rilevanza nell'ambito della disciplina della fattispecie potrebbe essere soltanto circostanziale, mentre le previsioni sono strutturate invece come titoli autonomi di reato.

Effettivamente, la dottrina [20] ha parlato di "intangibilità informatica" intesa come "*esigen-*

in senso antropologico, per il metro attuale dell'esistenza in vita, sia in senso tecnico di ragguaglio dell'evoluzione giuridica.

[18] Per un approfondimento della tematica si rinvia a: S. COTTA, *Le probléme de la justification scientifique des normes*, in *Riv. int. fil. dir.*, 1979; ID., *Giustificazione e obbligatorietà delle norme*, Milano, 1981, il quale precisa che oggetto della giustificazione è la prescrizione normativa. Sulla necessità del legislatore di recepire le nuove esigenze di tutela che si manifestano nella società cfr. F.C. PALAZZO, *I confini della tutela penale: selezione dei beni e criteri di criminalizzazione*, in *Riv. it. dir. proc. pen.*, 1992, p. 453 ss.

[19] Escludono l'emersione di un nuovo e unitario bene giuridico, meritevole di autonoma protezione penale, F. BERGHELLA-R. BLAIOTTA, *op. cit.*, p. 2335; L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 87 secondo il quale la categoria dei reati informatici non individua un ambito di tutela dai contenuti omogenei "*od ancor meno connotato da un unitario bene giuridico ... bensì una categoria cui devono ricondursi fatti che offendono beni giuridici molto diversi tra loro*"; D. FONDAROLI, *La tutela penale dei "beni informatici"*, in *Dir. inf.*, 1996, p. 302 e A. ROSSI VANNINI, *La criminalità informatica: le tipologie di computer crimes di cui alla legge 547/93 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. dir. pen. ec.*, 1994, p. 433, le quali motivano la predetta esclusione sulla base della scelta del legislatore di estendere alle nuove ipotesi di criminalità informatica la tutela già prevista per beni giuridici "consolidati"; F. RUGGIERO, *op. cit.*, p. 213, il quale esprime dei rilievi critici sull'automatico recepimento di beni di nuova emersione nell'alveo della protezione penale in quanto "*l'eccessiva rapidità del processo di diffusione informatica rende problematica la costruzione teorica di un autonomo ed unitario bene giuridico meritevole di protezione penale, ove si rifletta sulla necessità di collocare nel lungo periodo la formazione delle intese socio-culturali necessarie all'aggregazione di un distinto oggetto di tutela*". Secondo l'autore il processo tecnologico "*da un lato, senza dar vita ad un distinto bene giuridico, ha frequentemente conferito una dimensione sociale a situazioni giuridiche individuali, che hanno così subito quell'evoluzione dalla sfera del privato a quella del pubblico tipica degli interessi diffusi; dall'altro, ha esposto valori già garantiti nell'ordinamento a nuove possibilità di lesione*".

[20] In riferimento all'emersione di un nuovo bene, meritevole di protezione penale, legato allo sviluppo dell'informatica e della telematica all'interno del sistema penale si rinvia a D. PETRINI, *op. cit.*, p. 29, il quale evidenzia che il "bene informatico" è costituito da tre diverse entità: i dati (la rappresentazione originaria di un fatto o evento attraverso i simboli), le informazioni (l'insieme di dati, organizzati secondo una logica che consente di attribuire loro un particolare significato) ed il programma, cioè il *software* (una sequenza di istruzioni, comprensibili dal *computer*, per ottenere il compimento di operazioni prestabilite); G. PICA, *Reati informatici*, cit., p. 522 ss., secondo il quale la *ratio* della tutela penale si radica nella "*necessità di salvaguardare e garantire la 'libertà informatica' di ciascuno*", intesa sia in senso positivo (poter accedere alla tecnologia informatica e soprattutto telematica), che negativo (escludere l'altrui ingerenza); L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 70 ss., il quale segnala l'emersione sia del bene della riservatezza informatica sia di quello dell'integrità e della sicurezza informatica, quale garanzia del corretto e genuino funzionamento dei programmi informatici

za di non alterare la relazione triadica tra dato della realtà, rispettiva informazione e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)"[21] oppure di "*bene immateriale con carattere di diritto reale, ossia di inerenza del diritto al bene che ne rappresenta l'oggetto*"[22] o ancora di "tutela dell'informazione", affidata alla memoria del computer, considerata come diritto della personalità e bene economico e politico[23].

Tuttavia, l'identificazione del bene giuridico categoriale[24] si presenta di non semplice soluzione perché i reati informatici compaiono all'interno di titoli e di capi preesistenti del codice, oppure, se sono previsti da leggi speciali, le fattispecie sono soltanto sanzionatorie dell'inosservanza della normativa extrapenale del settore di riferimento[25]. Dall'analisi della

nonché di ogni altra elaborazione o trattamento automatizzato di dati, rilevante nei rapporti giuridici, la cui tutela è affidata alle fattispecie di danneggiamento.

[21] V. MILITELLO, *Informatica e criminalità organizzata*, cit., p. 85; ID., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. ec.*, 1992, p. 374.

[22] V. FROSINI, *La criminalità informatica*, cit., p. 488, secondo il quale il reato informatico colpisce un nuovo bene economico che, "*riconosciuto e protetto dalle leggi, diventa un nuovo bene giuridico. Esso è infatti l'oggetto di un nuovo diritto di carattere reale, ossia di inerenza del diritto al bene che ne rappresenta l'oggetto, di jus in re propria, anche se si tratta di una res o cosa immateriale, come lo sono del resto anche i prodotti intellettuali, ma che è stata resa oggettiva, cioè misurabile in termini di valore economico e trasmissibile*"; ID., voce *Telematica ed informatica giuridica*, cit., p. 64; ID., *L'orizzonte giuridico dell'internet*, in *Dir. inf.*, 2000, p. 275, nel quale l'autore lega l'emergere del nuovo bene, il diritto di libertà informatica (intesa nel senso di libertà dalle intrusioni delle tecnologie informatiche), allo sviluppo di *internet*. Critici nei confronti di questa impostazione S. AMORE-V. STANCA-S. STARO, *op. cit.*, p. 52 ss., che ritengono il concetto di libertà informatica troppo indefinito per poter costituire un efficace strumento di unificazione concettuale delle nuove incriminazioni; G. PICA, *Reati informatici*, cit., p. 523, secondo il quale è necessario non limitare il concetto di libertà informatica agli aspetti di tutela della persona dalle altrui informazioni, ma estenderlo ai profili concernenti la generale regolamentazione (della libertà) di uso delle nuove tecnologie).

[23] U. SIEBER, *La tutela penale dell'informazione*, in *Riv. trim. dir. pen. ec.*, 1992, p. 492. L'autore si riferisce alle informazioni intese in senso ampio, cioè a tutto ciò che un privato cittadino, un'impresa o un'amministrazione pubblica affida alla memoria di un computer, e non alle informazioni in senso tecnico, ovvero alla aggregazione dei dati per renderli comprensibili all'uomo. Secondo la predetta impostazione l'informazione costituisce una "grandezza di base", come la materia e l'energia. Aderisce a tale proposta D. PETRINI, *op. cit.*, p. 33.

[24] Sull'identificazione del bene giuridico protetto si veda L. PICOTTI, *Reati informatici*, cit., p. 6; ID., *Sistematica dei reati informatici*, cit., p. 21; ID., *Internet e diritto penale*, cit., p. 191. L'autore individua diversi beni giuridici protetti che "*mentre nelle fattispecie codicistiche essi sembrano facilmente enucleabili dalla stessa collocazione dei fatti tipici che li offendono, affiancati a quelli più simili già prima vigenti, distinguendosene soprattutto per le nuove modalità di lesione o i diversi oggetti passivi su cui le condotte ricadono, negli altri reati informatici, in cui la norma penale si limita sostanzialmente a stabilire le sanzioni, rinviando per il precetto, o per fondamentali elementi del fatto tipico, alle specifiche discipline extrapenali a cui accedono, talora anche a provvedimenti concreti delle autorità amministrative competenti alla vigilanza e regolamentazione in dettaglio di singole situazioni o parti della materia ... la determinazione dei beni giuridici appare molto più incerta, ponendosi a cavallo fra interessi sostanziali tutelati dal complesso sistema ... e la mera osservanza delle statuizioni extrapenali ovvero la tutela delle funzioni delle menzionate autorità, competenti alla gestione e controllo dei rispettivi settori*".

[25] Si pensi, ad esempio all'art. 167 del d.lgs. n. 196 del 2003, che sanziona il trattamento illecito dei dati, consistente nel fatto di procedere alle varie attività rientranti nel concetto generale di "trattamento" (definito dall'art. 4, lett. a) del d.lgs. n. 196 del 2003) in violazione dei precetti contenuti negli artt. 18 e 19 (sui principi regolatori applicabili al trattamento dei dati da parte di soggetti pubblici), 23 (sul consenso dell'interessato), 123, 126 e 130 ovvero in applicazione dell'art. 129 (norme che attengono al settore della telefonia e delle "comunicazioni elettroniche"); all'art 170 del d.lgs. n. 196 del 2003, che punisce l'inosservanza dei provvedimenti adottati dal Garante ai sensi degli artt. 26, secondo comma, 90, 143, comma 1, lett. c) e 150, commi 1 e 2. Per una compiuta trattazione delle norme penali meramente sanzionatorie di precetti extrapenali nell'ambito dei reati informatici si veda L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 38 ss.; ID., *Internet e diritto penale*, cit., p. 191.

normativa[26], però, emerge che l'individuazione dei *computer crimes* come offensivi di beni tradizionali con modalità nuove è insufficiente, in quanto risulta "*incapace di descrivere alcune delle tipologie più comuni, pericolose e diffuse di criminalità informatica*"[27].

Inoltre, la sussistenza di un bene ulteriore deve essere ritenuta a causa dell'ampliamento di alcune delle fattispecie tradizionali, eseguita *non* con la previsione di circostanze aggravanti, di per sé evidentemente insufficiente[28], bensì di titoli autonomi di reato di nuove fattispecie incriminatrici. Altra volta si fa, invece, ricorso a norme interpretative definitorie[29], come ad es. gli artt. 616 e 621 c.p., necessarie per identificare la materia (i fatti nuovi cui la norma vecchia può essere applicata) per evitare l'applicazione analogica *in malam partem*[30] delle disposizioni preesistenti. Inoltre, non si deve trascurare che i reati informatici si consumano in un mondo virtuale, sicché deve essere adattato ad essi il tradizionale concetto di oggetto mate-

[26] Il recepimento o meno di un nuovo bene, meritevole di protezione penale, non deve essere verificato sulla base della collocazione topografica delle norme, ma attraverso l'analisi degli elementi costitutivi della fattispecie cfr. D. PETRINI, *op. cit.*, p. 42 ss.

[27] Sul punto si rinvia D. PETRINI, *op. cit.*, p. 27 ss., il quale sottolinea come la diffusione dell'informatica pone un problema di tutela (anche penale) qualitativamente nuovo "*che non possono ridursi ad un mero restyling delle fattispecie esistenti*". In riferimento, ad es., all'accesso abusivo l'autore osserva come il reato *de quo* "*non è un furto commesso con l'uso del computer, ma qualcosa di radicalmente, qualitativamente diverso, in virtù dell'irriducibilità del bene informatico alle tradizionali modalità aggressive del patrimonio*"; mentre in riferimento alla frode informatica afferma che non si tratta di una truffa commessa con l'uso del *computer*, ma di un illecito che si caratterizza per la modalità di estrinsecazione della condotta ovvero l'accesso abusivo alla memoria di un *computer* (o lo sfruttamento indebito della liceità del proprio accesso) per alterare un sistema o per intervenire su dati, informazioni e programmi (47).

[28] In merito alla difficoltà di ricostruire i reati commessi nei contesti informatizzati nel caso di "*adozione dei meccanismi giustificativi tradizionali*" si rinvia a F. RUGGIERO, *op. cit.*, pp. 213 e 217, il quale osserva che la particolare natura dei beni informatici (privi di materialità) e la problematica qualificazione dell'elaboratore elettronico come soggetto passivo del reato ostacolavano l'applicazione delle norme penali classiche. In riferimento alla truffa informatica *ex* art. 640-*ter* c.p., ad es., D. FONDAROLI, *La tutela penale dei "beni informatici"*, cit., p. 305 osserva che la *ratio* della disposizione discende dalla difficoltà di applicazione della fattispecie tradizionale di truffa *ex* art. 640 c.p. nel caso in cui la medesima sia perpetrata attraverso l'impiego di tecniche informatiche e telematiche.

[29] Per un esame delle nozioni definitorie di oggetti informatici e dell'integrazione ed estensione delle nozioni comuni si veda L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 48 ss.; ID., *Internet e diritto penale*, cit., p. 191 ss. In merito D. PETRINI, *op. cit.*, p. 26 ss. sottolinea che il ricorso a norme interpretative è inidoneo quando si prendono in considerazione situazioni più complesse quali, ad es., l'accesso abusivo ad un sistema informatico o telematico. Il legislatore, infatti, non ha potuto estendere il concetto di "cosa" anche ai dati, alle informazioni protette nel *computer* e ai programmi di un sistema informatico perché quest'ultimi "*non possono, per loro natura, essere oggetto di appropriazione e di sottrazione*", pena la violazione del divieto di analogia in *malam partem* (in merito alla mancata assimilazione dei "beni informatici" ai beni corporali e alle energie si rinvia anche a C. SARZANA DI SANT'IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010, p. 95 ss. e all'approfondita analisi di D. FONDAROLI, *La tutela penale dei "beni informatici"*, cit., p. 295 ss.).

[30] Un esempio significativo è costituito dall'art. 635-*bis* c.p., che nella sua struttura di base ricalca il modello del delitto di danneggiamento comune di "cose", di cui all'art. 635 c.p., ma dallo stesso si discosta non solo sul piano sanzionatorio, per la maggiore gravità della pena, ma soprattutto per la diversità dell'oggetto materiale della condotta (informazioni, dati o programmi informatici), la cui lesione è stata ritenuta dal legislatore meritevole di una diversa valutazione giuridica. L'art. 635-*bis* c.p. mostra con chiarezza come la sua formulazione sia necessaria per evitare l'applicazione analogica *in malam partem* dell'art. 635 c.p.: infatti nell'art. 635-*bis* c.p. non si tratta di *cose*, mobili o immobili. Differentemente, infatti, dall'art. 624 c.p., ove il legislatore al secondo comma dispone che "*Agli effetti della legge penale si considera cosa mobile anche l'energia elettrica e ogni altra energia che abbia valore economico*", l'art. 635-*bis* c.p. non è costruito come una norma pseudo-interpretativa (che, cioè, interpreta, ma sostanzialmente amplia la materia del divieto, svolgendo la funzione di norma incriminatrice, cfr. F. RAMACCI, *Corso di diritto penale*, Torino, 2007, p. 208). Ciò può essere considerato un indice che rivela come questa nuova incriminazione non si limita a proteggere il solo valore economico-patrimoniale della "cosa", ma tutela la stessa funzionalità delle procedure di elaborazione e trasmissione dati, profilo estraneo all'art. 635 c.p.

riale del reato[31]: cosa che non è senza significato per le fattispecie quali il furto o il danneggiamento[32].

4. Il bene giuridico di categoria

L'interesse sopranazionale allo sviluppo e alla protezione dello spazio cibernetico, testimoniato dalle numerose direttive e convenzioni UE, tra cui la più recente convenzione c.d. *Cybercrime*, indirizza indubbiamente l'operatore del diritto ad interpretare il diritto penale dell'informatica alla luce del suo oggetto di tutela categoriale: l'affidabilità e la sicurezza del ricorso alla tecnologia informatica, telematica e cibernetica[33].

Questo oggetto categoriale si specifica in vari profili, ad esempio quello della protezione, del controllo, della garanzia.

Come già in precedenza sottolineato[34], detto bene, così come sopra delineato, rievoca un suo antecedente, la fede pubblica[35], in quanto pur avendo una sua consistenza ontologica chiaramente individuabile[36], è idoneo a designare un fenomeno che ha varie implicazioni[37],

[31] Per un'esauriente trattazione del concetto di *corpus criminis* si rinvia a: A. GARGANI, *Dal corpus delicti al Tatbestand. Le origini della tipicità penale*, Milano, 1997.

[32] La specificità delle modalità di realizzazione dei reati informatici impongono all'interprete, ma ancor prima al legislatore, uno sforzo di rielaborazione delle tradizionali categorie dogmatiche della teoria del reato. Sul punto L. PICOTTI, *Internet e diritto penale*, cit., p. 204, afferma che "*il passaggio dall'epoca del computercrime a quella del cybercrime non deve, dunque, determinare tanto l'introduzione aggiuntiva di nuove incriminazioni, con moltiplicazioni 'all'infinito' dei reati e delle regole, quanto portare, innanzitutto, ad una profonda rielaborazione sistematica della materia, toccando anche categorie fondamentali del diritto e della procedura penale, compresi alcuni tradizionali concetti di teoria generale – quali quelli di azione e di evento, con la correlata disciplina del tempus e del locus delicti, nonché di dolo, colpa, partecipazione criminosa, ecc. – su cui si basano la struttura e l'accertamento della responsabilità penale*". In senso contrario F. RUGGIERO, *op. cit.*, p. 217, secondo il quale sebbene l'informatica e la telematica hanno introdotto elementi di novità in ordine all'oggetto materiale del reato, al *locus commissi delicti*, ai soggetti e alle dinamiche di accertamento della responsabilità, lo sforzo dell'interprete "*dovrà essere orientato all'inserimento di questo materiale incandescente in ambiti di tutela di solida tradizione, sperimentando – se necessario – lievi correttivi rispetto a criteri e principi già metabolizzati dall'ordinamento*".

[33] L'informatica può essere definita come la scienza che studia l'elaborazione dei dati ed il loro trattamento automatico per mezzo di elaboratori elettronici; la telematica, invece, è la disciplina che si occupa dello scambio di informazioni tra sistemi di elaborazione dati per mezzo di reti di telecomunicazione. In merito cfr. V. FROSINI, voce *Telematica ed informatica giuridica*, cit., p. 61 ss.; F. MANTOVANI, *Diritto penale. Delitti contro la persona*, cit., p. 482; F. RUGGIERO, *op. cit.*, p. 213.

[34] F.R. FULVI, *La Convenzione Cybercrime*, cit., p. 642.

[35] L'individuazione di un bene giuridico di categoria riferibile a tutti i reati di falso è un obiettivo a lungo inseguito dalla scienza penalistica, all'interno della quale tuttavia numerose e autorevoli sono state le voci che, sul punto, hanno manifestato scetticismo, quando non decisa contrarietà. Per un'approfondita analisi del concetto di fede pubblica si veda F. RAMACCI, "*La falsità ideologica nel sistema del falso documentale*", Napoli, 1965, p. 221 ss. e ID., *Il progetto penale della bicamerale*, in *Studi Senesi*, 1998, f. 2, p. 205 ss., il quale rileva che la fede pubblica (come l'ambiente) costituisce un argomento importante per sostenere, in generale, che accanto alla rilevanza costituzionale diretta, è necessario considerare anche quella indiretta dei beni giuridici, se non altro per spiegare la costante sopravvivenza della tutela penale di beni costituzionalmente amorfi, come la fede pubblica, l'ambiente, ecc.

[36] È difficile descrivere compiutamente la consistenza ontologica del bene giuridico nell'espressione sincopata con cui si usa designarlo. Ciò non toglie che tutti ormai capiscono benissimo di cosa esso consista, anche se, per descrivere le sue varie specificazioni occorre illustrarlo con un discorso lungo e articolato.

[37] Dall'idoneità del bene fede pubblica a designare un fenomeno che ha varie implicazioni (ad es.: falsità in monete, in carte di pubblico credito e in valori di bollo; falsità in contrassegni, ovvero in sigilli o strumenti o se-

presenta le caratteristiche dell'immaterialità e dell'apparente eccessiva genericità e sembrerebbe, altresì, tutelare mezzi di prova o di comunicazione (sicché in luogo della tutela di un bene molti preferiscono parlare – come si è detto – di caratterizzazione dei reati sulla base del mezzo utilizzato per l'aggressione al bene protetto).

L'individuazione di un generico oggetto di tutela che si specifica nelle singole previsioni, pertanto, nella prospettiva di un'unificazione auspicabile, tende a limitare la rilevanza di singoli beni individuali offesi, ad esempio il patrimonio, la riservatezza, la proprietà intellettuale, che non possono più essere considerati come beni esclusivi [38] ma piuttosto come *marcatori di zona*, per graduare la gravità delle fattispecie, alcune delle quali, tra l'altro, potranno assumere la figura del reato transnazionale [39].

5. Conclusioni

L'esame della normativa dimostra che il diritto penale dell'informatica non costituisce un sottosistema autonomo di diritto penale speciale [40], ma un ibrido in parte aggregato al codice e

gni di autenticazione, certificazione o riconoscimento; falsità documentale o in atti; falsità personale) deriva, infatti, la genericità categoriale.

[38] In merito si rinvia a G. MARINUCCI-E. DOLCINI, *Corso di diritto penale*, Milano, 1995, p. 177 ss. i quali distinguono tra beni giuridici individuali, che fanno capo a singole persone e che l'ordinamento riconosce e garantisce in linea di principio a tutti gli esseri umani, rappresentando il contenuto di altrettanti diritti soggettivi individuali, e beni collettivi, che ricomprendono sia i c.d. beni istituzionali, cioè facenti capo allo Stato come espressione della collettività organizzata, ai suoi poteri od organi o ad altri enti pubblici, sia i beni la cui integrità rispecchia un interesse diffuso tra tutti i consociati o comunque fra cerchie ampie ed indeterminate di soggetti. Nell'ambito di quest'ultima categoria è possibile individuare i c.d. beni "strumentali" o "intermedi", tutelati dalle norme come autonomi beni giuridici e la cui integrità è strumento e condizione per la sopravvivenza di uno o più beni ulteriori, i c.d. "beni finali". Quest'ultimi "*restano sullo sfondo, nel senso che la loro lesione o messa in pericolo è irrilevante: ciò che richiede la norma incriminatrice è soltanto la lesione o la messa in pericolo del bene strumentale*". Sulla distinzione tra beni strumentali e finali cfr. anche F.C. PALAZZO, *I confini della tutela penale*, cit., p. 470 ss. Al riguardo la Corte costituzionale, nella sentenza n. 394/07 (in *Giur. cost*., 2006, 6, p. 4127 ss., con nota critica di G. DE MARTINO, *Brevi osservazioni in tema di norme penali di favore e di reati strumentali*, p. 4170 ss.) ha osservato che "*i reati di falso hanno natura tipicamente strumentale. Comune ad essi è difatti la protezione di un bene giuridico 'strumentale-intermedio', tradizionalmente compendiato nella formula della "'fede pubblica', intesa quale affidamento dei consociati nella genuinità e veridicità – ovvero, da un altro angolo di visuale, nell'efficacia probatoria – di determinate fonti documentali. Questo valore – ed in ciò risiede appunto la sua "strumentalità"– non è fine a se stesso, ma rappresenta un mezzo di protezione di beni 'finali' ulteriori, atti ad essere compromessi dalle manipolazioni delle predette fonti: beni 'finali' che, in rapporto alla loro variegata caratura (patrimoniale, personale, pubblica, collettiva, ecc.), ben possono contribuire a qualificare, sul piano del disvalore, le differenti ipotesi di falso*".

[39] Le nuove tecnologie informatiche hanno favorito la commissione di comportamenti illeciti che vanno oltre i confini territoriali di un singolo Stato, per assumere un carattere transnazionale: la mobilità dei dati nelle reti internazionali di telecomunicazione consente di commettere in un determinato Stato un reato che esplica i propri effetti in un altro Stato (cfr. U. SIEBER, *La tutela penale dell'informazione*, cit., p. 485). Con la legge n. 146 del 2006 è stata ratificata dal Parlamento Italiano la Convenzione dell'ONU che riguarda il crimine organizzato transnazionale. In particolare all'art. 3 si definisce quale "reato transnazionale" quello punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

[40] In questo senso F. RUGGIERO, *op. cit.*, p. 217, secondo il quale non è opportuno parlare della nascita di una nuova branca del diritto penale, il diritto penale dell'Informatica, "*ove con tale espressione s'intendano sot-*

in parte disperso in norme di legge non collegate tra loro, ma piuttosto connesse alla normativa extrapenale di settore nella quale sono inserite.

La dimensione unitaria del fenomeno, che appartiene alla natura delle cose in quanto prodotto della tecnologia informatica, telematica, cibernetica, e la crescente attenzione da parte dell'Unione europea devono però indurre il legislatore, così come è stato fatto in altri ordinamenti, a sistematizzare questo insieme eterogeneo di norme organizzandolo in un settore unificato attorno a un bene giuridico immateriale unitario anche se generico, che trovi via via specificazione nella differenziazione delle varie fattispecie attraverso le quali attinge la concretizzazione [41].

Tale conclusione necessita di due precisazioni.

In primo luogo, l'insistenza sull'individuazione di un bene giuridico generico, di categoria, non deve intendersi come una supina e tardiva adesione alla concezione metodologica [42] del predetto bene giuridico in funzione meramente classificatoria. [43].

Ciò che importa è invece che, ai fini di un'interpretazione sistematica, l'individuazione di un bene giuridico di categoria consenta di espungere dall'ambito delle opzioni ermeneutiche possibili quella che vorrebbe considerare "informatici" i reati caratterizzati dal peculiare mezzo di aggressione "informatico" [44]; opzione non condivisibile perché trascura il dato fonda-

tolineare risvolti di specificità e di dignità scientifica tali da trascendere le finalità descrittivo-didattiche di una trattazione omogenea".

[41] Per una compiuta elaborazione teorica del procedimento di concretizzazione del bene giuridico si rinvia a: G. MARINUCCI-E. DOLCINI, *Corso di diritto penale*, cit., p. 180 ss. In merito gli autori osservano che "*la dottrina è concorde nell'assegnare un modesto ruolo interpretativo ai c.d. beni giuridici 'di categoria' ('l'oggetto giuridico generico' nella terminologia di Arturo Rocco), spesso anzi ritenuti fuorvianti ed inesatti: ciò che solo può decidere ai fini dell'interpretazione della norma incriminatrice è 'l'oggetto giuridico specifico', vale a dire il bene, o i beni, che o sono espressamente menzionati nel testo della norma (e non soltanto nella rubrica o nell'intitolato), o si lasciano ricavare alla luce della specifica attitudine offensiva della condotta tipica*". In particolare, in riferimento al bene di categoria "fede pubblica" rilevano che l'interprete deve individuare "*i singoli documenti, contrassegni, dichiarazioni, attestazioni, ecc., destinati a provare singole verità, che rappresentano i veri oggetti capaci di tutela: solo nei loro confronti possono infatti sensatamente dirigersi aggressioni tipiche, capaci di offenderli ... minando la fiducia riposta dagli svariati destinatari nei singoli mezzi di prova documentali, per contrassegni, ecc.*". Si rinvia anche a F.C. PALAZZO, *I confini della tutela penale*, cit., p. 481, secondo il quale la concretizzazione deve essere intesa come un criterio di criminalizzazione che "*allude piuttosto alla necessità che la "distanza prospettica" tra il comportamento incriminato e l'interesse finale tutelato non sia così ampia da impedire di scorgere quest'ultimo nella concretezza del primo*".

[42] Per una critica, in generale, alla concezione metodologica del bene giuridico si rinvia a: F. RAMACCI, *Corso di diritto penale*, cit., p. 28 ss. Secondo la predetta impostazione "*l'indagine sul bene giuridico non è altro che la ricerca della ragion d'essere che è teleologicamente, finalisticamente individuata nella funzione che la norma è indirizzata a svolgere, nello scopo che con la sua emanazione il legislatore si proponeva di raggiungere*". In riferimento ai reati informatici F. RUGGIERO, *op. cit.*, p. 214 osserva che l'accoglimento della concezione metodologica comporta il rischio "*di tornare su sentieri esegetici che, enfatizzando in chiave criminologia i connotati fenomenici e lo scopo dell'azione criminosa, si rivelano – in subiecta materia – non risolutivi, se non fuorvianti*".

[43] L'adesione alla concezione metodologica del bene giuridico comporta l'eliminazione della sua funzione critica "*di riscontro oggettivo, di spiegazione e di prova della necessarietà dell'opzione penale sancita da una norma incriminatrice*". L'imposizione di una norma penale, infatti, in un ordinamento laico e liberale deve trovare la sua *ratio* in "*un'oggettiva esigenza, in un intenso bisogno sociale di tutela*". In questo senso F. RAMACCI, *Corso di diritto penale*, cit., p. 28. Sul bene giuridico si rinvia a G. FIANDACA-E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2009, p. 9 ss.; F. MANTOVANI, *Diritto penale. Parte generale*, Padova, 2007, p. 190 ss.; F.C. PALAZZO, *I confini della tutela penale*, cit., p. 454 osserva che la nozione di bene giuridico "*rimane generalmente accreditata per il suo ruolo liberale e garantista di strumento critico di contenimento del magistero punitivo*".

[44] Appare riduttivo limitare il profilo offensivo ai beni giuridici tradizionali, come il patrimonio, la fede pubblica, ecc. in quanto nessuno di essi, se isolatamente considerati, esaurisce la dimensione materiale delle of-

mentale che il presunto "mezzo" appartiene, invece, alla specificità dell'offesa.

In secondo luogo, benché non si reputi necessario che tutti i reati informatici debbano essere ricompresi e disciplinati all'interno del sistema codicistico, occorre comunque osservare che, anche volendo accogliere la proposta di un sottosistema, quest'ultimo, affinché abbia una ragione d'essere unitaria, deve essere ricostruito su un bene giuridico di categoria.

L'identificazione del bene, pertanto, è necessaria per conferire sistematicità al diritto penale dell'informatica, perché costituisce lo strumento concettuale indispensabile non tanto per la classificazione dei reati, quanto soprattutto "*per la loro analisi ermeneutica e la successiva valutazione critica*"[45]. Una volta acquisita la rilevanza di un bene giuridico unitario, costantemente offeso, non vi sono ostacoli per la ricostruzione come fattispecie plurioffensive della fattispecie tradizionali ampliate del diritto penale comune, ad esempio il furto o il danneggiamento informatici, come reati plurioffensivi, poiché in esse è percepibile anche l'offesa contro il patrimonio.

La validità di questa ricostruzione non è inficiata dalla Convenzione *Cybercrime*[46], recentemente ratificata dall'Italia, che distingue tra i reati a tutela del bene informatico "in senso stretto o proprio" dai reati "relativi ai contenuti" e quindi o "in senso ampio o improprio"[47] e trova conferma anche nell'art. 83 del Trattato di Lisbona sul funzionamento dell'Unione Eu-

fese realizzate dalla maggioranza degli illeciti informatici. Ad es., nella truffa informatica *ex* art. 640-*ter* c.p. sono stati eliminati i requisiti della truffa, cioè gli artifici o raggiri e l'induzione in errore, sia perché costituivano l'ostacolo all'applicazione dell'art. 640 c.p., sia perché non sono ipotizzabili nel sistema della computerizzazione delle operazioni economiche, operanti su macchine prive delle caratteristiche dell'essere umano (si veda F. MANTOVANI, *Diritto penale. Delitti contro il patrimonio*, II, Padova, 2002, p. 209, il quale non condivide l'opinione di coloro i quali ritengono che la frode informatica sia ispirata allo schema della truffa, poiché il passaggio di ricchezze da un patrimonio all'altro senza il tramite di un atto di disposizione, cosciente e volontario (pur se viziato dall'inganno), priva la fattispecie della natura di reato con la cooperazione artificiosa della vittima e la avvicina alla categoria del furto con mezzi fraudolenti). L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 55 ss., il quale osserva che il bene protetto non può essere identificato, accanto al patrimonio, "*nella sfera di libera formazione ed autodeterminazione dell'effettiva volontà del soggetto passivo, normativamente sancita dal rilievo tipico dell'errore (psicologicamente inteso) in cui egli deve cadere, ai sensi della fattispecie comune di truffa tipizzata dall'art. 640 c.p.*", ma nella garanzia "*di una corretta e fedele attivazione nonché esecuzione delle procedure programmate, contro il rischio di interventi non solo manipolatori in senso stretto, ma anche meramente abusivi*".

[45] Sulla funzione del bene giuridico nel diritto penale dell'informatica cfr. L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 24.

[46] Legge 18 marzo 2008, n. 48, contenente la ratifica e l'esecuzione della Convenzione del Consiglio di Europa sulla criminalità informatica (approvata a Budapest il 23 novembre 2001) e le norme di adeguamento dell'ordinamento interno, pubblicata nella *G.U.* 4 aprile 2008, n. 80, suppl. ord. n. 79. Per una dettagliata analisi della legge n. 48 del 2008 e degli effetti prodotti sull'ordinamento giuridico interno dalla sua introduzione si rinvia a: L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2008, 6, p. 700 ss., il quale riscontra l'inserimento o la modifica di fattispecie penali che non sembrano esecutive della Convenzione, ma piuttosto rispondenti ad autonome scelte del legislatore nazionale, il quale sembra aver colto l'occasione della legge 48/2008 per disciplinare alcune parti controverse della disciplina già vigente in materia; Id., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'internet*, 2008, 5, p. 437 ss.; F. RESTA, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura*, in *Giur. merito*, 2008, 9, p. 2147 ss.; C. SARZANA DI SANT'IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc.*, 2008, 12, p. 1562 ss.

[47] In merito L. PICOTTI, *Internet e diritto penale*, cit., p. 197, precisa che la Convenzione *Cybercrime* distingue al suo interno tra "reati cibernetici in senso stretto o proprio", dalla stessa definiti ai Titolo I e II, della Sezione I, del Capitolo II, in cui il sistema informatico è il bene giuridico tutelato, e "reati cibernetici relativi ai contenuti o in senso improprio" (Titolo III, della Sezione I, del Capitolo II), potenzialmente comprensivi di qualsiasi fattispecie criminosa, anche non realizzata nel *cyberspace*, ovvero gli illeciti commessi mediante un sistema informatico o qualsiasi altro reato di cui si debbano o possano raccogliere prove in forma elettronica (art. 14, comma 2 e art. 23 della Convenzione *Cybercrime*).

ropea, che disciplina le attuali competenze penali indirette dell'Unione[48]. Nel primo paragrafo dell'art. 83, infatti, ove la competenza viene stabilita *ratione materiae*, sono indicate nominalmente nove materie[49], tra le quali figura anche la criminalità informatica, il che costituisce un indice dell'importanza sopranazionale del fenomeno e sottolinea l'opportunità della sua valutazione globale da parte dei legislatori nazionali[50].

[48] Antecedentemente all'entrata in vigore del trattato di Lisbona l'Unione Europea disponeva solo di una competenza indiretta in materia penale, cioè di una competenza a richiedere agli Stati membri di emettere norme di tutela penale. Questa competenza, attraverso la quale l'Unione europea esprime una politica criminale europea, è di due tipi: nel primo è connessa alla necessità di realizzare lo spazio di libertà, sicurezza e giustizia mediante la cooperazione giudiziaria prevista nel terzo pilastro (in tale ipotesi l'Unione Europea non può prevedere norme incriminatrici direttamente applicabili e i fatti penalmente rilevanti devono essere necessariamente collegati ad esigenze di natura processuale); nel secondo la competenza è connessa alle esigenze di tutelare mediante pena gli interessi emergenti dalla legislazione comunitaria nell'ambito del primo pilastro (in merito occorre ricordare che, a seguito della sentenza del 13 settembre 2005 della Corte di Giustizia (C-176/03) l'Unione risulta competente a svolgere un giudizio di necessità di pena in quanto la Corte ha stabilito che il diritto comunitario, per le materie di sua competenza, può imporre anche obblighi di tutela penale, qualora necessario all'attuazione delle sue disposizioni normative, rimettendo in discussione l'assunto secondo il quale solo una norma di terzo pilastro può prevedere un obbligo di tutela penale). Successivamente il quadro normativo è mutato: l'Unione Europea, sebbene non possa ancora esercitare una propria potestà punitiva, può attualmente svolgere un giudizio di "necessità di pena", connessa al raggiungimento di uno spazio di libertà, sicurezza e giustizia, non essendo più subordinata alla sussistenza delle esigenze di cooperazione processuale. Al riguardo si rinvia a C. SOTIS, *Il diritto senza codice. Uno studio sul sistema penale europeo vigente*, Milano, 2007, 162; Id., *Le novità in tema di diritto penale europeo*, in *La nuova Europa dopo il Trattato di Lisbona*, a cura di P. BILANCIA-M. D'AMICO, Milano 2009, 139 ss.

[49] Si tratta del terrorismo, della tratta degli esseri umani e dello sfruttamento sessuale delle donne e dei minori, del traffico illecito di stupefacenti, del traffico illecito di armi, del riciclaggio di denaro, della corruzione, della contraffazione di mezzi di pagamento, della criminalità informatica e della criminalità organizzata (nel secondo paragrafo dell'art. 83 TFUE le competenze non sono, invece, individuate per specifici settori, ma sono connesse in generale al riavvicinamento delle disposizioni legislative e regolamentari). In riferimento alle predette materie il Parlamento europeo e il Consiglio, ai sensi del primo paragrafo dell'art. 83 TFUE, possono, deliberando mediante direttive secondo la procedura legislativa ordinaria, "*stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni*". In merito cfr. C. SOTIS, *Il trattato di Lisbona e le competenze penali dell'Unione Europea*, in *La magistratura*, 2009, 3-4, p. 27; ID., *Le novità in tema di diritto penale europeo*, cit., p. 147 ss. ha osservato che il riferimento alla "particolare gravità" sembra presupporre un intervento comunitario su settori che devono aver già registrato a livello nazionale una reazione di tipo penale. L'Autore evidenzia che dall'analisi testuale della disposizione emergerebbe, pertanto, che l'Unione non può operare una antecedente ed originaria valutazione dell'esigenza di irrogare la sanzione penale, ma è vincolata all'ambito della normativa penale già stabilita a livello statale, potendo imporre l'inflizione di una pena solo nei confronti di fatti già puniti dagli ordinamenti interni. Opererebbe, pertanto, solo una valutazione concernente la necessità di una lotta comune nei confronti di fatti già penalmente previsti dagli ordinamenti nazionali. Circa le osservazioni critiche sulle implicazioni scaturenti dal giudizio di "necessità" (o di "indispensabilità") l'autore rileva che se il legislatore comunitario avesse subordinato il predetto giudizio alla tutela del bene giuridico e non della norma, avrebbe non solo stabilito un criterio più garantista, perché idoneo a svolgere una valutazione della razionalità dei beni coinvolti, ma anche più efficace, perché maggiormente coerente con le altre norme previste in materia di libertà, sicurezza e giustizia.

[50] In merito S. AMORE-V. STANCA-S. STARO, *op. cit.*, p. 53 rilevano che nella Costituzione spagnola il bene informatico è menzionato esplicitamente: l'art. 18, quarto comma, della Costituzione spagnola dispone che "*La legge limita l'uso dell'informatica al fine di garantire l'onore e la riservatezza personale e familiare dei cittadini e il pieno esercizio dei loro diritti*"; l'art. 20 prevede che non solo sono protetti e riconosciuti i diritti ad esprimere e diffondere liberamente pensieri, idee e opinioni, attraverso la parola, lo scritto e qualsiasi altro mezzo di riproduzione ma anche "*a comunicare e a ricevere liberamente informazioni veritiere, attraverso qualsiasi mezzo di diffusione*"; l'art. 105 al secondo comma afferma che la legge regola "*L'accesso dei cittadini agli archivi e ai registri amministrativi, salve le informazioni che riguardino la sicurezza e la difesa dello Stato, le indagini sui delitti e il diritto alla riservatezza*". Si tratterebbe, pertanto, di un bene giuridico autonomo, che non è riconducibile al diritto alla riservatezza o alla *privacy*, ma si avvicina in qualche modo alla libertà ideologica.

CAPITOLO 11

Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*

di *Roberto E. Kostoris*

SOMMARIO: 1. Ricerca di dati informatici e tutela dei diritti fondamentali. – 2. Sequestro o intercettazione? – 3. Sequestro informatico per clonazione dei dati: un accertamento tecnico non ripetibile? – 4. Prova informatica ed eclissi dell'oralità. – 5. Alla ricerca abusiva di *notitiae criminis*?

1. Ricerca di dati informatici e tutela dei diritti fondamentali

Finora abbiamo ascoltato le riflessioni dei sostanzialisti, ma non bisogna dimenticare che numerosi e delicatissimi sono i problemi che la rivoluzione informatica pone sul versante del processo.

Su questo terreno, le nostre categorie giuridiche tradizionali devono confrontarsi e interagire con gli strumenti inediti offerti dalle nuove tecnologie. E ciò investe a largo raggio gli istituti processuali e il sistema; ma prima ancora lo stesso modo di intendere alcuni diritti fondamentali, di cui va aggiornato e implementato il contenuto, se non addirittura l'inventario, a fronte delle nuove insidie che possono nascere dall'uso dei mezzi informatici.

Ad esempio, una perquisizione e un sequestro di dati elettronici non si limitano certo a incidere sulla mera tutela del "domicilio", come avviene per un normale provvedimento di cautela reale; specie quando avvengano *on line* essi intaccano soprattutto la sfera della riservatezza, e anche quell'esigenza di affidamento nell'uso di sistemi informatici in rete, che non è ancora riconosciuta nel nostro sistema, ma che, data l'importanza crescente che assumono le forme di comunicazione telematica nella vita di relazione, non potrà non essere prima o poi costruita alla stregua di una garanzia fondamentale, come avviene già in altri ordinamenti, magari facendola derivare proprio dal diritto alla riservatezza, o, come ha pionieristicamente affermato di recente la Corte costituzionale tedesca – lo ricordava ieri nella sua relazione il dott. Flor – dal più generale diritto alla dignità umana, inteso come diritto all'autodeterminazione (in questo caso informativa): un diritto che, beninteso, potrebbe essere comunque soggetto a compressioni, ma con l'osservanza di particolari garanzie (indicazione tassativa dei casi, rispetto rigoroso del principio di proporzionalità, provvedimento motivato di un giudice).

2. Sequestro o intercettazione?

Anche restando però ad un livello normativo sottordinato, i problemi, come si diceva, si

* Contributo che si inserisce nell'attività di ricerca svolta nell'ambito del Progetto di Ateneo *Criminalità informatica ed accertamento penale* (codice CPDA084200/08), finanziato dall'Università degli Studi di Padova.

affollano e non appaiono tutti adeguatamente risolti (né talora neppure affrontati) dalla legge di ratifica – giunta assai tardivamente – della Convenzione di Budapest (legge 18 marzo 2008, n. 48), dove, tra l'altro, perquisizioni e sequestri informatici sembrano disciplinati solo con riferimento ai luoghi dove si trovano i computer, e non quando avvengano da postazioni remote.

Sorvolo in questa sede, per la sua eccentricità rispetto ai temi di questa sessione, su una pur delicatissima problematica rappresentata dagli inediti problemi di "territorialità" che pongono le azioni criminose commesse attraverso strumenti telematici, le quali, sottraendosi alle ordinarie regole spaziali sotto il profilo del luogo del commesso reato, che può risultare in questi casi di assai difficile individuazione, presentano evidenti ricadute sul piano della competenza, e anche su quello della cooperazione internazionale.

Mi limito a pochi flash più direttamente legati al tema della ricerca e della formazione della prova elettronica.

Anzitutto ci si può chiedere se le forme investigative di apprensione di dati telematici si debbano rapportare alla disciplina delle perquisizioni o a quella, più garantistica, delle intercettazioni.

È indubbiamente assai difficile cercare di adattare i moduli tradizionali ai nuovi strumenti investigativi digitali. Basti pensare che l'intercettazione telefonica presuppone una comunicazione sincrona e in forma orale fra due persone, mentre la posta elettronica implica una comunicazione asincrona e in forma scritta. Qualcuno suggerisce di individuare la linea di discrimine nel fatto che il messaggio di posta elettronica sia già stato letto (diventando così un documento, come tale sequestrabile) o no (nel qual caso potrebbe essere più corretto ricorrere alla disciplina delle intercettazioni ai sensi dell'art. 266-*bis* c.p.p.). Ma non si può neppure dimenticare che l'art. 254, comma 1, c.p.p. come modificato dalla legge n. 48 del 2008, prevede espressamente la possibilità di sequestrare presso i fornitori di servizi telematici corrispondenza inoltrata per via telematica, che si deve supporre non ancora conosciuta dal destinatario, al pari degli altri oggetti di corrispondenza, come lettere, pieghi, pacchi, telegrammi di cui fa parola la disposizione. D'altro canto, quella corrispondenza telematica inoltrata e non ancora letta dal destinatario sembrerebbe integrare proprio quel "flusso di comunicazioni" in atto che rappresenta nell'art. 266-*bis* c.p.p. il presupposto per l'attività di intercettazione.

Ora, poiché sono in gioco in materia opzioni molto delicate da cui dipende l'applicazione di livelli ben diversificati di garanzia, è opportuno che il legislatore intervenga per chiarire meglio gli ambiti di applicazione delle due discipline.

3. Sequestro informatico per clonazione dei dati: un accertamento tecnico non ripetibile?

Un altro aspetto peculiare del dato informatico è costituito dal fatto che esso si può giovare di forti capacità mimetiche: come noto, il sequestro è ammesso solo rispetto al corpo del reato e alle cose ad esso pertinenti, ma le risorse dell'informatica possono rendere anche assai disagevole l'individuazione di questi elementi; è sufficiente che essi si trovino custoditi in un *file* occultato in un altro dall'apparenza innocua. E se fossero necessarie operazioni lunghe, complesse e delicate per identificarli, la praticabilità del sequestro potrebbe risultarne frustrata.

Ma, soprattutto, consideriamo l'anatomia del sequestro: esso dovrà portare alla clonazione del disco rigido o di quanto è contenuto su un supporto informatico, e ciò pone di fronte a delicati problemi, sia di tipo strettamente tecnico (ad esempio, a computer acceso sarà possi-

bile ottenere una serie di informazioni che andrebbero irrimediabilmente perse spegnendo la macchina), sia di tipo giuridico, legati al modo in cui la clonazione deve avvenire.

L'art. 247, comma 1-*bis*, c.p.p., inserito dalla legge di ratifica, prescrive che vadano adottate al riguardo le misure tecniche in grado di assicurare la conservazione dei dati originali e di impedirne l'alterazione.

Pur non fornendo indicazioni sulle metodiche da seguire, il legislatore in tal modo, per un verso, sembra riconoscere implicitamente il carattere intrinsecamente modificabile della prova digitale, e, per altro verso, sembra assimilare la clonazione ad un prelievo di campioni da sottoporre ad analisi; in sostanza, ad un vero e proprio accertamento tecnico, di cui andrebbe verificata la ripetibilità o la non ripetibilità.

A tal fine, occorrerebbe capire se l'operazione apprensiva sarebbe di per sé suscettibile di determinare una modifica dei dati. La risposta – a detta dei tecnici – sembrerebbe essere affermativa, almeno nel caso in cui si intervenga a computer acceso.

Ciò dovrebbe allora orientare anzitutto ad individuare e adottare metodiche standardizzate e affidabili di captazione che garantiscano la massima genuinità possibile del prodotto, onde evitare che i dati – che sembrerebbe corretto ritenere formalmente utilizzabili anche in assenza di simili accorgimenti (almeno finché il legislatore non prescriva espressamente l'obbligo di adottarli) – risultino però inaffidabili sotto il profilo probatorio. Un obiettivo importante da realizzare anche nella prospettiva di rendere quei dati fruibili pure ai fini della cooperazione giudiziaria. Certo potrebbe essere difficile cristallizzare in veri e propri precetti normativi le *best practice*, per la difficoltà di adeguare la lentezza dei tempi legislativi alla rapidità dell'evoluzione tecnologica. Ma potrebbe essere almeno opportuno che gli Stati dell'Unione europea facciano riferimento a protocolli uniformi fissati da un'autorità centrale e costantemente aggiornati.

Per altro verso, la non ripetibilità dell'accertamento dovrebbe richiedere adeguate forme di tutela difensiva, che però siano pur sempre compatibili con il tipo di operazione che si sta svolgendo, e cioè tali da non pregiudicarne la necessaria natura di atto a sorpresa. Un obiettivo che il preventivo avviso all'indagato contemplato dall'art. 360 c.p.p. non sembrerebbe certo in grado di assicurare.

4. Prova informatica ed eclissi dell'oralità

Peraltro, occorre aggiungere che quest'intrinseca volatilità della prova informatica si trova paradossalmente a convivere con una sorta di aura di infallibilità che sembra invece circondarla nell'immaginario collettivo.

Non si tratta di una semplice osservazione di carattere sociologico. L'uso dell'informatica nell'indagine penale potrebbe trasformare quasi impercettibilmente, ma profondamente, il quadro generale di contesto. I dati telematici – insieme a quelli forniti dalle intercettazioni telefoniche tradizionali – potrebbero finire per relegare in ambiti sempre più ristretti la prova orale.

In questa prospettiva, il contraddittorio nella formazione della prova consacrato dall'art. 111, comma 4, Cost. sarebbe sempre più destinato a cedere il passo alle documentazioni telematiche; esso resterebbe confinato soprattutto all'ambito tecnico, per verificare la genuinità del prodotto; mentre la credibilità, l'affidabilità del contenuto dichiarativo che vi è inglobato potrebbero finire per essere considerate implicite nell'esistenza stessa del messaggio, sottraendolo così a quel prezioso controllo di tutti i c.d. "tratti prosodici" che nella prova orale si accompagnano alla sua trasmissione.

5. Alla ricerca abusiva di *notitiae criminis*?

Non si possono infine chiudere questi brevissime considerazioni senza segnalare un timore, ben presente in chi conosce questi temi e della cui importanza si è recentemente fatta interprete anche una delle Risoluzioni del XVIII Congresso internazionale dell'*Association International de Droit Pénal* tenutosi a Istanbul nel settembre 2009.

Si sa che l'attività investigativa di perquisizione e di sequestro presuppone l'esistenza di un reato, del quale, come prima si ricordava, si devono ricercare le cose pertinenti. Ma i dati telematici raccolti contengono anche un'infinità di informazioni ulteriori ed estranee alla regiudicanda.

Vi è allora il rischio che sfruttando quella messe enorme di dati, gli organi inquirenti possano arbitrariamente muovere alla ricerca di nuove notizie di reato, utilizzando in modo surrettizio a tal fine gli strumenti della perquisizione e del sequestro. Ancor più che nelle intercettazioni telefoniche, nella perquisizione in rete si dilatano da questo punto di vista i rischi di arbitri da parte degli organi investigativi.

CAPITOLO 12

Le perquisizioni e i sequestri informatici

di *Diego Buso* e *Daniele Pistolesi*

SOMMARIO: 1. Premessa. – 2. *Computer forensic* e legge n. 48 del 2008. – 3. Cosa ricercare nella perquisizione informatica. – 4. Sequestro nei reati informatici. – 5. La perquisizione informatica. – 6. L'analisi del materiale informatico. – 7. *Live Data Forensics.*

1. Premessa

Dalla delibera AIPA di metà anni '90 [1] che definiva evidenza informatica «un messaggio elettronico, composto da dati utente e da codici universali, che viene validamente impiegato a fini probatori, amministrativi e contabili» ad oggi, molta strada si è fatta nell'ambito della ***computer forensic*** e, per ciò che ne attiene, della ***digital evidence***.

Siamo di fronte ad un percorso che nel corso degli anni ci ha sempre di più avvicinato a modelli operativi d'ispirazione anglosassone. In Inghilterra e soprattutto negli Stati Uniti, da tempo si è andata sviluppando una particolare attenzione verso la *computer evidence* o *digital evidence*, intesa quale prova o elemento di prova riscontrato all'interno di un computer e/o di un qualsivoglia supporto informatico in grado di contenere dati per documentare la perpetrazione di un crimine, soprattutto un crimine informatico, e consentire l'individuazione del responsabile.

2. *Computer forensic* e legge n. 48 del 2008

Nel linguaggio comune l'evidenza informatica o *digital evidence* costituisce la prova o quel complesso d'indizi (tracce) che permettono la ricostruzione di un fatto accaduto nel passato, commesso per mezzo o a danno di un sistema informatico.

Al pari di quella tradizionale, la prova digitale può costituire dimostrazione di reità o d'innocenza di un soggetto ed essere posta a fondamento della decisione finale del giudice [2].

[1] Delibera AIPA del 9 novembre 1995 recante la "*Definizione delle regole tecniche per il mandato informatico*" pubblicata nella *G.U.* 22 novembre 1995, n. 273.

[2] Poniamo il caso di una conversazione telematica in tempo reale tra due utenti (*chat line*), i quali dopo essersi conosciuti in Rete scoprono di avere un interesse in comune per il collezionismo e decidono di scambiarsi non solo informazioni ma anche immagini per approfondire la reciproca conoscenza. Se i soggetti sono collezionisti di foto e filmati aventi per oggetto immagini pornografiche di minori, lo scambio di *file* illeciti integra fattispecie penalmente sanzionate nel nostro ordinamento. Questo comportamento illegale può avvenire in realtà non solo tramite servizi di comunicazione in tempo reale (*chat line*), ma anche per mezzo della posta elettronica, di un programma di condivisione *file* e in molti altri modi che potenzialmente lasciano nei sistemi e nei supporti informatici utilizzati almeno una traccia. Nel caso di specie gli inquirenti dovranno acquisire al processo le prove dell'avvenuta conversazione, dimostrare i contenuti della *chat*, lo scambio di foto e il loro contenuto *contra legem* e naturalmente identificare gli utenti in modo inequivoco. All'opposto, la difesa opererà per dimostrare

La *computer forensic* si propone di studiare quali siano gli elementi probatori utili al processo penale, di elaborare le tecniche per la ricerca e l'individuazione e per l'acquisizione di tali prove e i limiti da osservare nel porre in essere tali attività.

Lo sviluppo di tali tecniche e le discussioni fra gli addetti ai lavori contribuiscono a delineare uno *standard operativo* che possa essere di riferimento a tutte le parti coinvolte nel procedimento tendente all'accertamento della verità processuale.

A differenza di quanto accade nel crimine tradizionale, la prova digitale ha un ambito ben delimitato entro il quale essere ricercata. Chi deve scoprire tracce di attività informatiche c*ontra legem,* deve concentrare la propria attenzione sugli elaboratori elettronici utilizzati per porre in essere il crimine, sui sistemi informatici contro i quali il crimine è stato commesso ovvero verso quegli elaboratori, se diversi, che potrebbero contenere le registrazioni (*logfiles*) di tali attività.

Invero l'attenzione sarà indirizzata verso il personal computer nel suo complesso, principalmente sulle componenti *hardware* e *software* di esso, sui supporti digitali e magneto-ottici [3] idonei a contenere informazioni digitali ovvero altri dispositivi-depositi che custodiscono dati utili alla ricostruzione del fatto storico, anche con rimando a unità esterne, magari sedenti in spazi virtuali all'interno della rete Internet.

Un compito, quello della ricerca, molto delicato il quale deve esser assicurato avendo cura di non modificare lo *status* delle componenti che si devono analizzare e soprattutto avendo le conoscenze tecniche adeguate per "trovare" le tracce del delitto anche in quegli spazi nei quali un occhio inesperto potrebbe non vedere nulla.

La condivisione e lo scambio di esperienze in ambito nazionale e transnazionale, le discussioni che nel corso dell'ultimo decennio hanno caratterizzato le aule processuali hanno portato all'individuazione di standard operativi unitari atti a salvaguardare le informazioni "elettroniche" essenziali per il prosieguo dell'attività giudiziaria.

Le innovazioni normative al codice di rito, nel delicato settore dell'acquisizione delle fonti di prova, introdotte con la legge n. 48 del 2008 nella fase delle indagini preliminari, in parte figlie delle predette esperienze e discussioni, impongono alla polizia giudiziaria italiana, sotto il profilo delle tecniche operative, di accettare nuove sfide e di attrezzarsi per apprendere il funzionamento di un sistema informatico, avendo chiaro quali possono essere i rischi, sia in tema di alterazione del dato che di perdita definitiva dello stesso, che un'incauta ricerca può arrecare alle indagini.

I provvedimenti d'ispezione, di perquisizione e di sequestro informatico delegati dall'autorità giudiziaria ovvero le attività d'iniziativa della medesima natura poste in essere dalla polizia giudiziaria, spesso indispensabili per l'acquisizione della fonte di prova, presuppongono comunque una invasività nelle reti e nei sistemi informatici ed un rischio potenziale per la corretta raccolta del dato digitale che devono essere mitigati da prassi operative consolidate e formazione professionale adeguata.

l'innocenza del proprio assistito anche semplicemente generando il ragionevole dubbio che l'autore possa essere una persona diversa.

[3] Così vengono definiti tutti quei contenitori di informazioni che abbiano una qualche attinenza con il computer. L'elenco potrebbe essere molto lungo: oltre ai noti *hard disk, floppy-disk, cd-rom* potremmo brevemente aggiungere quelli più utilizzati quali *usb-stick*, *dvd-rom*, *blue-ray* e altri capaci di contenere mole di dati assai elevate 8 fino a 25 Gb).

3. Cosa ricercare nella perquisizione informatica

La prassi ormai induce gli operatori ad effettuare un'accurata valutazione del materiale oggetto di perquisizione e di quello da sottoporre a conseguente sequestro. È chiaro che ogni *media* e ogni appunto potrebbero agevolare l'attività degli investigatori. È altresì vero che un'eccessiva mole di dati e d'informazioni non organizzate e depurate equivale a non avere elementi su cui lavorare. L'attenzione va posta quindi verso i supporti che si assumono in uso al soggetto perquisito, a quelli nella sua prossimità (si pensi ad *hard disk* esterni, *storage usb* di vecchia e nuova generazione, dispositivi di *backup*) e nel caso di reati di particolare gravità protrattisi per un lungo periodo, anche a tutti quei supporti all'apparenza "archiviati" per obsolescenza.

Non si dimentichi che dispositivi quali lettori multimediali portatili, macchine fotocopiatrici, telefoni di ultima generazione, navigatori satellitari, *memory card* normalmente usate per memorizzare fotografie digitali, possono contenere utili elementi probatori assolutamente funzionali all'obiettivo investigativo.

L'analisi dei contenuti effettuata dagli esperti informatici tenderà all'individuazione di tutte le tracce utili per ricostruire il profilo dell'imputato e il percorso criminoso e per accertare la penale responsabilità ovvero la parziale o assoluta estraneità ai fatti del soggetto perquisito.

L'attenzione sarà rivolta pertanto a fogli elettronici, documenti, *data base*, immagini e filmati presenti nei supporti. Di chiara rilevanza possono essere i *file* relativi alla navigazione *web* (*cookies*,cronologia, indirizzi IP) ed alla posta elettronica, agli eventi (c.d. *file di log*) e a tutti i *file* inerenti il registro del sistema operativo.

Uno studio tecnicamente più approfondito può consentire il recupero dei file cancellati, delle informazioni nascoste in altri *file* (c.d. steganografia), e la lettura di "spezzoni" dei *file* eliminati ma in parte ancora giacenti nelle zone di memoria non utilizzate dei supporti in esame.

4. Sequestro nei reati informatici

La disciplina del sequestro del corpo del reato e delle cose pertinenti al reato, quando si operi per l'accertamento di reati informatici o di reati comuni commessi utilizzando lo strumento informatico e/o telematico, sia che esso venga eseguito su disposizione dell'Autorità Giudiziaria sia che esso venga effettuato a seguito dell'iniziativa dalla polizia giudiziaria, è stata novellata e integrata dalla legge n. 48 del 2008 che ha posto particolare enfasi sulla necessità di conservare correttamente i sistemi informatici e telematici oggetto dell'attività, al fine di impedire la loro alterazione nonché quella dei dati, delle informazioni e dei *software* in essi contenuti [4].

È stata altresì introdotta una norma *ad hoc* per il sequestro di dati informatici e telematici presso i fornitori di servizio [5] la cui reale portata applicativa deve essere valutata anche alla luce dell'istituto del dovere d'esibizione che grava sugli stessi soggetti per effetto dell'art. 256 c.p.p., comma 1, anch'esso modificato nella stessa ottica dal legislatore del 2008.

Altra innovazione significativa, riguarda l'esplicito riferimento al sequestro di corrispondenza telematica [6] diretta all'indagato o comunque ad esso spedita che può essere disposto con

[4] Cfr. art. 354, comma 2, c.p.p.

[5] V. art. 254-*bis* c.p.p.

[6] Cfr. artt. 254 e 353 c.p.p.

provvedimento dell'Autorità Giudiziaria o, ricorrendone i presupposti, essere eseguito dalla polizia giudiziaria d'iniziativa. L'accesso alla casella di posta elettronica operato presso il *provider* fornitore del servizio non offre particolari problemi interpretativi nel caso di messaggi di posta elettronica già pervenuti, mentre postula il ricorso all'istituto dell'intercettazione e alla relativa disciplina nel caso in cui i messaggi vengano acquisiti e duplicati al momento del loro arrivo presso il server di posta.

Bisogna infine ricordare come nelle fattispecie più gravi di delitto introdotte dalla legge n. 269 del 1998 concernenti la prostituzione minorile, le iniziative turistiche volte al c.d. turismo sessuale e la pornografia minorile, il legislatore abbia da tempo previsto per gli inquirenti la possibilità di fare ricorso al differimento dell'esecuzione di provvedimenti doverosi di cattura, arresto o sequestro [7].

In particolare, laddove l'attività di contrasto ai predetti fenomeni si concentri in ambito telematico, può essere disposto con decreto motivato dell'Autorità Giudiziaria, il differimento del sequestro del corpo del reato che può consistere in un supporto informatico o magari in uno spazio virtuale [8]. Il ricorso a tale strumento è consentito solo quando appaia correlato alla necessità di acquisire rilevanti elementi probatori o per identificare e catturare i responsabili dei gravi delitti sopra menzionati.

Come è facilmente intuibile, il ricorso a tali strumenti di contrasto, nei limiti stabiliti dalla norma, riveste una notevole importanza strategica consentendo agli investigatori di differire atti altrimenti dovuti, la cui immediata esecuzione potrebbe nuocere alla proficua prosecuzione delle attività di indagine. Il differimento di tali attività consente di raccogliere elementi indispensabili per la corretta ricostruzione di un completo quadro probatorio, evitando di palesare prematuramente l'esistenza di un'attività investigativa *in itinere.*

5. La perquisizione informatica

Le attività d'individuazione delle cose e del dato digitale in esse contenuto e quella conseguente di sequestro di detti beni, devono essere effettuate in modo da garantire innanzitutto che i supporti da analizzare e quanto in essi contenuto non vengano alterati.

La prima delle raccomandazioni rivolte alle forze di polizia impegnate in tali attività è stata da sempre quella di evitare di accedere al sistema informatico e ai supporti di memorizzazione nel luogo stesso del sequestro, a meno che ciò non sia strettamente necessario per la prosecuzione delle indagini, non si disponga di strumenti e apparecchiature tecniche adatte e non si abbiano le conoscenze indispensabili per l'effettuazione della ricerca in condizioni di sicurezza.

Nel caso si decida di operare secondo tale modalità, particolare attenzione deve essere prestata durante la raccolta del materiale che deve essere sottoposto a sequestro.

[7] Cfr. art. 14, comma 3, legge n. 269 del 1998 recante "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*".

[8] Può essere il caso del centro assistenza che riceve da un cliente un personal computer con un *Hard Disk* contenente materiale pedopornografico ovvero quello di una segnalazione da parte dei colleghi di un soggetto che detiene nel computer d'ufficio materiale *contra legem*. In entrambi i casi il differimento del sequestro andrebbe accompagnato con la duplicazione del dispositivo *in loco*, la restituzione del *media* originale e la predisposizione di ulteriori attività di indagine. Pensiamo infine al caso in cui una persona gestisca da remoto uno spazio web con contenuti illeciti presso un provider sedente in Italia. In tale occasione bisognerà procedere con la duplicazione dello spazio virtuale, il monitoraggio dello stesso per il tempo necessario all'identificazione del responsabile e degli altri soggetti eventualmente coinvolti nella turpe attività.

Dopo l'individuazione del materiale è necessario procedere alla sua elencazione e repertazione. Per la corretta conservazione è consigliabile utilizzare imballi realizzati con materiali atti a contenere apparecchiature e supporti informatici, sì da preservarli da alterazioni causate da agenti esterni (onde elettromagnetiche, calore, ecc.) che potrebbero avere effetti deleteri sul contenuto.

Nel caso la polizia giudiziaria sia attrezzata per compiere la perquisizione informatica, sia sotto il profilo delle conoscenze tecniche necessarie, sia sotto quello della disponibilità della strumentazione *hardware* e *software* adeguata, le metodologie di approccio variano a seconda che il sistema informatico da perquisire sia spento ovvero sia acceso.

Nel caso di computer spento, l'accesso al sistema informatico e ai supporti in esso contenuti viene in genere realizzato utilizzando dei blocchi *hardware* che consentono l'accesso ai dati in sola lettura con conseguente inibizione di ogni altra attività. Le possibilità di ricerca e i tempi necessari per perfezionarla variano in ragione del sistema operativo utilizzato dall'indagato, di ciò che deve essere ricercato all'interno del supporto (programmi, *file* multimediali, *logfile*, *file* testuali, dati di navigazione, ecc.), della capacità del supporto/i in cui la ricerca deve essere eseguita (è sempre più frequente durante le perquisizioni imbattersi in supporti di memorizzazione superiori ai 500 *gigabyte*), del fatto che ciò che si ricerca possa essere stato in precedenza cancellato ovvero che si ipotizzino attività anteriori di formattazione.

Nel caso di computer acceso, la prassi normalmente consigliata agli operatori sprovvisti di adeguata preparazione, per evitare manovre con effetti indesiderati, era quella di procedere allo spegnimento del personal computer mediante disconnessione dello stesso dalla rete elettrica.

Per gli operatori specializzati e attrezzati, si consiglia di procedere chiudendo tutti i processi attivi fino allo spegnimento completo del sistema, documentando nel relativo verbale le operazioni compiute e dando atto di tutte le informazioni reperite nel corso di tale attività.

Una volta messo in sicurezza il sistema informatico e i supporti su cui focalizzare l'attenzione, l'accesso agli stessi potrà essere effettuato nelle stesse modalità sopra descritte per il sistema spento.

La ricerca di evidenze probatorie perfezionata nel corso dell'esecuzione di una perquisizione informatica è di gran lunga più difficile e necessariamente meno accurata di quella posta in essere attraverso una attività di analisi delegata del materiale informatico sottoposto a sequestro.

È quindi possibile che l'attività di ricerca effettuata nel corso della perquisizione informatica non porti risultati significativi. Ciò potrebbe creare l'aspettativa nel soggetto sottoposto alle indagini e nel difensore che il materiale informatico sottoposto a perquisizione non venga sequestrato.

L'investigatore ha invece la necessità di valutare fino a quale livello di accuratezza la ricerca delle evidenze digitali è stata portata. Se ragioni di tempo, obiettive difficoltà di carattere tecnico, volume dei supporti da analizzare suggeriscono un possibile diverso esito di una completa attività di analisi, gli investigatori dovranno procedere egualmente al sequestro del materiale già sottoposto a perquisizione con esito negativo, dandone adeguata motivazione nel verbale di sequestro.

6. L'analisi del materiale informatico

Una volta eseguito il sequestro secondo le modalità previste dal codice di rito novellato nel 2008, gli esperti informatici procederanno all'acquisizione e alla successiva analisi dei dati presenti nei supporti sequestrati.

La metodologia attualmente utilizzata per l'attività di analisi si sviluppa attraverso alcuni passaggi fondamentali condivisi dagli addetti ai lavori, sia a livello nazionale che internazionale.

Il primo passo consiste nella creazione di una copia integrale del contenuto del supporto oggetto d'indagine, tramite elaboratori dotati di specifico *hardware e software* certificato, allo scopo di garantire la non alterazione dell'originale e la fedeltà della copia. Per copia integrale deve intendersi una copia fisica (dal primo all'ultimo *bit*) del supporto stesso, comprendente quindi anche le parti del *media* informatico che al momento del sequestro, non sono state adoperate dal sistema operativo.

È indispensabile che il sistema usato per creare la copia assicuri anche un'operazione di *hashing*, cioè generi per mezzo di un algoritmo certificato una stringa alfanumerica di un determinato numero di caratteri, la quale rappresenti il contenuto del supporto stesso. Una sorta di sigillo di controllo o di firma digitale univoca. In tal modo, ripetendo le predette operazioni di copia del supporto originale, sarà sempre possibile verificare che il contenuto del supporto non sia stato modificato, poiché anche la sola variazione di un *bit*, produrrebbe una stringa differente.

Il secondo passo è quello di mettere in sicurezza il supporto originale e di procedere all'archiviazione della copia ottenuta su supporti non alterabili (ad es. *cd-rom o dvd-rom* non riscrivibili [9] dopo la masterizzazione). Questo permette un duplice momento di sicurezza, poiché consente la ripetizione di qualsiasi attività si volesse effettuare sull'originale e la disponibilità di una copia fisica del supporto per eventuali richieste delle parti.

Il terzo passaggio prevede che l'analisi del contenuto dei supporti sia svolta lavorando sulla copia fisica, attraverso l'utilizzo di applicativi (in genere integrati nel *software* utilizzato per la copia), che permettano di scandagliare tutte le parti del supporto stesso.

Tali procedure garantiscono concretamente la possibilità di ripetere le operazioni descritte e rendono quindi le attività stesse atti ripetibili.

È per tale ragione che nel corso degli anni la magistratura inquirente ha spesso delegato le attività di accertamento tecnico sui supporti informatici assicurati al procedimento con il sequestro, direttamente a quelle strutture della polizia giudiziaria dotate di adeguate competenze tecniche e delle necessarie strumentazioni, senza ricorrere agli istituti previsti dagli artt. 359 e 360 c.p.p.

Nel caso di attività di consulenza o di attività peritali, essendo oramai pressoché universalmente accettate le prassi operative sopra descritte, l'importanza della presenza di rappresentanti delle parti interessate, quali il difensore, il perito e i consulenti tecnici è in genere limitata al momento dello svolgimento delle operazioni di copia dei supporti da analizzare, unica attività di cui si tende a disquisire circa la ripetibilità.

7. *Live Data Forensics*

Tra gli aspetti sempre più frequentemente discussi in consessi internazionali di taglio tecnico-giuridico, in tema di *Computer forensic* vi sono le modalità di attuazione ed i principi di tutela coinvolti nelle operazioni del c.d. ***Live Data Forensics***.

Questa particolare branca del *Forensic*, chiaramente destinata ai computer accesi (*live*) al momento dell'esecuzione di un'ispezione o di una perquisizione delegata dall'Autorità Giudi-

[9] Questo termine gergale vuole significare l'impossibilità di inserire, modificare o eliminare ulteriori dati oltre a quelli già introdotti e fissati con la prima operazione di scrittura.

ziaria o eseguita d'iniziativa, sembra contraddire i tradizionali principi di svolgimento delle attività tecniche di carattere informatico in precedenza sommariamente indicati.

Infatti l'utilizzo di tali tecniche apporta inevitabilmente modifiche nel sistema informatico in uso, in quanto viene effettuato un accesso direttamente sul supporto originale, in apparenza in disaccordo con alcuni dei principi di diritto del nostro ordinamento, ponendo in essere un'attività evidentemente non ripetibile, con le sole garanzie previste per i c.d. *atti a sorpresa*.

Ma allora quali sono gli effettivi vantaggi di tali operazioni e perché si procede in tal guisa? Ebbene tali procedure sono mirate all'acquisizione e all'analisi dei cosiddetti *dati volatili*, sempre più importanti nell'ambito delle indagini prettamente informatiche. L'evoluzione tecnologica che favorisce la disponibilità di computer sempre più potenti con maggiori capacità di *storage* e l'esigenza di acquisire elementi di prova di tipo informatico, rilevabili unicamente al momento di perquisizioni o ispezioni, fanno di tali tecniche forensi uno strumento di indagine irrinunciabile.

Dati importanti quali c*ache* di sistema, cronologia, pagine *web*, *file* temporanei, *database* in uso, mail in bozza e dialoghi di *chat*, dati contenuti nella memoria RAM [10] (attualmente tale memoria può arrivare ad una capacità di 8 Gb con ampio spazio per testo, immagini, password, chiavi di cifratura), supporti decriptati solo perché connessi con il computer da perquisire, sistemi di immagazzinamento virtualizzati o come sempre più spesso accade, remotizzati nel *web*, potrebbero essere persi definitivamente, laddove non rilevati attraverso il ricorso alle tecniche di *live forensics.*

La realtà operativa sta quindi portando a una rapida definizione di nuove regole procedurali per garantire l'acquisizione di tali elementi di prova, secondo un modus operandi garantito e legalmente riconosciuto da sottoporre peraltro, di volta in volta, al necessario vaglio dibattimentale.

Non vi è dubbio che il buon esito di tali complesse attività si basa sulla professionalità e sulla comprovata esperienza degli operatori di polizia giudiziaria di profilo tecnico informatico, sulla loro capacità di ponderare con obiettività se procedere a un'attività di *Live Data Forensics*, valutando volta per volta, necessariamente d'intesa con l'Autorità Giudiziaria titolare del procedimento, i benefici che da questa ne potrebbero scaturire e i rischi di alterazioni che l'accesso al supporto *live* comporta.

Parimenti importante si dimostrerà la scelta delle tecniche "intrusive" da adottare e dell'*hardware* e *software* da usare per il caso di specie.

Nel caso di ricorso a tali tecniche, è imprescindibile documentare integralmente con istantanee e idonee registrazioni audio/video l'attività eseguita, sì da fugare ogni eventuale dubbio che potrebbe inficiare l'intera procedura di acquisizione forense assolutamente non ripetibile.

Tali operazioni, assai dispendiose sotto il profilo delle risorse umane e tecnologiche da investire, postulano la presenza nel corso dell'attività di un coordinatore, figura di riferimento che sappia fugare con autorevolezza perplessità che, laddove non risolte nell'immediatezza, possono pregiudicare la raccolta di utili ed importanti elementi di prova residenti nel computer, ma non recuperabili in un momento successivo.

[10] *Random Access Memory*: particolare memoria presente in tutti i computer utilizzata dal processore per depositare temporaneamente informazioni di uso frequente al fine di ridurre i tempi di accesso ad esse. Caratteristica comune a tutti i tipi di RAM utilizzati per la memoria principale è quella di perdere il proprio contenuto nel momento in cui viene a mancare l'alimentazione elettrica.

CAPITOLO 13

Le cosiddette perquisizioni *on line* (o perquisizioni elettroniche)*

di *Stefano Marcolini*

1. Le perquisizioni *on line:* descrizione del fenomeno

Gli scopi del presente scritto sono due: dare una sommaria descrizione di quella che ben può definirsi una nuova modalità di investigazione all'interno del procedimento penale; così inquadrato il fenomeno sotto il punto di vista tecnico, cercare quindi di individuare, se esiste, quale sia il suo trattamento giuridico.

Le c.d. perquisizioni *on line* (od elettroniche) rappresentano un mezzo di indagine relativamente recente, che al momento non è stato oggetto di particolari riflessioni nel panorama dottrinario e giurisprudenziale italiano, ma che si è viceversa trovato al centro di un vivace dibattito nell'ordinamento tedesco, a seguito di un'importante sentenza del *Bundesverfassungsgericht* (Corte costituzionale federale) del febbraio del 2008 sulla c.d. *Online Durchsuchung* [1].

Dal punto di vista tecnico, le perquisizioni *on line* consentono di far copia, parziale o totale, delle unità di memoria del sistema informatico "attenzionato" (*on line search* o *one-time copy*); di rilevare e registrare nel tempo quali siti *web* vengono visitati attraverso quel sistema od attraverso i particolari *account* che si riferiscono a quel sistema (*on line surveillance*); al limite, di decifrare quel che viene digitato sulla tastiera collegata al sistema stesso [2]. L'intrusione è possibile in due modi: inserendo, nel sistema informatico da "osservare", un programma *ad hoc*, che sia in grado appunto di captare i dati sopra descritti e di trasmetterli, in tempo reale o ad intervalli prestabiliti agli organi dell'investigazione; leggendo tali dati duran-

* Testo dell'intervento al Congresso nazionale di beneficenza per gli studenti abruzzesi dal titolo *Internet e diritto – Il futuro dell'informatica giuridica e del diritto delle nuove tecnologie in Italia: prospettive* de iure condendo *e urgenza di una "ricostruzione normativa"*, tenutosi a Pescara il 19-20 giugno 2009, integrato alla luce delle non poche novità, normative e giurisprudenziali, successivamente intervenute.

[1] Per ogni aspetto della vicenda tedesca cfr. la traduzione, per stralci, della sentenza in *Riv. trim. dir. pen. ec.*, 2009, 679 ss., con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung, *ivi*, p. 695.

[2] Sulla diversa gamma di possibilità tecniche cfr. sempre R. FLOR, *op. cit.*, pp. 696-697.

te la loro trasmissione tramite uno *sniffer*[3], secondo un ampio ventaglio di possibilità tecniche, dipendenti dagli scopi dell'indagine e dalla sofisticatezza tecnica del "programma spia" che viene inserito nel sistema ospite o dello *sniffer*. Il tutto avviene, ovviamente, all'insaputa dell'utilizzatore del sistema, che *si presume* sia appunto l'indagato[4].

Sono evidenti le potenzialità di un simile strumento investigativo nell'accertamento di determinate tipologie di reati, in specie per quell'ampia serie di violazioni che la dottrina penalistica accomuna sotto il nome di "reati informatici"[5].

Non interessa qui indagare le eventuali, possibili conseguenze di diritto penale sostanziale a carico degli investigatori che compiano atti di perquisizione *on line*: conseguenze da articolare a seconda delle diverse strumentazioni e modalità tecniche impiegate e che ruotano, quantomeno, intorno alle fattispecie di accesso abusivo ad un sistema informatico o telematico qualora si inserisca un programma nel sistema (art. 615-*ter* c.p.), e di intercettazione di comunicazioni informatiche o telematiche nel caso di utilizzo di uno *sniffer* (art. 617-*quater* c.p.).

Preme invece sin da subito sottolineare che le perquisizioni elettroniche, come tutti gli atti a sorpresa, trovano precipuo (se non esclusivo) ambito di applicazione nella fase delle indagini, in cui il soggetto nei cui confronti si procede non è ancora a conoscenza della propria qualità e non sospetta di essere posto sotto osservazione.

Nel caso delle indagini in discorso, oltretutto, ciò che si pone sotto osservazione è un sistema informatico: nulla le perquisizioni *on line* possono dire, di per sé, circa l'identità della persona che in quel momento lo sta utilizzando, si tratti o meno della persona indagata. Il problema, già postosi nella prassi[6], è risolto caso per caso, alla luce di tutte le risultanze in concreto disponibili.

Allo stesso modo in cui nessun atto di investigazione, comportante limitazione di diritti fondamentali dell'indagato, può essere posto in essere da privati (e nemmeno dal difensore in sede di investigazioni difensive), coerentemente alla sistematica del codice di rito, su un piano definitorio non possono essere ricomprese nell'ambito delle perquisizioni *on line* le attività che, pur rispondendo alla descrizione proposta, siano poste in essere non già dagli organi dell'investigazione penale, bensì da "semplici" privati (che non agiscano quali ausiliari dei predetti organi).

Su un piano temporale, le perquisizioni *on line* devono collocarsi, almeno ai fini del presente lavoro, nella fase di investigazione *successiva* all'acquisizione di una notizia di reato, giammai prima ed al fine di ricercare notizie di reato. Per evitare scenari da *inquisitio generalis*, la giurisprudenza afferma tradizionalmente che nessun mezzo di ricerca della prova può trasformarsi in strumento di ricerca della stessa *notitia criminis*[7]. In realtà, per le perquisizioni *on line* dovrebbe farsi un discorso parzialmente diverso, se solo si riflette intorno alla già citata vicenda tedesca della *Online Durchsuchung*, strumento dotato – nella sua duplice veste di *on line search* e di *on line surveillance* – non solo di potenzialità investigative rispetto ad un

[3] "*Sniffers, also known as network analyzers, can read electronic data as it travels through a network. Network administrators use them to monitor networks and troubleshoot network connections. Sniffers can help network administrators find and resolve network problems. However, a hacker can break into a network and install a sniffer that logs all activity across a network, including the exchange of passwords, credit card numbers, and other personal information*": K.T. KLEINDIENST-T.M. COUGHLIN-J.K. PASQUARELLA, *Computer crimes*, in 46 *Am. Crim. L. Rev.*, p. 318.

[4] Dato, ci si rende conto, per nulla scontato, essendo possibile che un sistema sia utilizzato da più soggetti, non solo con *account* diversi ma anche in modo "promiscuo". Sul punto cfr. subito *infra* nel testo.

[5] Sul tema dei reati informatici cfr., per tutti, L. PICOTTI, voce *Reati informatici*, in *Enc. giur. Treccani*, XXVI, Roma, 1999.

[6] Si pensi all'attività di contrasto contro la pedopornografia di cui all'art. 14 della legge 3 agosto 1998, n. 269.

[7] Cfr. Cass. pen., sez. III, 18 giugno 1997, n. 2450, Sirica, in *Cass. pen.*, 1998, 2081, con nota di ROMBI.

reato commesso, bensì anche di una spiccata attitudine preventiva e proattiva rispetto a reati futuri o comunque non ancora noti [8]. Ma una tale estensione di campo aprirebbe scenari troppo vasti, per cui, come il legislatore interno ha inteso distinguere le intercettazioni propriamente "giudiziali" (artt. 266 ss. c.p.p.) dalle intercettazioni preventive (art. 226 att. c.p.p.), allo stesso modo è bene tener distinte le perquisizioni *on line* da effettuarsi all'interno del procedimento penale da quelle che, in ipotesi, si potrebbero svolgere prima o al di fuori di esso ed è bene precisare che, nel presente lavoro, per "perquisizioni *on line*" si intenderanno solo quelle del primo tipo.

Descritto per sommi capi il fenomeno, si formula il quesito cui si vorrebbe cercare di dare risposta. Posto che l'impressionante progresso tecnico-scientifico rende ormai possibile l'impiego di programmi che consentono le perquisizioni *on line*, una tale attività d'indagine, se effettuata, che trattamento ha nel processo penale? Prescindendo da ogni considerazione di carattere penale sostanziale, essa è giuridicamente ammissibile nel processo? In caso di risposta affermativa, di quali garanzie deve essere circondata, prima, durante e dopo la sua esecuzione? E, sempre in caso di risposta affermativa, i contributi conoscitivi ottenuti sono utilizzabili unicamente nella fase procedimentale od anche nel dibattimento?

2. Il principio di atipicità delle indagini preliminari

Come noto, vige nell'ordinamento processuale italiano il c.d. principio di atipicità delle indagini preliminari secondo cui, accanto agli atti espressamente previsti dal legislatore, gli organi dell'investigazione possono anche porne in essere di non specificamente normati. A riconoscerlo è stata la stessa Relazione al Progetto preliminare del codice di rito vigente [9], in ciò poi seguita tanto dalla dottrina [10] quanto dalla giurisprudenza [11]. A tale *genus* la Cassazione ha ad es. ricondotto il pedinamento tradizionale [12], nonché la c.d. localizzazione mediante GPS [13], ritenendoli ambedue di competenza della polizia giudiziaria, anche in carenza di previo provvedimento dell'autorità giudiziaria [14].

[8] Cfr. R. FLOR, *op. cit*., pp. 696-697 e 703 ss.

[9] *Progetto preliminare del codice di procedura penale – Relazione*, Istituto Poligrafico e Zecca dello Stato, Roma, 1988; in particolare, per la polizia giudiziaria si afferma che "*nel quadro delle attività ad iniziativa della polizia giudiziaria da compiersi prima dell'intervento del pubblico ministero, si è inteso distinguere una attività 'informale', diretta ad assicurare le fonti di prova mediante una azione di ricerca, individuazione e conservazione, sostanzialmente libera nei modi di suo svolgimento, e taluni atti 'tipici' soggetti ad una più rigorosa disciplina*" (191); per il P.M., si parla di attività "*ispirata alla 'forma libera e alla atipicità degli atti'*" (p. 198).

[10] Cfr., per tutti, A. NAPPI, *Guida al codice di procedura penale*, X ed., Milano, 2007, pp. 259-260 e 283, nonché TRANCHINA, in AA.VV., *Diritto processuale penale*, II, Milano, 2006, pp. 97-99 e 128-129.

[11] Cfr., ad es., Cass. pen., sez. II, 27 marzo 2008, n. 16818, Gori, in *CED*, rv. 239774, relativa a riconoscimento fotografico di polizia giudiziaria, secondo cui "*la disciplina processuale (artt. 55 e 348 c.p.p.) è orientata al principio dell'atipicità degli atti di indagine della polizia giudiziaria, alla quale compete pertanto il potere-dovere di compiere di propria iniziativa, finché non abbia ricevuto dal pubblico ministero direttive di carattere generale o deleghe per singole attività investigative, tutte le indagini che ritiene necessarie ai fini dell'accertamento del reato e dell'individuazione dei colpevoli e quindi anche quegli atti ricognitivi che quest'ultima finalità sono diretti a conseguire, quali l'individuazione di persone o di cose*".

[12] Cass. pen., sez. II, 30 ottobre 2008, n. 44912, Sozzo, in *Guida dir.*, 2009, 5, p. 90.

[13] Cass. pen., sez. VI, 11 dicembre 2007, n. 15396, Sitzia, in *CED*, rv. 239635 (fattispecie relativa al pedinamento satellitare dell'autovettura di un indagato).

[14] Opinione per la quale si impone, probabilmente, un ripensamento, quantomeno per la localizzazione mediante GPS (cfr. *infra*, par. 6).

Prima di approfondire il tema delle investigazioni atipiche, però, occorre chiedersi se le perquisizioni *on line* non siano suscettibili di essere ricondotte in una figura tipica di atto di indagine, il che consente, tra l'altro, di rimarcare alcune loro peculiarità.

3. Le perquisizioni *on line* come atti di indagine atipici incidenti sulla riservatezza della vita privata

Va preliminarmente precisato che, nella ricerca di un modello tipico cui ricondurre le perquisizioni *on line*, deve adottarsi un canone ermeneutico di interpretazione tassativa. Per diretto mandato costituzionale, infatti, in queste ipotesi la norma processuale penale è volta a dare attuazione alla riserva di legge, ovvero a stabilire "casi e modi" attraverso cui i pubblici poteri possono attingere diritti altrimenti definiti inviolabili (artt. 13-15 Cost.): casi e modi insuscettibili, pertanto, di interpretazioni analogiche od estensive.

Nello sforzo di ricercare un parametro legale già esistente, cui ricondurre le perquisizioni *on line*, un primo riferimento potrebbe essere fatto alle perquisizioni tradizionali. Ma emergono subito molteplici punti di divergenza, che non consentono di ricondurre le prime alla disciplina tipica delle seconde (artt. 247 ss. c.p.p.). Le perquisizioni tradizionali possono essere unicamente personali o locali e sono strutturalmente orientate alla ricerca del corpo del reato e/o delle cose pertinenti al reato che, in caso di reperimento, vengono senz'altro sequestrate; le perquisizioni *on line*, invece, si svolgono per lo più in quel luogo virtuale che è il *web*, possono prescindere dalla ricerca del corpo del reato e/o delle cose pertinenti al reato e non sfociano necessariamente in un sequestro. Soprattutto, è vero che le perquisizioni tradizionali sono atti a sorpresa, nel senso che non deve essere dato previo avviso del loro compimento all'indagato, ma quest'ultimo, ove presente, ben si accorge, durante lo svolgimento delle operazioni, di essere sottoposto all'atto coercitivo, tanto da avere diritto ad una serie di avvisi in chiara funzione garantistica (notifica del decreto motivato, invito a nominare un difensore di fiducia ovvero, in mancanza, designazione di un difensore d'ufficio [15], conseguente diritto di farsi assistere dal difensore [16]; le perquisizioni *on line*, invece, non sono solamente atti a sorpresa ma, per essere fruttuose, devono restare ignote all'indagato durante tutto il corso del loro svolgimento.

Né le novità introdotte dalla legge n. 48 del 2008 possono far mutare tale conclusione [17]. Alla luce dell'art. 247, comma 1-*bis*, c.p.p., infatti, anche quando hanno per oggetto sistemi informatici o telematici, le perquisizioni "tradizionali" non vengono meno alla loro finalità di ricerca di cose pertinenti al reato e rimangono comunque presidiate dagli ordinari diritti difensivi appena sopra menzionati.

Quanto sin qui detto potrebbe allora portare ad un accostamento alle intercettazioni, specie di comunicazioni informatiche o telematiche (art. 266-*bis* c.p.p.): anche le intercettazioni,

[15] Cfr. Cass. pen., sez. un., 23 febbraio 2000, n. 7, Mariano, in *Cass. pen.*, 2000, p. 2225.

[16] Art. 365 c.p.p.

[17] Sulla legge n. 48 del 2008 cfr. AA.VV., *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, a cura di L. LUPARIA, Milano, 2009; L. PICOTTI-L. LUPARIA, *La ratifica della convenzione Cybercrime del consiglio d'Europa (commento alla l. 18 marzo 2008 n. 48)*, in *Dir. pen. e proc.*, 2008, p. 696; F. NOVARIO, *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla l. 18 marzo 2008 n. 48 al codice di procedura penale*, in *Riv. dir. proc.*, 2008, p. 1069. Utili spunti anche in L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007.

durante il loro svolgimento, devono restare ignote al soggetto attinto, cioè all'indagato. L'iniziale, suggestiva similitudine lascia peraltro il campo a insormontabili differenze. Come noto, il *common core* delle intercettazioni è dato dalla captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo [18]: definizione che si deve ritenere applicabile anche alle intercettazioni di comunicazioni informatiche o telematiche intercorrenti tra utenti del *web*. Sia ben chiaro: ove le perquisizioni *on line* fossero preordinate a (o comunque consentissero nel concreto di) captare delle conversazioni tra utenti, il tutto si risolverebbe in una intercettazione ai sensi dell'art. 266-*bis* c.p.p., obbligando al rispetto delle forme ivi previste e comportando, in caso di inosservanza, l'inutilizzabilità degli esiti (art. 271, comma 1, c.p.p.). Ma non è questo il fenomeno su cui si vuol portare l'attenzione (se non altro perché esso, risolvendosi in una intercettazione illegittima, troverebbe già una compiuta disciplina, anche sanzionatoria) [19]: le perquisizioni *on line* sono concepite per ottenere un elevato numero di informazioni utili senza alcuna necessità di percepire comunicazioni in atto tra utenti, bensì semplicemente attraverso la sistematica o periodica raccolta di dati presso il sistema informatico utilizzato dall'indagato (*on line search*) od attraverso la registrazione dei suoi movimenti sul *web* (*on line surveillance*). A questo proposito, premesso che, sotto il profilo tecnico, "muoversi" nella rete comporta necessariamente l'invio ed anzi lo scambio di dati tra più sistemi informatici o telematici (il proprio e, quantomeno, quello del *provider* del servizio), giovi la seguente precisazione. Captare tali dati integra senza dubbio, in astratto, il reato di cui all'art. 617-*quater*, comma 1, c.p. che punisce, tra l'altro, l'apprensione di comunicazioni "*intercorrenti tra più sistemi*", ma non integra ancora l'intercettazione di comunicazioni processualmente rilevante, la quale richiede, rispetto alla norma sostanziale, un *quid pluris*: che le comunicazioni intercorrano non tra meri sistemi informatici, bensì tra utenti, vale a dire tra persone fisiche che agiscono con l'intenzione di comunicare l'una con l'altra a mezzo della rete [20]. Ecco che allora risulta chiaro, per sottrazione, il possibile oggetto delle perquisizioni *on line*: per non ricadere sotto la disciplina *tipica* delle intercettazioni, esse devono avere come fine l'apprensione di dati aventi carattere "non comunicativo tra utenti", per utilizzare l'espressione di recente giurisprudenza di legittimità [21].

Nemmeno la categoria delle ispezioni pare in grado di offrire una soluzione appagante. Si è soliti insegnare che, rispetto alle perquisizioni, la cui finalità è la ricerca di determinati oggetti (corpo del reato, cose pertinenti al reato), le ispezioni sono strutturalmente tese a fotografare una situazione di fatto suscettibile di modifica (artt. 244 ss. c.p.p.). Né il quadro è mutato per effetto delle modifiche introdotte dalla legge n. 48 del 2008, che si è limitata a contemplare, all'art. 244, comma 2, c.p.p., anche i sistemi informatici e telematici come possibili oggetti di ispezione, ma senza mutare la natura genetica dell'atto ispettivo. Viceversa, le perquisizioni *on line* risultano totalmente estranee alla funzione denotativa-descrittiva, tipicamente statica, delle ispezioni, essendo atte ad una "subdola" raccolta, anche prolungata nel tempo, di dati ed informazioni di pertinenza dell'indagato, alla sua insaputa. Da ciò discende l'inadeguatezza delle garanzie legali previste: ai sensi dell'art. 364 c.p.p., l'ispezione è normalmente sottopo-

[18] Definizione pacifica: Cass. pen., sez. VI, 9 febbraio 2005, n. 12189, Rosi, in *Cass. pen.*, 2006, p. 606.

[19] Cfr. ancora par. 1.

[20] L'intuizione relativa a questo "scollamento" tra la nozione di intercettazione penalmente rilevante *ex* art. 617-*quater* c.p. e di intercettazione rilevante a fini processuali è già in R. FLOR, *op. cit*., p. 698. Esemplificando, ove un utente si colleghi ad un sito di aste *on line* e vi osservi alcuni oggetti, sicuramente genera uno scambio di dati tra sistemi, ma ancora non comunica a fini processuali; ove egli effettui un'offerta ad altro utente, pone in essere un'attività comunicativa.

[21] Cfr. *infra*, par. 4.

sta a termini di preavviso (comma 1) e, anche nei casi di maggior urgenza, è sempre "*fatta salva [...] la facoltà del difensore d'intervenire*" (comma 5): facoltà che presupporrebbe una *discovery* che frustrerebbe radicalmente gli scopi di qualsiasi perquisizione *on line*.

Potrebbe allora, da ultimo, venir naturale accostare le perquisizioni *on line* al pedinamento, atto sia pure (o forse appunto) *atipico* di indagine, magari mediante il suggestivo accostamento dello spazio fisico in cui si svolge il pedinamento con lo sterminato spazio virtuale (il *web*) in cui potrebbe avvenire la perquisizione *on line*. Ma anche tale accostamento è fallace ed anzi consente di porre un punto fermo da cui muovere per ogni successiva riflessione.

Ed in effetti, se l'accostamento avvenisse per applicare alla perquisizione *on line* la disciplina del pedinamento, sarebbe chiaro l'errore. La giurisprudenza, infatti, ritiene che il pedinamento sia atto di indagine atipico di polizia giudiziaria e che *non* sia intrusivo della sfera privata, perché non limiterebbe, diversamente dai mezzi di ricerca della prova, la libertà morale del controllato [22].

Non si vuole al momento sottoporre a critica la correttezza di simile assunto, bensì solamente notare come, viceversa, non vi sia atto più intrusivo della sfera privata della perquisizione *on line*, a prescindere (come già detto) da ogni considerazione in ordine alla possibile violazione di una qualche norma di diritto penale sostanziale. Sia che si presenti sotto forma di "pedinamento virtuale", cioè di raccolta dei dati di navigazione sul *web* (*on line surveillance*) sia che consista nella copia dei dati già contenuti nel sistema informatico di riferimento (*on line search* o *one-time copy*) o nella captazione *on line* di qualsiasi altro dato "non comunicativo tra utenti", essa consente di raccogliere una impressionante mole di "dati personali" – secondo la definizione data dall'art. 4, comma 1, lett. b), d.lgs. 30 giugno 2003, n. 196, c.d. codice della privacy – del soggetto interessato (come, per la verità, anche di altri soggetti) [23] e, quindi, di incidere in modo drammatico sul bene giuridico costituito dalla c.d. riservatezza dei dati personali: riservatezza che, a tutto voler concedere, non pare non possa essere ricondotta *quantomeno* alla protezione offerta dall'art. 2 Cost., in assenza di una diversa e più specifica disposizione costituzionale che la protegga.

4. Il limite al compimento degli atti di indagine atipici: le garanzie costituzionali

Aver concluso per l'atipicità delle perquisizioni *on line* (nonché per la loro non assimilabilità nemmeno al pedinamento) non rappresenta ancora una soluzione al problema.

Definire atipico un determinato atto di indagine, in quanto non rientrante in nessuno schema legale, non significa ovviamente che vi sia assoluta libertà di compierlo, perché tale conclusione legittimerebbe ogni tipo di abuso [24].

Se si discute di un "riconoscimento" fotografico realizzato presso gli uffici della polizia giudiziaria, si può ancora consentire (pur con fondate perplessità in ordine alla genuinità di un successivo formale atto di individuazione *ex* art. 361 c.p.p. o di una ricognizione dibattimentale *ex* artt. 213 ss. c.p.p.) che esso, di per sé, non vulneri una libertà fondamentale dell'indagato; ma valori costituzionali come la libertà personale, quella domiciliare, nonché la segre-

[22] Così Cass. pen., sez. II, 30 ottobre 2008, n. 44912, cit.

[23] La raccolta di quella che, nel testo, definisco "impressionante mole" di informazioni è ovvia conseguenza delle premesse investigative da cui muove la perquisizione *on line*: la ricerca di dati *a carattere probatorio*, relativi all'indagato.

[24] Cfr., per considerazioni ormai "classiche", M. NOBILI, *Scenari e trasformazioni del processo penale*, Padova, 1998, pp. 43 e 202.

tezza delle comunicazioni (artt. 13, 14 e 15 Cost.) non possono essere incisi se non con le garanzie previste dalla Carta fondamentale.

È quello che si può definire "approccio funzionale" della giurisprudenza al tema degli atti di indagine atipici: in carenza di disciplina legale, quel che conta per capire se e come possono essere compiuti è su quali valori costituzionali vadano ad incidere.

Premesso che sono ipotizzabili tre livelli decrescenti di garanzia del privato di fronte a possibili atti di indagine compiuti nei suoi confronti – riserva di legge e riserva di giurisdizione, solo l'una o solo l'altra, nessuna di esse [25] –, emblematico di quello che si vuole definire approccio funzionale della giurisprudenza è il caso deciso dalle sezioni unite della Corte di cassazione nel c.d. caso Prisco [26].

Vale la pena di ripercorrere i passaggi fondamentali di tale pronunzia, avente ad oggetto la spendibilità processuale della captazione di videoriprese non comunicative in luoghi aperti al pubblico effettuata dalla polizia giudiziaria.

Appare ancora una volta doveroso premettere che, ove si captassero comunicazioni, si rientrerebbe nello schema tipico delle intercettazioni, con quanto ne consegue in punto di garanzie (richiesta del P.M., provvedimento autorizzatorio del G.I.P., modalità esecutive, ecc.) e di invalidità nel caso di loro inosservanza (art. 271, comma 1, c.p.p.).

Ma se si captano videoriprese di comportamenti non comunicativi, secondo le sezioni unite in esame rileva in modo decisivo il luogo di ripresa.

La videocaptazione di comportamenti non comunicativi nel *domicilio* richiede il rispetto delle doppie garanzie previste dall'art. 14 Cost., posto appunto a tutela dell'inviolabilità domiciliare: garanzie che sono, segnatamente, la riserva di legge e quella di atto motivato dell'autorità giudiziaria. Poiché, pertanto, tale mezzo di indagine – captazione di videoriprese non comunicative – non è, almeno attualmente, disciplinato dalla legge, *non può* svolgersi nel domicilio: "*le riprese video di comportamenti "non comunicativi" non possono essere eseguite all'interno del "domicilio", in quanto lesive dell'art. 14 Cost. Ne consegue che è vietata la loro acquisizione ed utilizzazione anche in sede cautelare e, in quanto prova illecita, non può trovare applicazione la disciplina dettata dall'art. 189 c.p.p.*" [27]. Viene qui evocato il concetto di "prova incostituzionale": finalmente la Corte di cassazione, dopo decenni di intenso dibattito dottrinario (cui aveva sempre fatto eco una certa refrattarietà giurisprudenziale) [28], gli riconosce diritto di cittadinanza nell'ordinamento italiano, secondo un percorso ricostruttivo che fa discendere dalla violazione della norma costituzionale (in questo caso l'art. 14) la sanzione della inutilizzabilità della prova sotto il profilo della sua inammissibilità [29].

---

[25] Il massimo di tutela si realizza, ovviamente, quando all'astratta previsione della riserva di legge in ordine ai casi ed ai modi dell'intrusione si aggiunge la riserva di atto motivato dell'autorità giudiziaria per la singola autorizzazione all'intrusione: è il modello previsto appunto, sia pure con diverse sfumature, dagli artt. 13, 14 e 15 Cost.

[26] Cass. pen., sez. un., 28 marzo 2006, n. 26795, Prisco, in *Cass. pen.*, 2006, p. 3937, con note di RUGGIERI e DI BITONTO.

[27] *Ibidem*. Altro passaggio motivazionale interessante è il seguente: "*certo è che se il sistema processuale deve avere una sua coerenza risulta difficile accettare l'idea che una violazione del domicilio che la legge processuale non prevede (e che per questa ragione risulta* in contrasto *con il contenuto precettivo dell'art. 14 Cost.) possa legittimare la produzione di materiale di valore probatorio*" (*ivi*, p. 3942).

[28] Per i riferimenti in ordine al tema della prova incostituzionale sia consentito rinviare a S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia*, 2007, p. 407 ss.

[29] Dopo aver affermato, quasi a voler ridimensionare le proprie precedenti affermazioni, che "*non occorre però prendere posizione sul dibattito relativo agli effetti che la violazione delle norme costituzionali di garanzia può avere sull'attività probatoria prevista dal codice di rito, né stabilire se la sanzione dell'inutilizzabilità attenga solo alla violazione dei divieti stabiliti dalla legge processuale o riguardi anche la violazione di norme*

Viceversa, la captazione di comportamenti non comunicativi in *luoghi aperti al pubblico*, come i privé di un locale notturno (era questo il caso scrutinato dalla Corte) od i bagni di un bar o di un ristorante, non incide sul domicilio, bensì "solo" sulla riservatezza della vita privata, cioè sull'art. 2 Cost., che non pone alcuna riserva di legge espressa. Ne consegue, secondo la Corte di cassazione, che tale attività investigativa rientra pienamente nello schema dell'art. 189 c.p.p. e necessita unicamente del previo provvedimento dell'*autorità giudiziaria* (quindi, anche solo del P.M.), che deve comunque essere pur sempre *motivato*[30].

5. La riservatezza della vita privata nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e nel nuovo sistema delle fonti italiano

Secondo le sezioni unite appena viste, dunque, atti di indagine atipici che vulnerino "unicamente" il diritto alla riservatezza dell'indagato possono essere compiuti, pur in assenza di espressa previsione legale, a condizione che vi sia la garanzia del provvedimento motivato dell'autorità giudiziaria.

Su tale conclusione, apparentemente lineare, è però destinata ad incidere la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (di seguito CEDU). Successivamente alle sezioni unite appena viste, risalenti al 2006, si è infatti avuta una vera e propria rivoluzione nel sistema delle fonti di diritto interno: con sentenze n. 348 e 349 del 2007, nonché 39 del 2008, la Corte costituzionale, facendo leva sull'art. 117, comma 1, Cost., ha stabilito che le norme della CEDU hanno, nell'ordinamento italiano, rango interposto, vale a dire superiore a quello della legge ordinaria ed inferiore solo a quello delle norme costituzionali[31]. Ove si sospetti che una norma di legge ordinaria contrasti con la CEDU – e, annotazione essenziale, con la giurisprudenza della Corte europea dei diritti dell'uomo, che ne è l'interprete autentico – ed ove il contrasto non sia eliminabile con gli ordinari strumenti dell'interpretazione conforme, detta norma può ed anzi deve essere sottoposta allo scrutinio del giudice delle leggi, cui spetta appunto l'ultima decisione.

Importanti conferme di tale impostazione vengono da tre ulteriori, recenti pronunce della Corte costituzionale: la n. 311 e la n. 317 del 2009 ed infine la n. 93 del 2010.

---

costituzionali (...)" (Cass., sez. un., 28 marzo 2006, n. 26795, *cit.*, p. 3943), la Corte afferma appunto che il tema dell'inutilizzabilità riguarda solo le prove tipiche e che invece le prove atipiche, prima della loro ammissione non sono prove, "*perciò se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le sorreggono ci si deve interrogare innanzi tutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità, e a parere di queste Sezioni unite se si fa corretta applicazione dell'art. 189 c.p.p. le videoregistrazioni acquisite in violazione dell'art. 14 Cost. devono considerarsi inammissibili*" (*ibidem*).

In realtà, se è vero che la giurisprudenza non sembra aver mai compiutamente distinto, ai fini dell'operare della sanzione dell'inutilizzabilità *ex* art. 191 c.p.p., tra le varie fasi del procedimento probatorio, la dottrina ha da tempo affermato che l'inutilizzabilità riguarda sicuramente le fasi di acquisizione e, ancor prima, di ammissione della prova: N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Padova, 1992, pp. 102-110, anche per ulteriori rimandi.

[30] Cass., sez. un., 28 marzo 2006, n. 26795, *cit.*, p. 3944: "*sono queste, e non quelle in ambito domiciliare, le riprese che possono avvenire sulla base di un provvedimento motivato dell'autorità giudiziaria, sia essa il pubblico ministero o il giudice*".

[31] Sulle due sentenze del 2007 si vedano almeno: AA.VV., *Forum: La Cedu nelle sentenze 348 e 349/2007 della corte costituzionale*, in *Dir. pubbl. comp. ed eur.*, 2008, p. 171; L. CAPPUCCIO, *La corte costituzionale interviene sui rapporti tra convenzione europea dei diritti dell'uomo e costituzione*, in *Foro it.*, 2008, I, c. 47; R. CONTI, *La corte costituzionale viaggia verso i diritti CEDU: prima fermata verso Strasburgo*, in *Corr. giur.*, 2008, p. 205.

La prima di queste si segnala per il puntuale riepilogo che contiene, al par. 6 del "Considerato in diritto", sul rango e sull'efficacia delle norme della CEDU nel diritto interno, nonché sul ruolo dei giudici nazionali e della Corte di Strasburgo. In particolare, ove investita di una questione di legittimità di una norma interna, per sospetto contrasto con quella convenzionale, la Corte costituzionale "*dovrà anche, ovviamente, verificare che il contrasto sia determinato da un tasso di tutela della norma nazionale inferiore a quello garantito dalla norma CEDU*" [32].

La seconda pronunzia esplicita ancor meglio tale concetto: "*con riferimento ad un diritto fondamentale, il rispetto degli obblighi internazionali non può mai essere causa di una diminuzione di tutela rispetto a quelle già predisposte dall'ordinamento interno, ma può e deve, viceversa, costituire strumento efficace di ampliamento della tutela stessa. Se si assume questo punto di partenza nella considerazione delle interrelazioni normative tra i vari livelli delle garanzie, si arriva facilmente alla conclusione che la valutazione finale circa la consistenza effettiva della tutela in singole fattispecie è frutto di una* combinazione virtuosa *tra l'obbligo che incombe sul legislatore nazionale di adeguarsi ai principi posti dalla CEDU – nella sua interpretazione giudiziale, istituzionalmente attribuita alla Corte europea ai sensi dell'art. 32 della Convenzione – l'obbligo che parimenti incombe sul giudice comune di dare alle norme interne una interpretazione conforme ai precetti convenzionali e l'obbligo che infine incombe sulla Corte costituzionale – nell'ipotesi di impossibilità di una interpretazione adeguatrice – di non consentire che continui ad avere efficacia nell'ordinamento giuridico italiano una norma di cui sia stato accertato il deficit di tutela riguardo ad un diritto fondamentale*". Tale "*combinazione virtuosa*" viene anche definita "*continua e dinamica integrazione*", e lo scopo del meccanismo viene individuato nella "*massima espansione delle garanzie, anche attraverso lo sviluppo delle potenzialità insite nelle norme costituzionali che hanno ad oggetto i medesimi diritti*" [33].

La terza si segnala come l'ultima pronunzia – ovviamente allo stato – del percorso volto ad attribuire alla CEDU il rango di norma interposta, inferiore alla Costituzione ma superiore alla legge ordinaria. Essa contiene un puntuale riepilogo di tutti i principi illustrati nelle precedenti sentenze [34] e si segnala perché ribadisce con forza che, prima ed al fine di sollevare questione di legittimità costituzionale, il giudice *a quo* deve provare ad "*allineare la disciplina censurata alle pronunce della Corte europea per via d'interpretazione*" [35].

Ora, come noto, il sistema della CEDU contiene, a differenza della Costituzione italiana, una norma espressa in materia di tutela del diritto alla riservatezza. Secondo l'art. 8 CEDU, segnatamente, "*ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza*" (art. 8.1 CEDU); ed inoltre: "*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 una serie di finalità tassativamente previste e che non interessa al momento elencare (art. 8.2 CEDU) [36].

È vero che la stessa Corte europea dei diritti dell'uomo ha enucleato una concezione abbastanza flessibile dell'ingerenza "prevista dalla legge", dovendo ricavare un minimo comune

[32] Corte cost., sent. n. 311 del 2009, Considerato in diritto, par. 6.

[33] Corte cost., sent. n. 317 del 2009, Considerato in diritto, par. 7.

[34] Corte cost., sent. n. 93 del 2010, Considerato in diritto, par. 4.

[35] Corte cost., sent. n. 93 del 2010, Considerato in diritto, par. 8.

[36] Su tale norma ed altre omologhe nel panorama internazionale cfr. G. TIBERI, *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti internazionali*, in *Cass. pen.*, 2009, p. 4467 (I parte) e 2010, p. 355 (II parte).

denominatore tale da abbracciare 47 ordinamenti giuridici, che spaziano dal *common law* al *civil law*[37]; però è altrettanto vero che, una volta filtrata nell'ordinamento italiano, la locuzione "ingerenza prevista dalla legge" non può che essere ricondotta al preciso ed univoco significato nazionale di "riserva di legge", con quanto ne consegue in punto alla doverosità, per il legislatore interno, di prevedere casi e modi di aggressione del bene tutelato.

Ma vi è di più: se l'art. 8 CEDU accomuna la riservatezza della vita privata, il domicilio e la corrispondenza sotto un unico "ombrello" di tutela, prevedendo che le ingerenze nell'esercizio di questi tre beni debbano trovare un fondamento legale, sarebbe razionale il comportamento di un legislatore interno che preveda casi e modi di intrusione solo per due di essi (segnatamente, domicilio e corrispondenza) e lasci invece piena libertà in ordine ai casi e modi di intrusione nel terzo (vita privata)[38]?

In definitiva, in forza dell'art. 8 CEDU, direttamente applicabile nell'ordinamento italiano per effetto dell'art. 117 Cost., è oggi necessaria una legge ordinaria per consentire ingerenze dei pubblici poteri nella riservatezza della vita privata delle persone, nonostante l'art. 2 Cost. nulla dica a riguardo. Ciò perché, nell'ottica ben evidenziata dalle pronunce costituzionali nn. 311 e 317 del 2009, in questo caso è evidente il maggior livello di tutela che la fonte convenzionale introduce rispetto a quella interna, che quindi subisce una "*virtuosa*" integrazione sul punto. Ed i pubblici poteri che agiscono nel processo penale non possono certo fare eccezione a ciò.

Ad analoga conclusione è possibile pervenire anche attraverso un nuovo percorso di diritto comunitario, reso possibile dalla recente entrata in vigore – il 1° dicembre 2009 – del Trattato di Lisbona. Secondo l'art. 6 del Trattato sull'Unione europea, da un lato "*l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati*" (art. 6.1), dall'altro lato "*i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali*" (art. 6.3).

Nella prima prospettiva, la Carta dei diritti fondamentali dell'Unione europea protegge, all'art. 8, i dati di carattere personale, statuendo che essi possono essere trattati col consenso della persona interessata oppure sulla base di "*altro fondamento legittimo previsto dalla legge*" (art. 8.2). È vero che, secondo il successivo art. 51.1, la Carta dei diritti si applica unicamente nell'ambito dell'attuazione del diritto dell'Unione, ma è altrettanto vero che la materia

[37] Si veda, di recente, la sentenza della Corte europea, sez. II, 20 gennaio 2009, Sud Fondi c. Italia, parr. 105-110. La Corte si occupa del concetto di "diritto" nell'art. 7 CEDU, che è significativamente quello che pone il principio di riserva di legge in materia penale. Al par. 108, la Corte afferma: "*la notion de 'droit' ('law') utilisée à l'article 7 correspond à celle de 'loi' qui figure dans d'autres articles de la Convention; elle englobe le droit d'origine tant législative que jurisprudentielle et implique des conditions qualitatives, entre autres celles de l'accessibilité et de la prévisibilité (Cantoni c. France, 15 novembre 1996, § 29, Recueil 1996-V; S.W. c. Royaume-Uni, § 35, 22 novembre 1995; Kokkinakis c. Grèce, 25 mai 1993, §§ 40-41, série A no 260 A)*".

[38] In altri termini: la Convenzione mostra di ritenere assimilabili, per natura ed importanza, i beni della vita privata, del domicilio e della corrispondenza, tanto da assoggettarli ad un comune regime di tutela, quello di riserva di legge. Differenziarne il trattamento a livello interno, riconoscendo solo a due di essi ciò che la Convenzione espressamente statuisce anche per il terzo significa introdurre una disparità di tutela del tutto contrastante con la norma internazionale.

Il ragionamento non è distante da quello compiuto, nel *diverso* ambito comunitario, dalla Corte di giustizia delle comunità europee a partire dalla nota sentenza 21 settembre 1989, in causa 68/88 (c.d. sentenza sul mais greco), con cui si è posto l'obbligo, per gli Stati membri, di "*vegliare a che le violazioni del diritto comunitario siano sanzionate, sotto il profilo sostanziale e procedurale, in termini* analoghi *a quelli previsti per le violazioni del diritto interno* simili per natura ed importanza" (par. 24).

della protezione dei dati personali risulta ampiamente comunitarizzata, anche a livello interno[39]. Ed il diritto comunitario, come noto, prevale sul diritto interno contrastante: per cui, anche attraverso questa via, si può sostenere la necessità di una riserva di legge per incidere sui dati personali in assenza del consenso del titolare e la contrarietà al diritto comunitario non solo della legislazione ma anche della *prassi* eventualmente divergente.

Nella seconda prospettiva, non si farebbe altro che "attrarre" nel circuito comunitario, con l'effetto di rafforzarle (se ve ne fosse bisogno), le riflessioni poc'anzi svolte per quanto riguarda l'art. 8 CEDU.

6. Inammissibilità delle perquisizioni *on line* nell'attuale panorama italiano

Sono a questo punto intuibili le conclusioni del ragionamento.

Sul versante della disciplina ordinaria, le perquisizioni *on line* non rientrano in alcuna figura legale tipica, per cui potrebbero al più ritenersi mezzi di indagine innominati (cfr. *supra*, parr. 2 e 3).

Sul versante delle garanzie coinvolte, le perquisizioni *on line* incidono – quantomeno – sul bene giuridico della riservatezza della vita privata (cfr. *supra*, par. 3).

Secondo recente ed autorevole giurisprudenza di legittimità, una determinata attività investigativa *atipica* (e, quindi, non disciplinata dalla legge), che vada ad incidere su un bene giuridico costituzionalmente protetto da *riserva di legge*, contrasta direttamente con la norma costituzionale ed è perciò stesso inammissibile (cfr. *supra*, par. 4).

La giurisprudenza costituzionale ha affermato che le norme della CEDU penetrano nell'ordinamento interno attraverso l'art. 117 Cost. ed hanno natura interposta, *superiore* a quella della legislazione ordinaria. Inoltre, secondo l'art. 8 CEDU, la vita privata è un bene giuridico che tollera ingerenze solo ove *previste dalla legge* (cfr. *supra*, par. 5). Analoga riserva di legge è prevista anche dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea (*ibidem*).

Le conclusioni che se ne traggono è che, a prescindere da ogni possibile conseguenza di diritto penale sostanziale, se le perquisizioni *on line* fossero effettuate in un procedimento penale italiano, dovrebbero essere dichiarate inammissibili come prova perché, non previste dalla legge, verrebbero ad incidere su di un bene giuridico – la riservatezza della vita privata – la cui lesione, alla luce del nuovo combinato costituzionale-sovranazionale (ed oggi anche comunitario), esige la previa determinazione, da parte del legislatore ordinario, dei casi e dei modi di aggressione di quel bene.

La perentorietà di tali conclusioni trova giustificazione anche in precise scelte valoriali. Forse non si è sufficientemente messa in luce l'insidiosità del mezzo oggetto di riflessione, che consente la raccolta di una mole impressionante ed indiscriminata di dati personali all'insaputa del soggetto attinto (e di quelli con cui entra in contatto), per un tempo indeterminato. In un simile quadro, la riserva a favore dell'autorità giudiziaria, posta dalle sezioni unite nel caso Prisco per la videoripresa nei luoghi aperti al pubblico, appare una garanzia necessaria ma non certo sufficiente: ancor più a monte si avverte la pressante necessità che sia il legislatore stesso a prevedere con ogni dettaglio possibile i casi, i modi ed i tempi del bilanciamento tra libertà ed autorità, ogni qual volta il vorticoso progresso tecnologico consenta nuove ed impensabili forme di aggressione a primari beni giuridici.

[39] Cfr. l'art. 16 del Trattato sul funzionamento dell'Unione europea, l'art. 39 del Trattato sull'Unione europea, nonché soprattutto, per gli obblighi del legislatore interno, la direttiva 95/46/CE.

L'approdo sin qui raggiunto è suscettibile di proiettare l'ombra dell'inammissibilità per contrasto con norme costituzionali anche su altri ambiti. Si vuole alludere, ad es., alla già citata localizzazione mediante GPS: la facile assimilazione che la giurisprudenza compie tra quest'attività investigativa e il pedinamento tradizionale [40] non convince, se solo si riflette sulla mole e sulla minuziosità di dati personali in ordine allo spostamento del soggetto, magari anche in luoghi privati, che la localizzazione consente di raccogliere, con infinitamente maggior agio rispetto al pedinamento tradizionale [41]. Anche qui ad essere del tutto deficitaria è la previsione legale delle modalità, specie in ordine ai casi (ad es. alle tipologie di reati) ed alla durata della relativa attività investigativa.

Non si predica, sia chiaro, una antistorica chiusura delle porte del processo alle nuove modalità investigative; piuttosto, si esige che esse siano puntualmente normate, per elementari esigenze di garanzia.

Un esempio "virtuoso" in tal senso potrebbe trarsi dalla vicenda delle indagini genetiche (peraltro coinvolgenti la sfera di libertà personale, più intensamente tutelata dalla Carta fondamentale, rispetto alla "mera" riservatezza della vita privata) nella recente storia del processo penale italiano. Dopo che la Corte costituzionale aveva dichiarato, con sentenza n. 238 del 1996, l'incostituzionalità dell'art. 224, comma 2, c.p.p., nella parte in cui non predeterminava casi e modi con cui il giudice, in sede di perizia, avrebbe potuto incidere sulla sfera personale dell'indagato o dell'imputato [42], e dopo una colpevole, pluriennale inerzia del legislatore [43], la legge n. 85 del 2009 sembra finalmente aver normato con sufficiente chiarezza e determinatezza, all'art. 224-*bis* c.p.p., la fattispecie del compimento di perizie le cui modalità incidono sulla libertà personale, inserendo poi al successivo art. 359-*bis* c.p.p. anche la possibilità per il P.M. di disporre il prelievo di campioni biologici su persone viventi [44].

Altro esempio, non a caso dal contenuto del pari tecnologicamente elevato, è quello del c.d. *data retention*. A fronte delle oscillazioni registratesi nella giurisprudenza, è infatti intervenuto il legislatore ordinario a definire nel dettaglio, all'art. 132 d.lgs. 30 giugno 2003, n. 196 (c.d. codice della privacy), casi, modi e tempi di acquisizione dei dati del traffico telefonico.

Né si dimentichi, sul versante internazionale, che in Germania la *Online Durchsuchung* è stata ritenuta incostituzionale dal *Bundesverfassungsgericht* – con considerazioni peraltro legate anche alla sua ineliminabile valenza preventiva e proattiva, secondo la legge tedesca – proprio perché, nel bilanciamento tra l'esigenza di tutela dei diritti dei cittadini, tra cui il diritto di autodeterminazione informativa ed il diritto all'integrità ed alla riservatezza dei sistemi informatici, e l'opposta esigenza di prevenzione dei reati, la legge scrutinata era nettamente sbilanciata a favore di quest'ultima, non prevedendo in modo adeguato i presupposti ed i limiti della compressione dei diritti fondamentali dell'individuo e violando, in definitiva, il principio di proporzionalità [45].

---

[40] Cass. pen., sez. VI, 11 dicembre 2007, n. 15396, *cit.*

[41] Per un diverso approccio al tema, che muove da riflessioni di diritto comparato, cfr. G. DI PAOLO, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, 2008, p. 1219 ss., nonché EAD., *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*, Padova, 2008, *passim*.

[42] Corte cost., sent. n. 238 del 1996, in *Foro it.*, 1997, I, c. 58.

[43] A non voler ritenere tale l'art. 349, comma 2-*bis*, c.p.p. (introdotto dall'art. 10, comma 1, d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, in legge 31 luglio 2005, n. 155).

[44] Sulla prova genetica cfr., per ogni ulteriore rimando, P. FELICIONI, *Accertamenti sulla persona e processo penale – Il prelievo di materiale biologico*, Milano, 2007. Sulla legge n. 85 del 2009 cfr. AA.VV., *Prelievo del DNA e banca dati nazionale*, a cura di A. SCARCELLA, Padova, 2009.

[45] R. FLOR, *op. cit.*, pp. 708-709.

Si palesa qui la frontiera più avanzata di ogni successiva riflessione giuridica: tutte le volte in cui il legislatore abbia formalmente adempiuto il proprio obbligo di dare disciplina ad un dato istituto, spetterà al giudice delle leggi sindacare il merito di tali scelte, anche in virtù del fatto che l'art. 8.2 CEDU – parametro di riferimento "interposto" ormai necessitato – pone all'attività legislativa un limite "contenutistico" secondo cui ogni interferenza nel diritto al rispetto della vita privata e familiare del cittadino deve non solo essere prevista dalla legge ma pure costituire "*una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*"[46].

[46] Riporta che, con recente sentenza in data 8 ottobre 2009, la Corte costituzionale romena ha dichiarato l'incostituzionalità della legge nazionale proprio sul *data retention* per ragioni appunto contenutistiche, anche di contrarietà all'art. 8 CEDU, R. FLOR, *op. cit*., p. 713 (in nota).

CAPITOLO 14

Caratteristiche della prova digitale*

di *Marcello Daniele*

SOMMARIO: 1. L'universalità della prova digitale. – 2. L'immaterialità della prova digitale. – 3. La dispersione della prova digitale. – 3.1. Il debole accentramento delle indagini informatiche nazionali. – 3.2. L'autarchia nelle indagini informatiche sovranazionali. – 4. La promiscuità della prova digitale e i pericoli per la riservatezza. – 4.1. L'agevole accessibilità dei sistemi informatici. – 4.2. Le aporie del regime di conservazione delle prove digitali. – 5. La modificabilità della prova digitale. – 5.1. Antidoti alla modificabilità: l'uso delle migliori tecniche informatiche. – 5.2. L'attuazione del contraddittorio tecnico.

1. L'universalità della prova digitale

Stanno diventando indispensabili in un numero sempre crescente di processi prove che si trovano nascoste all'interno di sistemi informatici [1]: *files* che contengono testi, suoni o immagini o che registrano gli eventi occorsi nei sistemi, oppure tracce lasciate dall'utilizzo dei sistemi; più esattamente, prove 'digitali', in quanto originate da una manipolazione elettronica di numeri [2].

Prove di questo genere non sono utili solo per la repressione dei reati informatici, cioè i reati commessi contro un sistema informatico o grazie allo stesso [3]. Esse possono produrre conoscenze rilevanti ai fini dell'accertamento di qualunque reato, e dunque hanno un ambito operativo potenzialmente illimitato [4]. Lo riconosce a chiare lettere l'art. 14, § 2 *c*, Convenzione di Budapest, il quale invita gli Stati contraenti ad apprestare un'apposita disciplina finalizzata a "la collecte des preuves électroniques de *toute infractions pénales*".

La grande fruibilità processuale delle prove digitali dipende dal costante incremento della diffusione dei sistemi informatici e della digitalizzazione delle conoscenze nella società moderna, con le sempre maggiori occasioni di interconnessione tra il mondo fisico e il mondo digitale che ne derivano [5].

* Il presente contributo è frutto dell'attività di ricerca svolta nell'ambito del Progetto di Ateneo "*Criminalità informatica ed accertamento penale*" (codice CPDA084200/08), finanziato dall'Università degli Studi di Padova.

[1] Cioè *computers* e reti informatiche come internet: v. le definizioni previste dall'art. 1, lett. *a* della *Convenzione del Consiglio d'Europa sulla criminalità informatica*, stipulata a Budapest il 23 novembre 2001.

[2] Dall'inglese "digit" ("cifra"): *wikipedia*, voce *Digitale (informatica)*.

[3] Si vedano L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet*, a cura di L. PICOTTI, Padova, 2004, p. 86 s.; C. SARZANA DI SANT'IPPOLITO, *Informatica, internet e diritto penale*, III ed., Milano, 2010, p. 61 s.

[4] Cfr. L. LUPARIA, *La disciplina processuale e le garanzie difensive*, in L. LUPARIA-G.ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 130 s.

[5] Si veda C. SARZANA DI SANT'IPPOLITO, *Informatica*, cit., p. 7 s.

Di fronte all'irrompere delle prove digitali sulle scene dei crimini era indispensabile un intervento del legislatore, tale da predisporre specifiche regole volte a disciplinarne la raccolta e l'utilizzazione in giudizio. Diversamente – come è già iniziato ad accadere – dovrebbe essere la giurisprudenza a farsi carico dei problemi generati dalle indagini informatiche, con il pericolo di interpretazioni non ispirate da un disegno unitario.

Assolutamente doverosa, quindi, è stata la recezione in Italia della Convenzione di Budapest da parte della legge 18 marzo 2008, n. 48. Resta da stabilire in che misura la nuova disciplina tenga nel dovuto conto le caratteristiche delle prove digitali, che sono molto diverse da quelle delle prove tradizionali [6]. Se si vogliono salvaguardare le finalità cognitive del processo devono essere le norme e le loro applicazioni concrete a piegarsi alle esigenze del mondo digitale, e non viceversa.

2. L'immaterialità della prova digitale

Di fronte alle prove digitali i processualisti si trovano a disagio, in quanto sono abituati a pensare alle prove come a degli oggetti fisici, dotati di un'evidente corporeità. Le prove digitali si presentano, invece, come entità immateriali. Ciò non significa che esse non abbiano una loro fisicità: concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili. È, però, una fisicità che, in assenza del supporto, non può essere percepita come tale.

Ciò spiega perché, in passato, si tendessero a confondere le prove digitali con gli oggetti in cui le medesime sono contenute.

Una traccia di questa più risalente e fuorviante concezione emerge in modo chiaro dal previgente art. 491-*bis* c.p. [7], il quale identificava il "documento informatico" con qualunque "supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Se le cose stessero in questi termini non sorgerebbero particolari questioni in tema di raccolta delle prove digitali. Sarebbe sufficiente applicare le disposizioni in materia di acquisizione delle prove documentali. I supporti materiali contenenti informazioni digitali reperiti nel corso delle indagini potrebbero essere prodotti in giudizio ed inseriti nel fascicolo per il dibattimento ai sensi degli artt. 495, comma 3 e 515 c.p.p. L'unico spazio per il contraddittorio si aprirebbe in sede di discussione finale, e riguarderebbe il valore conoscitivo delle informazioni.

Oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sé processualmente irrilevanti [8]. Spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in grado di contenere una massa enorme di informazioni digitali.

La definizione di documento informatico è stata opportunamente aggiornata dall'art. 1, comma 1, lett. p), d.lgs. 7 marzo 2005, n. 82 (codice dell'amministrazione digitale): ora essa

[6] Sulla conseguente necessità di ripensare tutte le comuni regole probatorie, originariamente concepite per le prove tradizionali, v. O.S. KERR, *Digital evidence and the new criminal procedure*, in *105 Columbia Law Rev.*, 2005, p. 290 s.

[7] Introdotto dalla legge 23 dicembre 1993, n. 547, ed ora abrogato dalla legge n. 48 del 2008.

[8] Cfr. L. PICOTTI, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 702 s.; P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 402.

si impernia non più sul supporto materiale del documento, ma sulla "rappresentazione" informatica di atti, fatti o dati giuridicamente rilevanti.

Fortunatamente anche la legge n. 48 del 2008 appare consapevole dell'immaterialità delle prove digitali. Il nuovo comma 1-*bis* dell'art. 247 c.p.p. disciplina la ricerca di "dati, informazioni, programmi informatici o tracce comunque pertinenti al reato" che "si trovino in un sistema informatico" [9], mostrando di percepire la differenza tra le prove digitali ed i loro contenitori.

3. La dispersione della prova digitale

Dalla immaterialità discendono ulteriori caratteristiche delle prove digitali, che creano non pochi inconvenienti in rapporto alla loro acquisizione processuale.

Si pensi, anzitutto, al rischio della loro dispersione. Molto più frequentemente delle prove tradizionali, le prove digitali di un reato si trovano dislocate in luoghi distanti tra loro: ad esempio *servers* e *personal computers* fisicamente molto lontani. Considerata l'estensione mondiale delle reti informatiche, potenzialmente la dispersione può riguardare l'intero globo terrestre [10].

Di qui la necessità che il legislatore fissi regole precise per individuare la competenza degli organi inquirenti, in modo da evitare che si sovrappongano più procedimenti in rapporto agli stessi episodi criminosi. Tale problematica non riguarda solo i rapporti tra gli organi italiani, ma anche le relazioni tra gli organi italiani e quelli stranieri, quando il reato, lasciando delle tracce digitali anche all'estero, assume una dimensione sovranazionale.

3.1. Il debole accentramento delle indagini informatiche nazionali

Purtroppo la l. n. 48 del 2008 ha affrontato la questione della dispersione della prova digitale unicamente dal punto di vista interno al nostro ordinamento, e per di più l'ha risolta in un modo che non appare soddisfacente.

La scelta è stata quella di affidare le indagini relative ai reati informatici specificamente indicati dall'art. 51, comma 3-*quinquies*, c.p.p. alle procure "presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente" [11]. Si intendeva così – come si esprimono i compilatori della legge – "facilitare il coordinamento delle indagini e la formazione di gruppi di lavoro specializzati in materia" [12]. È dubbio, però, che un tale obiettivo sia stato raggiunto [13].

[9] Nello stesso senso l'art. 352, comma 1-*bis*, c.p.p.

[10] Cfr., fra i molti, M.L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*, 2008, p. 503 s.

[11] Conseguentemente l'art. 328, comma 1-*quater*, c.p.p. prescrive che le relative funzioni di giudice per le indagini preliminari vanno esercitate "da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente".

[12] In questi termini la Relazione che accompagna il disegno di legge C 2807, da cui la legge n. 48 del 2008 è derivata.

[13] In chiave giustamente critica nei confronti della disciplina v. H. BELLUTA, *Cybercrime e responsabilità degli enti*, in AA.VV., *Sistema penale e criminalità informatica*, a cura di L. LUPARIA, Milano, 2009, p. 100 s.; F. CASSIBBA, *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in AA.VV., *Sistema penale*, cit., p. 123 s.; L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della*

a) La norma in esame non è in grado di creare una titolarità esclusiva della raccolta delle prove digitali a favore delle procure distrettuali. Le ben più numerose procure presso i tribunali possono continuare ad acquisire qualunque prova digitale relative ai reati – informatici ed anche comuni – diversi da quelli ricompresi negli elenchi dell'art. 51 c.p.p., e non connessi con gli stessi. Esse, di conseguenza, non potrebbero astenersi dallo sviluppare per proprio conto le competenze tecniche che le indagini informatiche richiedono.

b) Non è stato istituito un organo centrale simile alla Direzione nazionale antimafia, con la conseguenza che il coordinamento è soggetto al buon volere delle procure di volta in volta coinvolte nelle indagini, tramite lo strumento del collegamento stabilito dall'art. 371 c.p.p.

c) Non è raro che il luogo di consumazione di un reato informatico non risulti determinabile in modo univoco [14]. In tali situazioni operano i criteri suppletivi di attribuzione della competenza stabiliti dall'art. 9 c.p.p. [15], il cui comma 3 impone di riferirsi, qualora ogni altro criterio risulti inapplicabile, al luogo in cui l'iscrizione della notizia di reato è avvenuta per prima [16]. Una disciplina del genere, lungi dal favorire il coordinamento, stimola al più la rapidità della conduzione delle indagini, la via più sicura per ottenerne il monopolio.

3.2. L'autarchia nelle indagini informatiche sovranazionali

Altrettanto censurabile è l'ottica monocolare dell'intervento della legge n. 48 del 2008, interamente calibrato sulla disciplina interna senza tenere conto dei rapporti con gli altri Stati in tutte le ipotesi in cui le indagini informatiche assumono un carattere sovranazionale.

I criteri di attribuzione della giurisdizione tradizionalmente impiegati in questa materia, da tempo previsti dal nostro codice penale, ed in parte ripresi dalla stessa Convenzione di Budapest, sono inadatti alle indagini informatiche, o comunque hanno una natura autarchica: non impediscono agli altri Stati di adottare soluzioni analoghe, e quindi non eliminano il pericolo della sovrapposizione di procedimenti in rapporto ai medesimi fatti [17].

a) Il criterio della commissione del reato nel proprio territorio [18] non sempre risulta utilizzabile, in quanto si impernia su un dato che, come si diceva, per i reati informatici spesso resta incerto.

b) I criteri della commissione del reato all'estero da parte di un proprio cittadino [19], o tale da ledere un proprio interesse [20], dal canto loro, non impediscono che un procedimento sia iniziato pure dalle autorità dello Stato estero, qualora il fatto sia penalmente rilevante anche nell'ambito di quest'ultimo.

Convenzione sul cybercrime, in AA.VV., *Le nuove norme sulla sicurezza pubblica*, a cura di S. LORUSSO, Padova, 2008, p. 65 s. A favore, invece, delle scelte operate dall'art. 51, comma 3-*quinquies*, c.p.p., M.L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. Internet*, 2008, p. 504 s.

[14] Si pensi all'accesso abusivo in un sistema informatico (art. 615-*ter* c.p.): esso si consuma già con l'ingresso nel sistema oppure successivamente, al momento dell'apprensione delle informazioni contenute nel sistema? Cfr. sul punto R. FLOR, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus*, in *Cass. pen*., 2009, p. 1517 s.

[15] I criteri dell'art. 9 c.p.p. operano anche nel caso di connessione tra reati distinti: cfr. Cass., sez. un., 16 luglio 2009, n. 40537.

[16] V. H. BELLUTA, *Cybercrime*, cit., p. 98; M.L. DI BITONTO, *L'accentramento*, cit., p. 505 s.

[17] Cfr. D. MICHELETTI, *Reato e territorio*, in *Criminalia*, 2009, p. 579 s.

[18] Artt. 4 e 6 c.p., e 22, § 1 *a*, *b* e *c* Convenzione di Budapest.

[19] Artt. 9 c.p., e 22, § 1 *d* Convenzione di Budapest.

[20] Artt. 7, 8 e 10 c.p.

A fronte di questi possibili conflitti di giurisdizione, l'art. 22, § 5 della Convenzione di Budapest prescrive la consultazione tra gli Stati interessati, "al fine di stabilire la competenza più appropriata per esercitare l'azione penale": un rimedio preventivo di cui la legge n. 48 del 2008 si è disinteressata.

Né è stato ascoltato il richiamo della Convenzione all'adozione di misure di cooperazione specificamente calibrate sulle indagini informatiche (artt. 23 s.). La cooperazione, in questa materia, nel nostro sistema continua ad essere affidata al metodo tradizionale della rogatoria: uno strumento che, a causa dei suoi tempi e delle sue viscosità, non sempre risponde alle esigenze di celerità imposte dalla raccolta delle prove digitali, la quale richiede in molti casi ingressi in tempo reale nei sistemi informatici [21].

4. La promiscuità della prova digitale e i pericoli per la riservatezza

Un'ulteriore caratteristica delle prove digitali, che deriva sempre dalla loro immaterialità, è la promiscuità. Queste prove possono trovarsi collocate in spazi virtuali enormi e pieni di dati di ogni tipo. Non è raro che siano mescolate ad informazioni irrilevanti rispetto al reato, e magari attinenti alla vita privata dell'indagato o di altre persone.

Le indagini informatiche, dunque, sono sempre potenzialmente in grado di pregiudicare la riservatezza degli individui [22]. La loro capacità lesiva della privacy è addirittura superiore a quella delle intercettazioni; queste ultime si limitano a carpire le informazioni che la persona intercettata ha deciso di rivelare ad altri, mentre l'analisi dei sistemi informatici e delle reti possono rivelare il contenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere. In ogni caso, dati riservati che nulla hanno a che fare con la commissione dei reati, e che sono facilmente divulgabili proprio grazie alle tecnologie informatiche e ad internet, in grado di renderle conoscibili da un numero sterminato di persone.

È inevitabile che il legislatore tenga conto anche di questa ulteriore peculiarità delle prove digitali, apprestando delle procedure in grado di contemperare la tutela della riservatezza e le esigenze di accertamento. Un difficile bilanciamento che può essere realizzato agendo sia sul profilo dell'accessibilità dei sistemi informatici che su quello della conservazione delle prove digitali [23].

4.1. L'agevole accessibilità dei sistemi informatici

Al fine di proteggere la riservatezza una via sarebbe regolamentare in modo preciso e con il massimo delle garanzie l'accessibilità dei sistemi informatici [24]. Si potrebbero prevedere re-

[21] Cfr. E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, in *Guida dir.*, 2008, 16, p. 72 s.

[22] V., per tutti, F. RUGGIERI, *Profili processuali nelle investigazioni informatiche*, in AA.VV., *Il diritto penale dell'informatica*, cit., p. 158 s.

[23] Per tale distinzione cfr. C. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in AA.VV., *Le nuove norme sulla sicurezza*, cit., p. 30 s., nonché Corte cost., 6 novembre 2006, n. 372.

[24] In questo senso cfr. il § 14 della Risoluzione del XVIII Congresso internazionale di diritto penale (Istanbul, 20-27 settembre 2009), commentata da R.E. KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale*, in *Riv. dir. proc.*, 2010, p. 330 s. Similmente, in rapporto all'acquisizione dei dati di traffico, C. CONTI, *L'attuazione della direttiva*, cit., p. 30 s.

quisiti analoghi a quelli delle intercettazioni[25]: autorizzazione di un giudice alle operazioni di apprensione, preesistenza di gravi indizi di uno dei reati previsti in un elenco legislativo, vaglio preventivo sulla indispensabilità del mezzo.

Le scelte operate dal legislatore, però, non sono andate in questa direzione: la disciplina vigente consente di entrare negli spazi digitali di pertinenza dei privati e dei fornitori di servizi informatici in base a modalità ben più agevoli.

Le indagini informatiche sono configurate come ispezioni, perquisizioni e sequestri: mezzi di ricerca della prova che possono essere disposti anche dal pubblico ministero[26] o, nella flagranza del reato o nei casi d'urgenza, dalla stessa polizia[27], i cui atti vanno poi convalidati dal pubblico ministero[28].

La previsione relativa alle ispezioni – che consistono in ricerche puramente visive – ha, in realtà, un ambito operativo ridotto: le prove digitali, come si diceva, non sono percepibili con i soli occhi, e le ispezioni possono al più servire per osservare in via preliminare il sistema informatico nelle sue sole componenti esterne[29].

Dunque il presupposto principale delle indagini informatiche coincide con quello delle perquisizioni, vale a dire il fondato motivo di ritenere che tracce digitali di qualunque reato si trovino in un dato sistema informatico. È una condizione il cui riscontro va adeguatamente giustificato, ma non difficile da osservare: la integra la presenza di qualunque elemento – al più anche mere supposizioni logiche basate sulla tipologia del reato commesso – in grado di qualificare quel sistema come un potenziale contenitore di prove, senza la necessità di individuare in anticipo che cosa sarà trovato[30].

Le prove digitali rinvenute a seguito della perquisizione devono essere sequestrate, in originale o in copia, in base all'art. 253, comma 1, c.p.p., se consistono nel corpo del reato o in cose pertinenti al reato necessarie per l'accertamento dei fatti. In alternativa, ove consentito, il sequestro può avere ad oggetto i supporti materiali che contengono le prove, ai fini della loro successiva analisi ed eventuale copia.

Lo stesso standard è richiesto per i dati attinenti al traffico, qualificabili come prove digitali quando riguardano comunicazioni avvenute tramite sistemi informatici[31] oppure l'uso di sistemi informatici[32]. L'art. 132, comma 3, d.lgs. 30 giugno 2003, n. 196 (codice della privacy) prescrive che essi sono acquisibili presso i fornitori di servizi informatici con decreto

[25] I quali operano già in forza dell'art. 266-*bis* c.p.p. in rapporto all'acquisizione delle comunicazioni in corso tramite sistemi informatici.

[26] Si vedano gli artt. 244, comma 2, 247, comma 1-*bis*, 248, comma 2, 254, comma 1, 254 *bis*, 256, comma 1, 260, comma 2, c.p.p.

[27] Cfr. in particolare gli artt. 352, comma 1-*bis* e 354, comma 2, c.p.p.

[28] Artt. 352, comma 4 e 355, c.p.p.

[29] Cfr. S. ATERNO, *Art. 8*, in AA.VV., *Cybercrime, responsabilità degli enti, prova digitale*, a cura di G. CORASANITI e G. CORRIAS LUCENTE, Padova, 2009, p. 205 s. In senso diverso v. A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir*., 2008, 16, p. 66, secondo cui rientrerebbero nelle ispezioni operazioni come il sequestro in copia dell'hard disk.

[30] Così, in rapporto alle perquisizioni in generale, tra le molte, Cass., sez. II, 19 giugno 2008, n. 35866.

[31] Delle quali i dati in questione consentono di stabilire le modalità (si veda l'art. 3, d.lgs. 30 maggio 2008, n. 109), senza però rivelarne i contenuti: ragione per cui sarebbe illogico includere la loro acquisizione nell'ambito delle intercettazioni, come invece dispone il discutibile disegno di legge S 1611 in materia di intercettazioni, giustamente criticato, sotto questo profilo, da V. GREVI, *Le intercettazioni come mero "mezzo di ricerca" di riscontri probatori?*, in *Cass. pen*., 2009, p. 850.

[32] Si pensi agli indirizzi ip, che permettono di determinare i tempi e la fonte degli ingressi nei sistemi, essenziali per risalire ai computers da cui gli ingressi hanno avuto origine: v. O.S. KERR, *Digital evidence*, cit., p. 283 s.

"motivato" del pubblico ministero. Nonostante che la norma non lo espliciti, è ragionevole pensare che la motivazione debba investire la probabilità di rinvenire prove del reato [33], ed inoltre che il provvedimento di apprensione dei dati sia impugnabile nelle stesse forme dei sequestri delle altre prove digitali [34]. Lo conferma il fatto che l'art. 254-*bis* c.p.p., introdotto dalla legge n. 48 del 2008, prevede la possibilità di sequestrare i dati detenuti dai fornitori, "compresi quelli di traffico": tale ultima disposizione, pur senza incidere sui termini di conservazione stabiliti dall'art. 132 codice della privacy, ha l'effetto di ricomprendere le operazioni in esame nell'orbita dei mezzi di ricerca di tutte le altre prove digitali.

La legge non commina nessuna inutilizzabilità nel caso in cui i requisiti previsti non fossero rispettati: nulla vieterebbe, ad esempio, di acquisire in dibattimento le prove digitali reperite a seguito di una perquisizione informatica ordinata direttamente dalla polizia pur in assenza di urgenza, oppure non convalidata dal pubblico ministero [35].

Questo regime di facile ingresso nei sistemi informatici, mirato a favorire la repressione penale anche a costo della riservatezza, è ineccepibile dal punto di vista del rispetto degli artt. 14 e 15 Cost.: quando le prove digitali sono situate in un domicilio o quando consistono in forme di corrispondenza la loro acquisizione avviene sulla base di un atto motivato dell'autorità giudiziaria, nei casi e nei modi legalmente prestabiliti.

Né la disciplina in esame appare criticabile sotto il profilo della sua opportunità. L'universalità delle prove digitali sconsiglia di limitarne la reperibilità solo in rapporto ad un elenco prestabilito di reati. Le prove digitali, inoltre, molto più frequentemente delle conversazioni intercettate, sono le prime tracce dei reati informatici: sarebbe irragionevole subordinarne l'acquisizione alla preesistenza di indizi di reato e al preventivo impiego di altri mezzi investigativi. Si aggiunga che le intercettazioni hanno ad oggetto dati comunicativi di tipo dinamico, in via di formazione al momento stesso della loro captazione, e vanno necessariamente eseguite in segreto, per evitare di pregiudicarne l'effetto. Le prove digitali, al contrario, anche quando contengono comunicazioni – si pensi alla corrispondenza inoltrata per via telematica [36] – sono già cristallizzate nel loro apporto informativo. Questa è la ragione per cui, come si vedrà, vanno ricercate tramite un'indagine percepibile da tutti i presenti, compreso il difensore dell'indagato [37]: un'attività che non necessita, per questo suo carattere pubblico, dei più severi requisiti richiesti per le intercettazioni.

4.2. Le aporie del regime di conservazione delle prove digitali

Se appare sconsigliabile difendere la privacy in via preventiva, restringendo le modalità di accesso ai sistemi informatici da parte degli organi inquirenti, in quali limiti una protezione è

[33] È naturale che tale probabilità non sia, invece, richiesta quando l'istanza proviene dal difensore dell'indagato, il quale "*può richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391 quater del codice di procedura penale*".

[34] Ritengono, al contrario, che l'acquisizione in base all'art. 132 codice della privacy non sia impugnabile S. ATERNO-A. CISTERNA, *Il legislatore interviene ancora sul data retention, ma non è finita*, in *Dir. pen. proc.*, 2009, p. 289 s.

[35] Così C. CONTI, *L'attuazione della direttiva*, cit., p. 26, anche se in riferimento ai soli dati di traffico. V. pure, prima dell'entrata in vigore della l. n. 48 del 2008, F. RUGGIERI, *Profili processuali*, cit., p. 161.

[36] Sequestrabile in base all'art. 254 c.p.p., e quindi non sottoposta al regime delle intercettazioni: cfr. L. LUPARIA, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 721.

[37] V. *infra*, par. 5.2.

conseguibile attraverso la disciplina della conservazione delle prove digitali?

Quest'ultima forma di salvaguardia deve esplicarsi sul duplice fronte della loro detenzione da parte dei fornitori dei servizi informatici e da parte dell'autorità giudiziaria. Si può già anticipare come la tutela appaia, nel complesso, eccessiva dal primo punto di vista, ed insufficiente dal secondo.

Quanto alle prove digitali presso i fornitori, le barriere per la riservatezza sono rappresentate dalle modalità di trattamento dei dati attinenti al traffico informatico e dai termini della loro conservazione.

Le regole di trattamento stabilite dal Garante per la privacy [38] sono senz'altro rigorose: esse consentono l'accesso ai dati solo a personale qualificato, tramite sistemi di autenticazione informatica e di registrazione degli ingressi. Sono, però, allo stato piuttosto costose da adottare, e non stupisce che la loro attuazione sia stata reiteratamente prorogata dal Garante.

La disciplina dei termini di conservazione dei dati, dal canto suo, appare eccessivamente sbilanciata a favore della tutela della riservatezza. I termini vigenti – dodici mesi dalla ricezione dei dati, ed inoltre ulteriori novanta giorni, prorogabili fino a sei mesi, per i dati oggetto della speciale procedura di congelamento introdotta dalla l. n. 48 del 2008 [39] – valgono indiscriminatamente per tutti i reati, e potrebbero risultare, in concreto, troppo ristretti [40], finendo con l'essere aggirati. Non si dimentichi che nessuna norma processuale vieta di acquisire i dati conservati oltre i termini prescritti [41]. Divieti probatori non appaiono ricavabili neppure dalla generica inutilizzabilità stabilita dall'art. 11 comma 2 codice della privacy, che si origina a seguito della "violazione della disciplina rilevante in materia di trattamento dei dati personali": nell'ambito di quest'ultima non si possono certo ricomprendere le regole di ammissione delle prove [42]. Sarebbe stato preferibile prevedere termini più ampi perlomeno in rapporto ai reati di maggiore gravità, e comunque non scendere al di sotto dei ventiquattro mesi consentiti dalla direttiva europea attuata dalle prescrizioni in esame [43].

La riservatezza appare eccessivamente pregiudicata, per converso, sul fronte della detenzione delle prove digitali da parte degli organi inquirenti. Ciò è dovuto al fatto che in giurisprudenza si tende a differenziare il regime di conservazione delle prove digitali originali sequestrate insieme ai loro supporti materiali da quello delle eventuali copie, conservate su altri supporti. Non si dubita che gli originali vadano restituiti ai legittimi proprietari ai sensi dell'art. 262 c.p.p., al più tardi dopo il passaggio in giudicato della sentenza [44]. Una volta riottenuti gli originali, però, l'indagato non avrebbe il diritto di entrare nel possesso anche delle copie [45].

Tale interpretazione trascura il fatto che non è in gioco solo il diritto di proprietà, a tutelare il quale sarebbe sufficiente la restituzione degli originali, ma anche la riservatezza. Le co-

[38] Si veda il provvedimento del 17 gennaio 2008, poi modificato dal provvedimento del 24 luglio 2008.

[39] Cfr. i commi 4 *ter-quinquies* dell'art. 132 codice della privacy, i quali hanno introdotto una normativa che non brilla per precisione: si vedano le critiche di F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in AA.VV., *Sistema penale*, cit., p. 236 s., e di L. LUPARIA, *La ratifica*, cit., p. 722 s.

[40] Così C. CONTI, *L'attuazione della direttiva*, cit., p. 16 s.

[41] In senso contrario v. C. CONTI, *L'attuazione della direttiva*, cit., p. 26.

[42] Cfr. C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, p. 120 s.

[43] Art. 6 direttiva 2006/24/CE.

[44] Con possibilità per il pubblico ministero di riesaminare gli originali qualora vi fosse la necessità di svolgere ulteriori indagini impraticabili sulle copie: v. Cass., sez. VI, 26 giugno 2009, n. 26699.

[45] Così Cass., sez. un., 24 aprile 2008, n. 18253, poco prima dell'entrata in vigore della legge n. 48 del 2008.

pie, in rapporto quest'ultima, sono pericolose tanto quanto gli originali, poiché contengono la medesima massa di informazioni. Se rimanessero indefinitamente a disposizione dell'autorità giudiziaria, aumenterebbe il rischio della loro apprensione da parte di terzi. Questo è il motivo per cui va preferita la lettura in base alla quale l'interesse in capo alla difesa ad impugnare i provvedimenti di sequestro dei dati digitali continua a sussistere anche dopo la restituzione degli originali [46].

5. La modificabilità della prova digitale

L'immaterialità delle prove digitali ne determina anche un'altra caratteristica: la loro congenita modificabilità. I dati contenuti in un sistema informatico sono facilmente alterabili da parte di chiunque ne venga in contatto. Sono altissimi i rischi che le prove digitali siano contraffatte o manipolate, volontariamente oppure a causa dell'impiego delle tecniche sbagliate [47].

Si capisce pertanto perché, affinché le prove digitali possano generare informazioni decisive in giudizio, è essenziale garantirne l'autenticità. A tale fine è necessario proteggere quella che quella che gli studiosi anglosassoni definiscono la "catena di custodia" (*chain of custody*): le prove digitali devono rimanere integre in tutti i loro passaggi dal sistema informatico di origine alla disponibilità da parte del giudice del dibattimento [48].

Esistono dei possibili rimedi alla contaminazione delle prove digitali, un pericolo che il legislatore non potrebbe permettersi di ignorare, a pena della vanificazione della pretesa punitiva, oppure della perdita di prove a difesa magari decisive per la sorte dell'imputato?

5.1. Antidoti alla modificabilità: l'uso delle migliori tecniche informatiche

Un primo antidoto è rappresentato dall'impiego delle metodologie di individuazione e di apprensione delle prove digitali in assoluto ritenute migliori dalla tecnica informatica.

Sotto questo profilo, l'ideale sarebbe che il legislatore prestabilisse una specifica tecnica di acquisizione dalle prove digitali, da osservare scrupolosamente a pena di inutilizzabilità ogni volta in cui un reato lasciasse tracce in un sistema informatico. Il metodo prescelto diventerebbe la "regola d'oro" [49] della formazione delle prove digitali, come l'esame incrociato lo è per l'assunzione delle prove dichiarative.

Al momento, però, purtroppo questa strada non è percorribile. L'informatica è una scienza relativamente giovane, e non si può dire che ad oggi esista un metodo di raccolta delle prove digitali in grado di imporsi su tutti gli altri [50]. Gli esperti in materia suggeriscono perlopiù

[46] Cfr. S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc*., 2009, p. 481; P. TONINI, *Documento informatico*, cit., p. 405.

[47] Si vedano, tra i molti, L. LUPARIA, *La disciplina processuale*, cit., p. 147 s.; P. TONINI, *Documento informatico*, cit., p. 404.

[48] Queste problematiche sono approfondite da E. CASEY, *Digital evidence and computer crime*, II ed., London, 2004, p. 169 s.

[49] L'espressione è di P. FERRUA, *La regola d'oro del processo accusatorio: l'irrilevanza probatoria delle contestazioni*, in AA.VV., *Il giusto processo, tra contraddittorio e diritto al silenzio*, a cura di R.E. KOSTORIS, Torino, 2002, p. 11 s.

[50] Per una rassegna v. E. CASEY, *Digital evidence*, cit., p. 193 s. Nella dottrina italiana, G. ZICCARDI, *Le tecniche informatico-giuridiche di investigazione digitale*, in L. LUPARIA-G. ZICCARDI, *Investigazione penale*, cit., p. 3 s.

un approccio pragmatico: la scelta della tecnica da impiegare dipende dalla situazione che si presenta in concreto agli investigatori [51]. Una normativa che cristallizzasse un metodo piuttosto che un altro sarebbe a rischio di immediata obsolescenza, in quanto fisserebbe regole che potrebbero essere velocemente superate dell'evoluzione.

Appare, quindi, giustificabile l'approccio della legge n. 48 del 2008, la quale non ha delineato una tecnica precisa di raccolta delle prove digitali, ma si è limitata a fissare gli obiettivi che gli organi inquirenti devono perseguire, in accordo con le *best practices* adottate a livello internazionale [52]. Si tratta di due indicazioni di fondo che vanno osservate in rapporto a qualunque attività di raccolta delle prove digitali, nonostante che il legislatore non abbia interpolato tutti gli articoli del codice rilevanti in materia.

a) Le operazioni di individuazione e di apprensione delle prove digitali – che il legislatore, come si diceva, ricomprende nelle ispezioni, nelle perquisizioni e nei sequestri – vanno svolte impiegando "misure tecniche" in grado di "assicurare la conservazione" e di "impedire l'alterazione" dei dati originali [53].

b) I sequestri tramite copia delle prove digitali devono avvenire su "adeguati supporti", tramite tecniche che assicurino "la conformità della copia all'originale e la sua immodificabilità" [54]. La scelta se sequestrare i dati originali o se copiarli, giustamente, non è effettuata in astratto dal legislatore, ma è lasciata agli operatori, sulla base della situazione concreta [55].

Se si ritiene condivisibile la scelta di non precostituire un metodo di conduzione delle indagini informatiche, si devono però accettare pure i corollari che ne discendono.

Una prima conseguenza è che la raccolta delle prove digitali rientra nella classe degli accertamenti tecnici. Di qui la necessità di integrare le norme in tema di ispezioni, di perquisizioni e di sequestri con quelle che prescrivono l'intervento di appositi esperti in tutti gli stadi del procedimento: in sede di indagini di polizia [56], quando il pubblico ministero assume la direzione delle investigazioni [57], ed anche in dibattimento, dove il giudice può valutare l'operato degli investigatori attraverso il canale della perizia [58]. Il che porta inevitabilmente al sostanziale monopolio degli esperti nella gestione e nella valutazione delle prove digitali, come del resto avviene in ordine ad ogni altra indagine scientifica immessa nel processo penale.

Mancando un preciso metodo di raccolta delle prove digitali consacrato dal legislatore, inoltre, è inevitabile che manchino pure le relative sanzioni. Non sono configurabili nullità di ordine generale o inutilizzabilità quando le indagini informatiche non sono svolte da esperti, o quando vengono impiegati metodi che non appaiono in grado di assicurare gli obiettivi perseguiti dal legislatore [59]. Affermare il contrario [60] significherebbe ricavare divieti probatori basa-

[51] V. A. GRILLO-U.E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen*., 2010, p. 375 s.

[52] Cfr. G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in AA.VV., *Sistema penale*, cit., p. 165 s.

[53] Art. 244, comma 2, c.p.p.; v. anche gli artt. 247, comma 1-*bis*; 254, comma 2; 259, comma 2; 352, comma 1-*bis* e 354, comma 2, c.p.p.

[54] Art. 260, comma 2, c.p.p.; v. anche gli artt. 254-*bis* e 354, comma 2, c.p.p. Una tecnica di copia in grado di assicurare questo risultato, anche se non sempre praticabile in concreto, è quella della *bit stream image*, su cui v. L. LUPARIA, *La ratifica*, cit., p. 719 s.

[55] Cfr. S. ATERNO, *Art. 8*, cit., p. 209 s.

[56] Art. 348, comma 4, c.p.p.

[57] Artt. 359 e 360 c.p.p.

[58] Artt. 220 s., 468 e 501, c.p.p.

[59] Così G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in AA.VV., *Sistema penale*, cit., p. 190 s. Ammette l'assenza di chiare previsioni di inutilizzabilità anche A. MONTI, *La nuo-*

ti sulla sola lesione dell'interesse tutelato dalla legge [61], ma privi, in realtà, di un'espressa copertura normativa [62].

L'assenza di regole di esclusione della prova digitale non comporta la totale arbitrarietà dell'indagine informatica. Tutti gli errori tecnici commessi in sede di raccolta, pur non sanzionati con l'inutilizzabilità, sono destinati a pesare al momento della valutazione della prova. In quest'ultima sede il giudice ha la possibilità, grazie agli apporti dei periti e dei consulenti tecnici della difesa, di testare le tecniche informatiche impiegate, e di verificare se la catena di custodia delle prove digitali si sia spezzata [63].

5.2. L'attuazione del contraddittorio tecnico

L'altro antidoto alla modificabilità delle prove digitali è rappresentato dall'attuazione del contraddittorio tecnico nella loro raccolta. È controverso, tuttavia, il modo in cui realizzare quest'ultimo: sono ipotizzabili almeno tre scenari interpretativi, variabili a seconda del bilanciamento tra le esigenze dell'accusa e i diritti della difesa che si ritenga preferibile.

a) *Negazione del contraddittorio tecnico*. È ricorrente l'affermazione giurisprudenziale secondo cui le operazioni di sequestro tramite copia delle prove digitali costituirebbero in ogni caso accertamenti tecnici ripetibili *ex* art. 359 c.p.p., da svolgere pertanto senza le garanzie fissate dall'art. 360 c.p.p. per gli accertamenti non ripetibili: il preavviso alla difesa in ordine al compimento delle operazioni, la possibilità di parteciparvi con un proprio esperto e il diritto all'instaurazione dell'incidente probatorio [64].

Questa asserzione, nella sua assolutezza, non è conciliabile con il carattere della modificabilità della prova digitale. Qualunque ingresso in un sistema informatico, anche se effettuato con le metodiche più avanzate, può alterare i dati in esso contenuti, generando mutazioni che, anche se minimali, rischiano di risultare decisive se riguardano circostanze fattuali rilevanti ai fini dell'affermazione della responsabilità dell'imputato [65].

Vale a dire che le procedure di copia delle prove digitali, anche quando non riguardano dati in procinto di modificarsi – condizione che già da sola consentirebbe l'esperibilità della

va disciplina del sequestro informatico, in AA.VV., *Sistema penale*, cit., p. 217. In giurisprudenza v. già Trib. Bologna, 22 dicembre 2005, in *Dir. Internet*, 2006, p. 153 s.

[60] Ritiene configurabile una nullità intermedia A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. Internet*, 2008, p. 509 s. Parla, invece, di inutilizzabilità E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in AA.VV., *Sistema penale*, cit., p. 162 s.; analogamente, prima della l. n. 48 del 2008, L. LUPARIA, *La disciplina processuale*, cit., p. 196 s.

[61] Secondo l'impostazione di N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Milano, 1992, p. 139 s.

[62] Per la necessità che le inutilizzabilità siano esplicitamente costruite dalla legge processuale nella forma dei divieti di acquisizione v. F. CORDERO, *Procedura penale*, VIII ed., Milano, 2006, p. 616 s.

[63] Cfr. G. BRAGHÒ, *L'ispezione*, cit., p. 188 s.

[64] Cfr. Cass., sez. I, 5 marzo 2009, n. 14511, secondo cui l'attività di copia non comporterebbe "*alcuna attività di carattere valutativo su base tecnico-scientifica*", né determinerebbe "*alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in prospettiva dibattimentale*": sarebbe assicurata "*in ogni caso, la riproducibilità di informazioni identiche a quelle contenute nell'originale*"; negli stessi termini Cass., sez. un., 25 febbraio 2010, n. 15208. V. pure Id., sez. I, 30 aprile 2009, n. 23035; Id., sez. I, 1º aprile 2009, n. 16942; Id., sez. II, 31 marzo 2009, n. 18581; Id., sez. I, 11 marzo 2009, n. 12472; Id., sez. I, 26 febbraio 2009, n. 15153; Id., sez. I, 26 febbraio 2009, n. 11863.

[65] V., *ex plurimis*, L. LUPARIA, *La disciplina processuale*, cit., p. 151 s.

procedura degli accertamenti tecnici non ripetibili – potrebbero risultare tali da mutare irreversibilmente l'oggetto su cui cadono, integrando la fattispecie dell'art. 117 disp. att. c.p.p., e legittimando comunque l'impiego dell'art. 360 c.p.p.

Ancora più criticabile è la statuizione della Corte di cassazione in forza della quale l'esame di un sistema informatico non di pertinenza dell'indagato, svolto in via d'urgenza dalla polizia in base all'art. 354, comma 2, c.p.p., non sarebbe garantito dal diritto di assistere in capo al difensore [66].

È una lettura che va decisamente respinta, in quanto contrasta con la scelta della legge n. 48 del 2008 di includere le investigazioni informatiche nei contenitori normativi delle ispezioni, delle perquisizioni e dei sequestri: mezzi di ricerca della prova in rapporto ai quali il difensore, pur non avendo il diritto di essere preavvisato, ha in ogni caso il diritto di assistere [67], stabilito a pena di nullità intermedia [68].

L'importanza di questo diritto è cruciale: assistendo al compimento dell'atto, un difensore anche privo di cognizioni in materia avrebbe maggiori possibilità di informare il proprio consulente in ordine alle operazioni svolte dagli investigatori, in modo da contestare più efficacemente in dibattimento le tecniche impiegate.

Ciò non comporta che il diritto all'assistenza vada esteso in modo indiscriminato: esso non arriva a ricomprendere il diritto ad ottenere l'interruzione dell'attività di indagine qualora il difensore non fosse immediatamente reperibile [69]. Al contempo, però, non va sistematicamente azzerato sulla base della sola urgenza dell'operazione [70].

Dalla configurazione legislativa delle indagini informatiche derivano precise ripercussioni anche ai fini della qualificazione giuridica di quelle operazioni di perquisizione occulta dei personal computers, previste dall'art. 19 della Convenzione di Budapest, possibili grazie all'impiego di appositi programmi in grado di introdursi nei sistemi informatici e di carpirne i contenuti [71].

Attività del genere rientrerebbero nel paradigma delle intercettazioni delineato dall'art. 266-*bis* c.p.p., seguendone la relativa disciplina, solo qualora riguardassero comunicazioni o conversazioni in corso mediante i sistemi informatici sotto controllo.

L'apprensione segreta dei dati digitali statici contenuti in un computer e non destinati ad essere condivisi con altre persone non trova, invece, legittimazione in nessuna norma [72]. Non si tratterebbe di una perquisizione, la quale, stando alle indicazioni del codice, dovrebbe essere compiuta da esseri umani di fronte ai presenti ed al difensore, e non da invisibili dispositivi elettronici. Né integrerebbe una prova atipica, dato che l'art. 189 c.p.p. non può essere impiegato per aggirare la regolamentazione dei mezzi di ricerca della prova disciplinati dalla legge [73]. Va

[66] Così Cass., sez. I, 25 febbraio 2009, n. 11503; v. pure Id., sez. III, 2 luglio 2009, n. 38087; Id., sez. I, 30 aprile 2009, n. 23035; Id., sez. I, 1º aprile 2009, n. 16942.

[67] Si vedano l'art. 356 c.p.p. riguardo alle indagini della polizia, e gli artt. 364, comma 5 e 365, c.p.p. quanto alle indagini del pubblico ministero.

[68] Per violazione di una norma attinente all'assistenza dell'imputato: cfr. gli artt. 178, lett. c) e 180, c.p.p.

[69] In questo senso si veda Cass., sez. fer., 25 luglio 2006, n. 27372.

[70] Non sorge nessuna nullità, invece, se il difensore, ritualmente avvisato, non si presenta: cfr. Cass., sez. VI, 22 ottobre 2008, n. 13523.

[71] Sull'adozione di questa forma di perquisizione nell'ordinamento tedesco, e sulla declaratoria di incostituzionalità da parte della Corte costituzionale federale il 27 febbraio 2008 v. C. SARZANA DI SANT'IPPOLITO, *Informatica*, cit., p. 680 s.

[72] Cfr. S. ATERNO, *Art. 8*, cit., p. 213 s.

[73] "*Non può considerarsi 'non disciplinata dalla legge' la prova basata su un'attività che la legge vieta*": Cass., sez. un., 28 marzo 2006, n. 26795.

considerata, dunque, un'attività di indagine irrituale, come tale giuridicamente improduttiva di effetti.

b) *Abuso del contraddittorio tecnico.* Muovendo dalla natura congenitamente non ripetibile delle indagini informatiche, altri affermano che, ai fini della piena realizzazione del contraddittorio tecnico, la raccolta delle prove digitali andrebbe svolta, almeno di regola, sulla base della procedura dell'art. 360 c.p.p. [74].

Questo secondo scenario interpretativo, speculare a quello appena considerato, è ineccepibile dal punto di vista dei presupposti teorici da cui muove. Proprio l'agevole modificabilità delle prove digitali, tuttavia, lo rende sconsigliabile. Le tracce più significative ai fini dell'accertamento della responsabilità, spesso, sono anche quelle nell'immediata disponibilità dell'indagato: si pensi alle prove situate nel suo personal computer o in dispositivi informatici di cui egli potrebbe facilmente entrare in possesso. Considerato che le prove digitali possono essere eliminate molto più rapidamente delle prove fisiche, è troppo alto il pericolo che, grazie al preavviso al difensore, l'indagato cancelli gli elementi a suo carico o, comunque, ne comprometta il valore conoscitivo.

c) *Graduazione del contraddittorio tecnico.* Nell'intento di contemperare le esigenze difensive con quelle dell'accusa, il contraddittorio tecnico, in questa materia, deve essere graduato.

Quando hanno ad oggetto dati nella potenziale disponibilità dell'indagato, le indagini informatiche vanno in linea di massima svolte nella forma degli atti a sorpresa, ai quali il difensore ha il diritto di assistere ma senza essere preavvisato.

In questa situazione il contraddittorio tecnico non può che essere posticipato in dibattimento, laddove la difesa ha la facoltà di contestare le procedure di raccolta e la genuinità dei dati digitali, anche tramite l'ausilio di propri esperti. Essenziale, a tal fine, è la documentazione audiovisiva integrale di tutte le operazioni svolte dagli organi inquirenti: tale adempimento, sebbene non sia previsto a pena di inutilizzabilità – e sotto questo profilo la legge n. 48 del 2008 appare criticabile – è indispensabile per rafforzare il peso conoscitivo delle prove digitali reperite.

Allo stesso tempo, in giudizio la difesa può escutere con l'esame incrociato i tecnici che si sono occupati della raccolta dei dati, anche qualora si trattasse degli stessi poliziotti: il divieto di testimonianza indiretta sancito dall'art. 195, comma 4, c.p.p. ha ad oggetto il contenuto di "dichiarazioni", tra cui certo non rientrano le operazioni necessarie per ricercare e sequestrare le prove digitali.

La più garantita procedura degli accertamenti tecnici non ripetibili va osservata quando, in rapporto al caso concreto, il pericolo della distruzione delle prove non sussiste. Il caso paradigmatico è quello delle operazioni di copia delle prove originali già sequestrate dagli organi inquirenti, e reperibili presso l'ufficio del pubblico ministero (art. 260, comma 2, c.p.p.). Venendo meno il rischio dell'alterazione dei dati, è opportuno che il contraddittorio tecnico si riespanda nella sua pienezza. Non è necessario, peraltro, che le operazioni in esame avvengano in dibattimento, come sostenuto in giurisprudenza [75]: diversamente la difesa non avrebbe la possibilità di estrarre ed esaminare una sua copia prima del giudizio, in tempo utile per apprestare al meglio la propria strategia.

[74] In questo senso v. P. TONINI, *Documento informatico*, cit., p. 405 s.; cfr. pure A. ESTER RICCI, *Digital evidence e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc*., 2010, p. 345 s.

[75] Cfr. Cass., sez. III, 9 giugno 2009, n. 28524, secondo la quale si tratterebbe, in questa ipotesi, non della "*semplice visione della cosa sequestrata che può essere effettuata fuori del contraddittorio alla sola presenza del custode*", ma di un'"*un'attività che deve essere necessariamente espletata nel dibattimento nel contraddittorio delle parti e sotto la direzione del giudice*".

CAPITOLO 15

Quella Casa nella Prateria: gli *Internet Service Providers* americani alla prova del caso Google Video*

di *Francesco Cajani*

1. Verso una III Guerra Mondiale?

Se sicuramente ha fatto il giro del mondo l'efficace immagine del Giudice Oscar Magi relativa alla "*sconfinata prateria di internet*", non tutti forse hanno avuto modo di soffermarsi attentamente sul seguito di quella espressione evocativa, laddove l'accento del Tribunale di Milano cade sul "*dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del web*" [1].

Ed infatti, a solo un mese di distanza ed in relazione al *Government Requests Tool*[2] quale risposta di Google alla lettera inviata da dieci Autorità di protezione dei dati personali[3], l'auto-

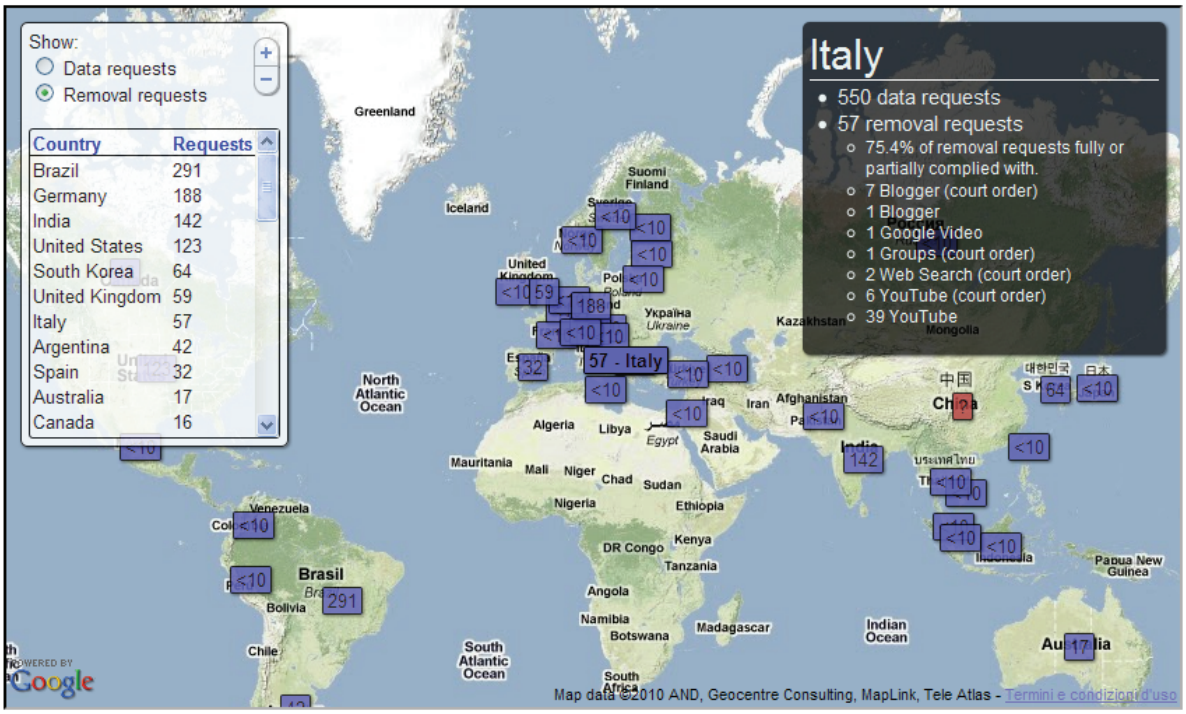
* Il presente scritto trae origine dalle sollecitazioni sul tema "*Diritti della personalità, tutela della privacy e libertà della rete*" emerse nel Seminario di Studi in memoria di Corso Bovio, tenutosi a Milano il 20 maggio 2010 presso il Circolo della Stampa: *http://www.fondazionecalamandrei.it/html/attivita/convegni/milano_20_maggio_2010_bovio.pdf*.

[1] Tribunale di Milano, sez. IV penale in composizione monocratica, sentenza 24 febbraio 2010, n. 1972, p. 95.

[2] Cfr. *http://www.google.com/governmentrequests/*.

[3] Per il comunicato stampa dell'Autorità Garante italiana e il testo della lettera cfr. *http://www.garanteprivacy.it/garante/doc.jsp?ID=1712353*.

revole testata *online* di *Wired* così intitolava: "*Word War III: Google vs. Governments*"[4].



Coloro che hanno avuto un'esperienza diretta della strategia mediatica[5] posta in essere durante i fatti relativi al caso Google Video[6] non si stupiranno del messaggio apparso in in-

[4] Cfr. *http://www.wired.com/epicenter/2010/04/word-war-iii-google-vs-governments/*.

[5] Cfr. *http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=4905&ID* (*La Stampa*, 27 maggio 2007).

[6] Trattasi della vicenda spesso denominata Google/Vividown dal nome dell'Associazione per la ricerca scientifica e per la tutela della persona Down che propose querela insieme al padre del minore disabile ripreso nel video. In questo scritto tale vicenda verrà invece significativamente chiamata "*caso Google Video*" perché l'indagine penale ha avuto ad oggetto proprio tale servizio, lanciato in Italia nel luglio 2006. In tal senso a pagina 8 della memoria dei Pubblici Ministeri depositata il 25 novembre 2009 all'esito della Requisitoria già si leggeva: "UNA DOVEROSA PREMESSA – "*Mentre ci preme rinnovare la nostra solidarietà alla famiglia del ragazzo e all'associazione Vividown, crediamo fermamente che questo procedimento non riguardi Google Video e quello che è successo, ma riguardi Internet come la conosciamo: un ambiente aperto e libero*". Sono queste le dichiarazioni rilasciate dall'ufficio stampa di Google Italy s.r.l. alla notizia della chiusura delle indagini della Procura di Milano. Di contro, riteniamo di aver raccolto un'istanza di giustizia proveniente dall'Associazione Vivi Down e dal padre di un ragazzo disabile ripreso in un filmato che è stato immesso sulla rete nelle pagine del sito *http://video.google.it* e che è rimasto per quasi due mesi nella categoria dei "video più divertenti", arrivando fino al 29° posto dei video più visti (per la precisazione: 5.500 volte) prima di essere rimosso. All'esito delle indagini, condotte tra mille difficoltà ed ostacoli frapposti, riportiamo oggi all'attenzione del Tribunale di Milano questa domanda di civiltà: esiste o no una zona franca di non applicabilità di alcune Leggi dello Stato e, in particolare, della normativa a protezione dei dati personali? Stiamo evidentemente parlando (unicamente, perché questo gli atti hanno accertato e solo a questo essi si riferiscono) del sistema Google e di coloro che, in relazione alla vicenda oggetto di indagine, si sono mossi – con i ruoli di responsabilità e di operatività – all'interno del richiamato sistema (vera miniera d'oro dei nostri giorni). Affermare invece che stiamo parlando di Internet significa, per spaventare o ancor peggio confondere, spostare artatamente l'attenzione su altro. Che nulla c'entra con il processo in corso e con la Decisione che ne seguirà, di qualunque tenore essa sia. Perché crediamo, a differenza di altri, che chi tratta i problemi di Google debba invece prendere seriamente in considerazione le norme di legge attualmente vigenti in materia di protezione dei dati personali".

È altresì doveroso ricordare come l'indagine della Procura della Repubblica presso il Tribunale per i mino-

glese sulle pagine del *blog* della società capogruppo [7], successivamente tradotto su tutti i *blog* [8] connessi alle relative filiali sparse in 32 Stati [9]. Se ne riporta, per quanto rilevante per il prosieguo, un ampio estratto [10]:

> "L'articolo 19 della Dichiarazione Universale dei Diritti Umani afferma che "ogni individuo ha il diritto alla libertà di opinione e di espressione; questo diritto include la libertà di sostenere opinioni senza condizionamenti e di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo ai confini". Scritto nel 1948, questo principio è oggi perfettamente applicabile ad Internet – uno dei più importanti strumenti per la libertà di espressione nel mondo. Tuttavia il controllo esercitato dai Governi sulla rete sta crescendo rapidamente: dal blocco completo al filtraggio dei siti, ai provvedimenti giudiziari che limitano l'accesso ad alcune informazioni, fino alle misure legislative che obbligano le aziende a controllare i propri contenuti".

Ove al nostro lettore sfuggano quali siano gli articoli della Dichiarazione Universale [11] che precedono quello sopra richiamato, basterà brevemente qui ricordare come l'art. 3 faccia riferimento alla "*sicurezza della persona*", l'art. 7 al "*diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge*" ed infine che l'art. 12 non dimentica di ribadire come "*nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata …. né a lesione del suo onore e della sua reputazione*".

Piccoli dettagli, evidentemente ….

Ma lo stesso *New York Times*, dapprima critico con la decisione del Tribunale di Milano [12], il giorno successivo ha pubblicato in prima pagina un editoriale [13] nel quale un simile paragone viene fatto in relazione alla Convenzione Europea dei Diritti dell'Uomo. Ed infatti significativamente si legge:

---

renni di Torino (Pubblico Ministero Marta Lombardi) abbia portato all'accertamento della responsabilità penale dei giovani protagonisti dell'odiosa vicenda; nello stesso senso, la Procura di Torino ha proceduto nei confronti della professoressa raffigurata nel video come presente in classe (essendo lo stesso stato girato durante l'orario scolastico).

[7] Cfr. *http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html.*

[8] Cfr. *http://www.google.com/press/blogs/directory.html#tab4.* La versione italiana del *post* in oggetto è rintracciabile su *http://googleitalia.blogspot.com/2010/04/piu-trasparenza-sulle-richieste-dei.html.*

[9] Cfr. *http://www.google.com/corporate/address.html.*

[10] "*Il colosso di Mountain View ha abbracciato l'iniziativa con entusiasmo, e ha scomodato addirittura la Dichiarazione dei Diritti dell'uomo, citata all'inizio del comunicato ufficiale. Un'enfasi che andrebbe ridimensionata, se solo si valutasse il peso reale del nuovo strumento: la lista delle rimozioni, che spesso hanno come bersaglio dei filmati di YouTube, non contempla le richieste legate alla pedopornografia, ai diritti d'autore e le segnalazioni di diffamazione da parte utenti. Lacune che vanno a sbilanciare una lettura già forzatamente approssimativa. Buona parte delle richieste tedesche, ad esempio, non sono mosse da chissà quali velleità autoritarie, ma da leggi comprensibilmente sensibili all'apologia del nazismo. Se poi ci si spinge a cliccare sulla Cina, si ottiene una risposta semplice quanto velatamente ipocrita: 'La Cina considera le richieste di censura un segreto di stato, quindi non possiamo rivelare le informazioni relative'*": M. PEDERSINI, *Tutte le censure di Google* (21 aprile 2010) in *http://www.ilfoglio.it/soloqui/4964.* Sulla trasparenza di Google rispetto ad altre società in materia di dati dei propri utenti cfr. anche le dichiarazioni di Peter Fleisher, Google's Global Privacy Counsel: "*I haven't seen any other company provide this level of transparency. Hopefully some others will be inspired to do this too*", in *http://peterfleischer.blogspot.com/2010/04/transparency-now-for-government.html.*

[11] Cfr. il testo in italiano in *http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=itn.*

[12] Cfr. E. FAZZINO, *La sentenza contro Google fa il giro del mondo* (25 febbraio 2010), in *http://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2010/02/sentenza-google-privacy-giro-mondo.shtml*.

[13] A. LIPTAK, *When American and European Ideas of Privacy Collide*, in *http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html.*

> "*On the Internet, the First Amendment is a local ordinance*," said Fred H. Cate, a law professor at Indiana University. He was talking about last week's ruling from an Italian court that Google executives had violated Italian privacy law by allowing users to post a video on one of its services. […] "*For many purposes, the European Union is today the effective sovereign of global privacy law*," Jack Goldsmith and Tim Wu wrote in their book "Who Controls the Internet?" in 2006. This may sound odd in America, where the First Amendment has pride of place in the Bill of Rights. In Europe, privacy comes first. Article 8 of the European Convention on Human Rights says, "Everyone has the right to respect for his private and family life, his home and his correspondence." The First Amendment's distant cousin comes later, in Article 10".

E dunque, alla notizia [14] che la società ha respinto "*oltre il 20% delle richieste di governi*", dal momento che vi sono "*troppe ingerenze contro la libertà sul web*", non si può che condividere la risposta dei Pubblici Ministeri del Brasile, Stato che viene collocato al primo posto di questa particolarissima classifica dei "censori digitali del Nuovo Millennio":

> "Desde quando ordens judiciais para entregar dados de criminosos è censura? […] È errado o Google classificar como censura atos judiciais legítimos de um país democrático" [15].

Ma forse continua ad essere economicamente più vantaggioso, per Google così come per tutti i grandi operatori di Internet, continuare a confondere i piani del discorso [16], facendo pubblicamente appello all'incondizionata fiducia del "libero popolo della Rete" nonché, più silenziosamente, ad una efficacissima azione di *lobbying* [17].

[14] Cfr. *http://www.ansa.it/web/notizie/rubriche/tecnologia/2010/04/21/visualizza_new.html_1765229459.html.*

[15] Articolo intitolato *Brasil è o país com mais censura, diz o Google* (20 aprile 2010), in *http://tecnologia.terra.com.br*.

[16] Secondo G. SCORZA, (*Quando la censura online è governativa,* in *http://www.wired.it/news/archivio/2010-04/26/quando-la-censura-online-e-governativa.aspx*) "*leggendo le note pubblicate da Google a margine della classifica relativa alle richieste di rimozione ricevute dal nostro Paese, invece, si scopre che solo 16 su 57 sono pervenute dall'Autorità giudiziaria mentre le altre – a quanto è dato capire e sembra comunque ricavabile a contrario – proverrebbero dal Governo e/o da enti o agenzie da esso dipendenti*". In realtà, e più semplicemente, basterebbe leggersi anche le FAQ (reperibili in *http://www.google.com/governmentrequests/faq.html)* ove si fa più chiaramente cenno alle richieste pervenute da "*government agencies like local and federal police*". Per un commento alla terminologia ivi utilizzata si rinvia a *http://www.wired.it/news/archivio/2010-04/26/quando-la-censura-online-e-governativa.aspx#comments:* "*le richieste e censure provengono da Polizia Postale, Carabinieri, Guardia di Finanza, insomma gente in divisa, mica da qualche tizio alle dipendenze del Presidente del Consiglio italiano!*".

[17] Cfr. J.H. BIRNBAUM, *Learning From Microsoft's Error, Google Builds a Lobbying Engine* (20 giugno 2007), in *http://www.washingtonpost.com/wp-dyn/content/article/2007/06/19/AR2007061902058.html?hpid=moreheadlines*; M. PANCINI (Responsabile rapporti istituzionali per Google Italy), *Le aziende non cercano più favori, ma relazioni* (23 giugno 2008), in *http://www.youtube.com/watch?v=SOh5rwCxmrc*; C. TAMBURINO, *Google e l'anticamera dei segreti – Negli ultimi anni aumentato da Mountain View il budget destinato alle attività di lobbying. Tanto da avvicinarsi alle cifre stanziate da Microsoft* (28 gennaio 2010), in *http://puntoinformatico. it/2796462/PI/News/google-anticamera-dei-segreti.aspx*. Significativa in tal senso la notizia fornita il 17 dicembre 2009 dal sito di Milano Finanza (tramite una *Dow Jones News*) secondo la quale i consulenti di Google avrebbero inviato a tutti i deputati italiani, dopo l'ordinanza del Tribunale di Roma del 16 dicembre 2009 (v. *infra*), una lettera nella quale si ribadisce che Youtube abbia natura di *hosting service provider*, regolato quindi dal d.lgs. n. 70 del 2003.

2. "Sparare nel mucchio": oltre il Far West ossia la Rete quale campo di battaglia

Forse alla penna del Giudice – la stessa che definirà "*inaspettata*"[18] la grande ricaduta mediatica del procedimento e della lettura del dispositivo, prima di farne addirittura le spese con ignobili minacce[19] figlie del clima di *disinformatia*[20] creato ad arte contro l'azione legale della Procura di Milano – sarà parsa stilisticamente troppo cruenta la metafora del "*Far West*" che, fino ad allora, era stata da molti utilizzata per esprimere lo stesso concetto.

Eppure il CEO di Google, in una recente intervista in esclusiva al *Financial Times*[21], non si scompone ed anzi rilancia con un certo-non-elegante "*bullshit*"[22], espressione che sembra ormai diventata di uso comune nella *Silicon Valley* dopo una analoga dichiarazione ad effetto di un altro CEO[23] paradossalmente proprio indirizzata al motto "*Don't Be Evil*" tanto caro ai *Google boys*:

> "The judge was flat wrong. So let's pick at random three people and shoot them. It's bullshit. It offends me and it offends the company.
>
> But this is not an indictment of Italy, says Mr Google, who earlier noted that Europe is a highly profitable market for the company".

Peraltro l'immagine della Prateria – rispetto a quella del Far West – rimane davvero felice in quanto è una rievocazione "naturalistica" del più arcano *The Blue Nowhere*[24], portando con sé anche l'idea di un qualcosa di non immediatamente percepibile o che è silenziosamente accaduto nell'attimo in cui solo il vento che la percorreva sembrava aver emesso un suono.

---

[18] Trib. Milano, sez. IV pen., in composizione monocratica, sentenza 24 febbraio 2010, n. 1972, p. 106.

[19] "*Io, giudice di Google, minacciato su Facebook per la mia sentenza*", in *http://danielelepido.blog.ilsole24ore.com/i-bastioni-di-orione/2010/04/esclusiva-io-giudice-di-google-minacciato-su-facebook-per-la-mia-sentenza.html.*

[20] Cfr. anche significativamente il *post* di S. QUINTARELLI, "*Vietato dissentire*", apparso due giorni dopo la lettura del dispositivo del Tribunale di Milano su *http://blog.quintarelli.it/blog/2010/02/vietato-dissentire-.html:* "*ho ricevuto alcune (poche) telefonate, anche da persone con ruoli di un certo livello, che, in sostanza, mi rimproveravano di non avere denunciato la 'ennesima aggressione ai diritti civili' ... nonostante la mia opinione sia nota da più di un anno, ovvero da quando avevo approfondito i pochi dettagli (allora) a disposizione*".

[21] L. BARBER-M. PALMER, *Google chief puts creativity at the heart of its culture* (4 giugno 2010), in *http://www.ft.com/cms/s/2/bdec0ee8-6f4f-11df-9f43-00144feabdc0.html*.

[22] A fronte di tale espressione il commento del collega Alfredo Robledo è stato il richiamo alle note parole di Georges-Louis Leclerc, conte di Buffon ("*Lo stile è l'uomo*"): cfr. intervista al *Corriere della Sera* (*Il pm, la privacy e Google: loro vogliono il Far West*), 6 giugno 2010, p. 21, in *http://archiviostorico.corriere.it/2010/giugno/06/privacy_Google_loro_vogliono_Far_co_8_100606029.shtml.*

[23] J.C. ABELL, *Google's 'Don't Be Evil' Mantra Is 'Bullshit,' Adobe Is Lazy: Apple's Steve Jobs* (30 gennaio 2010), in *http://www.wired.com/epicenter/2010/01/googles-dont-be-evil-mantra-is-bullshit-adobe-is-lazy-apples- steve-jobs.*

[24] "*Anderson continuò a leggere e a un certo punto emise una breve risata di sorpresa. Aveva trovato la fotocopia di un pezzo che Wyatt Gilette aveva scritto per la rivista on-line diversi anni prima. Era un articolo piuttosto famoso, e Anderson ricordò di averlo letto quando era stato pubblicato, anche se all'epoca non aveva prestato attenzione al nome dell'autore. Il titolo era 'Vita nel Nulla Blu'. Secondo Gilette i computer sono la prima invenzione tecnologica della storia capace di toccare ogni aspetto della vita umana, dalla psicologia all'intrattenimento, dall'intelligenza al benessere materiale al male, e gli essere umani e le macchine saranno sempre più vicini. Tutto questo apporta molta benefici, ma anche molti pericoli. Il termine 'Nulla Blu', che rimpiazzava la parola 'cyberspazio', indicava il mondo dei computer sia on sia offline o, come veniva anche chiamato, il 'Mondo delle Macchine'. Nella frase coniata da Gilette, Nulla Blu era un luogo intangibile eppure reale, e Blu indicava l'elettricità che permetteva ai computer di funzionare*": J. DEAVER, *Profondo Blu*, Milano, 2001 (titolo originale: *The Blue Nowhere*).

Perché anche nel *cyberspazio* tutto scorre (*πάντα ῥεῖ*) e muta, tanto è vero che – nel dibattito giuridico e sociologico – assistiamo con interesse alle distinzioni accademiche tra "corpo fisico" e "corpo elettronico" e, soprattutto, alle individuate possibilità di assumere diverse "identità personali" in Internet[25].

Ma per chi abbia una minima esperienza del mondo "reale" dei crimini informatici, la Rete – prima di tutto – rimane un insieme di computer che danno e chiedono connessione[26]: dietro ciascuno di essi, *Ecce Homo,* con le sue grandezze o miserie.

E così, se nella vita reale potrei alzarmi un giorno dal letto e – di buona lena – indossare la calzamaglia di Batman per entrare mascherato in una banca ad effettuare una rapina, sulla Rete tutto questo mi costerà forse meno fatica: con un indirizzo di posta elettronica *batman@gmail.com,* dove far automaticamente confluire le credenziali di accesso indebitamente acquisite tramite *phishing*[27], otterrò sostanzialmente lo stesso risultato, con pochi ulteriori passaggi volti al trasferimento delle somme di denaro presenti sui conti correnti *online* verso un altro salvadanaio elettronico a me solo riconducibile.

Ed anzi, operando *online* farò paradossalmente felice l'istituto di credito, perché invece se fossi davvero riuscito ad entrare con la mia calzamaglia reale e a realizzare il mio intento non ci sarebbe stato alcun dubbio che alla banca sarebbe poi toccato risarcire i propri correntisti…. ma questo è un altro discorso[28].

---

[25] Cfr. sul punto G. RESTA, *Identità personale e identità digitale*, in *Dir. inf. e informatica*, 2007, 3, p. 511 ss.

[26] "*Ciò è reso possibile da una suite di protocolli di rete chiamata 'TCP/IP' dal nome dei due principali, il TCP e l'IP, la 'lingua' comune con cui i computer di Internet si interconnettono e comunicano tra loro indipendentemente dalla loro architettura hardware e software*" (tratto da *Wikipedia*, voce Internet).

[27] Sulla tematica si consenta il rinvio a F. CAJANI-G. COSTABILE-G. MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008.

[28] Cfr. A. MONTI, *Le prime decisioni su casi di phishing limitano il diritto al risarcimento delle banche*, in *http://www.ictlex.net/?p=973*. In particolare, nell'ordinanza del Tribunale di Milano sulla costituzione delle parti civili all'udienza preliminare (G.i.p. Luerti, 10 ottobre 2008) così si legge: "[…] *In realtà, a ben vedere, il danneggiato diretto dal reato è e resta uno solo ed è il correntista, al quale sono state carpite maliziosamente le chiavi di accesso informatico al proprio conto corrente (non senza una sua volontaria, anche se incosciente, collaborazione, prestata in violazione dei rapporti con la banca e delle norme di sicurezza da questa dettate). Soltanto l'esistenza di un preciso obbligo contrattuale in capo all'istituto depositario di tenere indenne il cliente da ogni tipo – o quanto meno da questo tipo – di aggressioni alla provvista depositata potrebbe attribuire all'ente la qualità di danneggiato diretto dal reato. Al contrario, le costituzioni di PC di Intesa Sanpaolo e di Banca Mediolanum non fanno alcun cenno all'esistenza di tale obbligo; anzi, nel caso di Intesa Sanpaolo, si fa riferimento espresso a 'ragioni esclusivamente commerciali', così lasciando intendere che il ristoro al correntista è avvenuto su base volontaria, per ragioni di policy aziendale e quindi dal mero punto di vista fenomenico non direttamente collegato eziologicamente alla condotta dell'imputato o quanto meno dell'ignoto phisher. Nondimeno, appare innegabile che la condotta del phisher abbia innescato una concatenazione causale che ha determinato da un lato il proprio arricchimento e dall'altro il depauperamento del patrimonio dell'Istituto di Credito, pur attraverso il tramite dell'indennizzo della somma oggetto di prelievo informatico truffaldino. In altri termini, si deve osservare che il comportamento del 'phisher', nella specie direttamente coadiuvato dal ricettatore/riciclatore, ha cagionato un evento di danno alla banca, che – come anticipato – appare indiretto solo dal punto di vista fenomenico, per effetto della citata triangolazione del rapporto, ma non lo è dal punto di vista giuridico, per quanto concerne la concatenazione causale regolata dall'art. 1223 c.c. L'essenziale partecipazione degli odierni imputati a tale concatenazione legittima gli Istituti di Credito Intesa Sanpaolo e Banca Mediolanum ad esercitare una pretesa risarcitoria patrimoniale nei confronti degli odierni imputati nei limiti delle somme indennizzate ai correntisti che si assumono truffati.*

– singoli correntisti

Nulla quaestio in capo ad essi, che risultano titolari del patrimonio depauperato fraudolentemente e quindi sono direttamente lesi nei loro diritti soggettivi dai fatti reato ascritti non solo dei phisher, ma anche ai loro tramiti italiani che oggi sono chiamati a rispondere di ricettazione e/o riciclaggio. A costoro è infatti attribuita proprio la condotta che ha determinato l'acquisizione materiale e definitiva del denaro da parte dei phisher –

Per tornare al nostro, appare doveroso riportare l'attenzione sulla tutela dei diritti (non già quelli di "nuova generazione" in quanto "digitali" ma semmai quelli di più antica elaborazione dogmatica) sulla Rete: trattasi infatti, a sommesso ma fermo parere, del vero oggetto del processo sul caso Google Video, nascosto ai *mass media*[29] e – per esso – a molti commentatori giuridici.

E quindi, senza entrare nel merito della decisione del Tribunale[30] (peraltro non ancora passata in giudicato), nel prosieguo di questo scritto verrà sinteticamente riproposta la posizione giuridica della Procura di Milano sul tema dei profili di responsabilità degli *Internet Service Providers* e del complessivo rapporto tra Direttiva sul Commercio Elettronico e normativa (sempre di derivazione comunitaria) a protezione dei dati personali.

Con l'unico scopo di ribadire, ove fosse ancora necessario, che tale impostazione ha radici lontane in quanto fatta valere – nel suo ragionamento giuridico di base volto alla doverosa applicabilità di leggi europee già esistenti – anche nei confronti degli altri *Internet Service Provider* americani (Microsoft e Yahoo!).

E di riportare la Rete, nonostante i progetti militari legati alle sue origini[31], al centro di un pacifico dibattito culturale e giuridico dove i veri nodi della questione vengano finalmente affrontati.

3. La legislazione europea a protezione dei dati personali come l'*Habeas Corpus* della moderna era cibernetica[32]

In un diffuso approccio alle questioni relative ai rapporti tra Diritto ed Internet, c'è sempre qualcuno che è solito additare il tentativo di applicare vecchie norme a realtà nuove.

condotta che si colloca cronologicamente in un momento successivo al depauperamento, giuridicamente 'fuori dal caso di concorso', ma causalmente collegata al danno lamentato dai correntisti".

[29] Cfr. F. CELLA, *La trasparenza di Google* (23.6.2009), in *http://vitadigitale.corriere.it/2009/06/la_trasparenza_di_google.html:* "*il processo, in molti sensi unico nel suo genere a livello mondiale, è seguito con grande interesse anche da molti media americani: si tratta infatti di stabilire la responsabilità di chi ospita contenuti sul Web, o semplificando – come titola oggi un'agenzia della Associated Press – se nel Web debba prevalere il concetto di libertà oppure di responsabilità, legata a un maggiore controllo di quanto va online. Così diversi giornali italiani e statunitensi, tra cui il New York Times e il Wall Street Journal, avevano chiesto al giudice Magi la possibilità che l'udienza fosse pubblica. Ma le difese dei quattro imputati di Google si sono opposte e dunque il processo proseguirà a porte chiuse. 'Dont'be evil' è da sempre il motto dell'azienda di Mountain View. E forse a questa frase, involontariamente, ha voluto riferirsi il pubblico ministero Alfredo Robledo, che con il collega Francesco Cajani si era detto favorevole all'evenienza delle porte aperte, con il commento ironico seguito alla chiusura dell'aula ai giornalisti: 'Prendiamo atto della trasparenza di Google'* ".

[30] Tra i tanti commenti apparsi sul web, se ne riportano due molto approfonditi, sia pure radicalmente contrastanti nelle loro conclusioni: il *post* di *Eurolegal.it* del 15.4.2010, ore 22.31, *in http://blog.quintarelli.it/blog/2010/04/sentenza-google-vividown.html;* G. SARTOR-M. VIOLA DE AZEVEDO CUNHA, *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, in *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604411.*

[31] La c.d. ARPANET (*Advanced Research Projects Agency Network* ossia "Rete dell'Agenzia dei progetti di ricerca avanzata"), venne studiata e realizzata nel 1969 dal DARPA, l'agenzia del Dipartimento della Difesa degli Stati Uniti responsabile per lo sviluppo di nuove tecnologie ad uso militare. Dall'evoluzione di tale progetto nascerà, negli anni '80, la rete Internet come tutti noi la conosciamo.

[32] Viene qui riproposta (e fino al par. 5.4), in maniera sintetica ma dando volutamente ampio spazio alla rassegna dottrinale e giurisprudenziale, l'impostazione giuridica portata all'attenzione del Tribunale di Milano nel caso Google Video nelle due memorie depositate agli atti del processo di primo grado, redatte assieme al contitolare del procedimento penale Alfredo Robledo (Procuratore Aggiunto, coordinatore per i procedimenti relativi ai reati commessi in danno di enti pubblici, dello Stato e dell'Unione Europea) d'intesa con il Procuratore Aggiunto Corrado Carnevali.

Eppure mai come nel caso della normativa in materia di protezione dei dati personali il discorso è proprio il contrario: si tratta infatti di un complesso di disposizioni che già dalle origini di Internet avevano ben in mente l'evolversi della Rete, intesa nel senso prima ricordato ossia come un insieme di elaboratori elettronici tra loro interconnessi.

Ed infatti "*la novità fondamentale introdotta dal computer consiste non tanto nell'archiviazione di masse enormi di notizie, ma nell'accesso e circolazione rapidissima di tutti i dati memorizzati, l'interconnessione tra sistemi, l'aggregazione e combinazione in modi diversi delle notizie, quindi, in definitiva, nella possibilità di trasformare le informazioni disperse in informazione organizzata*" [33].

L'esigenza di trovare un punto di equilibrio tra interesse all'elaborazione delle informazioni e quello di salvaguardare gli spazi di libertà della persona ha sollecitato i legislatori europei, fin dagli anni '70, a codificare normative volte a disciplinare la costituzione e la gestione delle banche dati.

In tale ottica si poneva la Convenzione 108 del Consiglio d'Europa (aperta alla firma a Strasburgo nel 1981) sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale [34] che, all'art. 1, così ne individuava lo scopo:

> "… garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ('protezione dei dati')".

Con il passare del tempo e la progressiva espansione dell'informatizzazione nella società, tuttavia lo scenario cambia radicalmente: nel nuovo sistema normativo, cristallizzatosi nella dir. 46/95/CE [35] e successivamente – per quanto riguarda l'esperienza italiana – nella legge n. 675 del 1996 e successive modifiche (d.lgs. n. 467 del 2001 fino al d.lgs. n. 196 del 2003, d'ora in poi Codice privacy), "*il fenomeno delle banche dati perde di centralità, per inquadrarsi nella generale problematica del trattamento delle informazioni personali. I dati riguardanti una persona identificata o identificabile sono tutelati indipendentemente dal fatto che siano contenuti o destinati a figurare in un archivio, ciò che conta è il trattamento, ossia l'intervento su dati di una o più operazioni condotte con o senza* [36] *l'ausilio di mezzi elettronici o automatizzati*" [37].

---

[33] L. LAMBO, *La disciplina sul trattamento dei dati personali: profili esegetici e comparativistici delle definizioni,* in AA.VV., *Diritto alla riservatezza e circolazione dei dati*, a cura di R. PARDOLESI, Milano, 2003, p. 63: l'autore richiama sul punto, tra gli altri, il significativo scritto di S. RODOTÀ del 1973 dal titolo *Elaboratori elettronici e controllo sociale.*

[34] Testo reperibile su *http://conventions.coe.int/Treaty/ita/Treaties/Html/108.htm*; Convenzione ratificata con legge 21 febbraio 1989, n. 98.

[35] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in *G.U.* 23 novembre 1995, n. L 281). Il testo in italiano è reperibile su *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:IT:HTML.*

[36] Si noti come la Convenzione 108 del Consiglio d'Europa ignorava di disciplinare le informazioni gestite (anche o esclusivamente) con procedure manuali, e questo comportava un significativo pericolo di elusione delle norme ivi previste. In tal senso il considerando 27 della direttiva 95/46/CE. Cfr. inoltre A. GIANNACCARI, *L'ambito di applicazione della legge, l'importazione e l'esportazione dei dati personali*, in AA.VV., *Diritto alla riservatezza e circolazione dei dati*, a cura di R. PARDOLESI, Milano, 2003, p. 154.

[37] L. LAMBO, *La disciplina sul trattamento*, cit., p. 67. L'autore richiama sul punto G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 147; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 586.

Anche perché "*le stesse nozioni di archivio o di banche dati tendono a diventare insufficienti ed obsolete in un mondo in cui l'impetuoso svolgersi e dispiegarsi delle tecnologie interattive e delle reti di comunicazione – si pensi solamente ad Internet – stanno travalicando le aspettative dei loro stessi epigoni. Incentrare, allora, la tutela della persona su un concetto di difficile definizione e connotato da un elevato tasso di obsolescenza sarebbe stata probabilmente la scelta sbagliata*" [38].

Con la legge n. 675 del 1996 si "*introduce nel nostro ordinamento per la prima volta una disciplina completa ed organica dei dati personali … considera(ti) come oggetto di un diritto assoluto, esperibile cioè nei confronti di chiunque. … Oggetto del diritto non è l'attribuzione di un potere esclusivo di utilizzazione e di disposizione dei dati personali da parte del soggetto titolare. Questi non potrebbe impedire l'utilizzazione dei dati personali da parte della collettività per la necessaria funzione individuatrice che i dati personali hanno e che perderebbero una volta che fosse impedita la comunicazione da parte di altri. Il consenso da parte del titolare … si riferisce non all'utilizzazione dei dati personali ma al loro trattamento… Il diritto sui dati personali deve essere invece considerato come un vero e proprio diritto della personalità. La difesa dell'individuo nei confronti del potere informatico, l'habeas corpus della moderna era cibernetica*" [39].

3.1. 1884-2004: dalla circolazione delle fotografie istantanee alle immagini digitali sul Web

Se dunque alla fine del 1800 fu proprio l'avvento delle fotografie istantanee della Eastman Kodak Company ad ispirare gli Avvocati Warren e Brandeis nell'invocare l'introduzione nell'ordinamento statunitense di un nuovo diritto (*The Right to Privacy* [40]), un secolo dopo lo sviluppo della Rete e il correlato fenomeno della *digitalizzazione dell'io* [41] non ha trovato impreparato l'ordinamento europeo.

Ed è la stessa Legge a protezione dei dati personali che, in un'ottica di maggior tutela, vuole espressamente evitare, ai fini della sua applicabilità, l'aggancio al luogo di allocazione dei dati: ed in effetti "*quello della legge applicabile è stata da subito … avvertito quale uno dei punti nodali dell'*effettività *ed efficacia di una legge sul trattamento dei dati*" [42].

---

[38] A. GIANNACCARI, *L'ambito di applicazione della legge*, cit., pp. 153-154: l'autore in nota riporta altresì i lavori parlamentari, dai quali si trae ulteriore riscontro di quanto finora sostenuto. In particolare: "*(c)ome previsto dalla Direttiva, ed in sintonia con le leggi di altri Paesi, la legge dovrà avere come oggetto il "trattamento" dei dati e non i dati in sé e per sé, ovvero la 'banca dati'. Per quanto riguarda i trattamenti automatizzati, quindi, non ha importanza se sussista o meno, in concreto, una banca dati*".

[39] E. GIANNANTONIO, *Commento art. 1, comma 1*, in E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH, *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1997, p. 2.

[40] Il saggio *The Right to Privacy*, apparso sull'*Harvard Law Review* (vol. IV, n. 5) del 15 dicembre 1890, è reperibile in Internet su *http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2. html.*

[41] "*Google ha fatto apparire la Terra come un posto accogliente, ma in questo modo ha anche reso la nostra presenza più visibile, volenti o nolenti. Abbiamo iniziato a capire, se pure in ritardo, che la distanza serve a proteggere il nostro anonimato. All'interno del circoscritto mondo virtuale in cui tutti possono osservare ogni luogo e dove, se le fotografie sono associate alle mappe, ogni abitante diventa sempre più visibile agli occhi di un numero crescente di persone, la sensazione di privacy di un individuo viene meno con la stessa rapidità con cui il nostro pianeta sembra diventare sempre più piccolo*": R. STROSS, *Pianeta Google. Quanto manca alla conquista totale?*, Milano, 2009 (titolo originale: "*Planet Google*", 2008).

[42] S. SICA, in AA.VV., *La nuova disciplina della privacy*, a cura di S. SICA-P. STANZIONE, Firenze, 2004, p. 34.

La Convenzione del Consiglio d'Europa del 1981 si limitava a determinare, all'art. 3, il proprio campo di applicazione *ratione materiae,* nonostante i redattori avessero preso in considerazione – in sede di lavori preliminari[43] – l'ipotesi che, in alcuni casi aventi connotazioni di extra-territorialità, potesse verificarsi il problema della legge concretamente applicabile.

La dir. 46/95/CE contiene invece una espressa previsione in materia di ambito di applicazione, frutto di una precisa scelta di campo maturata durante i lavori preparatori[44].

In un primo momento, nel dichiarato tentativo di evitare il cumulo di legge applicabili, si prevedeva come ogni Stato membro applicasse le disposizioni della direttiva a tutti gli archivi di dati "situati" sul proprio territorio.

"*Durante i successivi approfondimenti emerse peraltro con chiarezza che il criterio del luogo di localizzazione dell'archivio, ai fini della determinazione della legge applicabile, non risultasse più al passo con la tecnologia: con l'avvento imperioso delle reti di comunicazione, infatti, le banche dati risultavano sempre più trattate in rete e risultavano sempre meno 'residenti' e meno collegate, invece, al luogo ove era installato il relativo mainframe*[45]*. Da ciò, ovviamente, ne conseguiva che la localizzazione territoriale degli archivi di dati personali diventava sempre più difficile da determinare, se non addirittura impossibile, laddove la banche dei dati personali fossero state multi-localizzate in più Stati, oppure tra questi suddivise, ovvero, ancora, qualora risultassero in continuo trasferimento. Si abbandonò dunque il luogo di localizzazione dell'archivio e si passò, da un criterio di collegamento fattuale ad uno giuridico ...: il luogo in cui risiede il responsabile ... del trattamento dei dati personali ... Onde evitare elusioni, si prevedeva inoltre che, qualora in responsabile del trattamento non risiedesse nel territorio della Comunità, ma in tale territorio ricorresse a strumenti [ivi] situati a fini di trattamento (ad es., con terminali o questionari), allora il diritto applicabile doveva essere quello dello Stato sul cui territorio erano localizzati detti strumenti ... Anche tale impostazione, peraltro, risultò non andare esente da critiche e fu necessario precisare i limiti e la portata, sottoponendo il trattamento di dati personali alla legge dello Stato di stabilimento del responsabile*"[46].

Si perviene così, alla luce del Considerando 20[47], al testo definitivo dell'art. 4 della dir. 95/46/CE[48].

---

[43] Cfr. l'*Explanatory report* (Rapporto esplicativo) reperibile in Internet *su http://conventions.coe.int/Treaty/EN/Reports/Html/108.htm.*

[44] Sul punto P. CERINA, *Commento art. 2*, in E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH, *La tutela dei dati personali,* cit., p. 20.

[45] *Mainframe* (o sistemi centrali) è il nome usato per indicare i computer utilizzati per applicazioni critiche soprattutto da grandi aziende e istituzioni, tipicamente per elaborare con alte prestazioni ed alta affidabilità grandi moli di dati.

[46] P. CERINA, *Commento art. 2*, cit., pp. 21-22.

[47] Se ne riporta il testo, per facilità di lettura: "*(20) considerando che la tutela delle persone prevista dalla presente direttiva non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; che, in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva*".

[48] Se ne riporta il testo, per facilità di lettura: "*Articolo 4 – Diritto nazionale applicabile. 1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:*

a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;

Con le modifiche apportate dal d.lgs. n. 467 del 2001 alla legge n. 675 del 1996, anche il legislatore italiano ha pienamente attuato tali criteri volti ad individuare il campo di applicazione della normativa: questo proprio "*nella considerazione della inadeguatezza della precedente scelta*[49]*, soprattutto se rapportata a nuovi strumenti di circolazione – si pensi ad Internet e alla facilità con cui i dati possono circolare attraverso le reti telematiche*"[50].

Ed infatti sul significato dell'art. 5 d.lgs. n. 196 del 2003 – c.d. Codice Privacy (norma[51] che riproduce l'analoga disposizione previgente: art. 2 legge n. 675 del 1996[52]) così è stato autorevolmente sostenuto: "*La ratio della disposizione è evidentemente di assicurare che ogni trattamento con effetto nel territorio dello Stato sia disciplinato dal Codice*" e, dunque, "*costituisce un'efficace barriera ad operazioni di elusione della normativa in materia di riservatezza, attuabili semplicemente trasferendo i server all'estero*"[53].

---

b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;

c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.

2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento".

Per un ulteriore approfondimento sul punto, si rinvia al "*Documento di lavoro sulla determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento dei dati personali su Internet da parte di siti Web non stabiliti nell'UE*" adottato il 30 maggio 2002 dal WP 29 (Gruppo per la tutela dei dati personali – art. 29) ed, in particolare, al par. 2 ("Articolo 4 della direttiva 95/46/CE in merito al diritto applicabile"): *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_it.pdf.*

[49] Ovvero quella del mero principio di territorialità di cui all'art. 2 legge n. 675 del 1996: "*la legge nazionale si applica a chiunque compia operazioni di trattamento sul territorio dello Stato*".

[50] S.M. MELONI, *Gli ambiti di applicazione del codice sulla protezione dei dati personali*, in AA.VV., *Il Codice del trattamento dei dati personali*, a cura di V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, Torino, 2007, p. 53.

[51] Se ne riporta il testo per facilità di lettura: "*Art. 5 – Oggetto ed ambito di applicazione:*

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31".

[52] Se ne riporta il testo per facilità di lettura: "*Art. 2. Ambito di applicazione.*

1. La presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato.

1-bis. La presente legge si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, mezzi situati nel territorio dello Stato anche diversi da quelli elettronici o comunque automatizzati, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.

1-ter. Nei casi di cui al comma 1-bis il titolare stabilito nel territorio di un Paese non appartenente all'Unione europea deve designare ai fini dell'applicazione della presente legge un proprio rappresentante stabilito nel territorio dello Stato".

(Commi 1-*bis* e 1-*ter* aggiunti dall'art. 1, comma 2, d.lgs. 28 dicembre 2001, n. 467).

[53] AA.VV., *Codice in materia di protezione dei dati personali*, a cura di G. CASSANO-S. FADDA, Milano, 2004, p. 59.

E dunque si comprende appieno la posizione espressa nel 2007 da Peter Schaar quale Presidente dell'*Article 29 Data Protection Working Party*[54] (Wp29) nella sua lettera aperta a Google[55]:

> "Although Google's headquarters are based in the United States, Google is under legal obligation to comply with European laws, in particular privacy laws, as Google's service are provided to European citizens and it maintains data processing activities in Europe, especially the processing of personal data that takes place at its European center".

Nella risposta che Peter Fleisher (*Google Global Privacy Counsel*) fornisce alcune settimane dopo (10 giugno 2007), significativamente si legge[56]:

> "Google is a U.S. company and we respect U.S. laws — but we are also a global company, doing business across Europe and across the world, and we recognize the need to respect the laws of the countries in which we do business".

E tuttavia lo stesso Fleisher, in un importante Convegno all'Università Statale di Milano nel febbraio del 2008[57], sembra aver dimenticato la parte finale di quella frase ("*siamo consapevoli di dover rispettare le leggi degli Stati nei quali svolgiamo una attività economica*") da lui stesso scritta.

Così infatti il resoconto tratto dal *blog* di Guglielmo Troiano[58]:

> "Quello della privacy è uno dei temi scottanti del web non tanto per la violazione dei suoi principi, quanto per la mancanza di armonizzazione delle normative nazionali. Ed una società come Google, che opera in 160 paesi nel Mondo, lo sa bene.
>
> Peter Fleischer ha affermato che, per l'azienda di Mountain View, è impossibile riuscire ad operare a livello globale rispettando in pieno 160 diverse legislazioni. Il motore di ricerca, ma anche tutti gli altri servizi offerti, opera tecnicamente allo stesso modo in tutti i paesi in

[54] Trattasi del Gruppo europeo per la tutela dei dati personali, costituito in virtù dell'art. 29 dir. 95/46/CE.

[55] Lettera di Peter Schaar a Peter Fleischer (Google) datata 16 maggio 2007. Il documento è reperibile in Internet: *http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf.*

[56] *http://64.233.179.110/blog_resources/Google_response_Working_Party_06_2007.pdf.*

[57] Sul punto la memoria dei Pubblici Ministeri, richiamata a p. 53 della sentenza del Tribunale di Milano, così significativamente precisa: "*Agli organi di stampa, proprio in contemporanea con la prima udienza del processo (3.2.2009), FLEISHER dichiarerà di essere stato accerchiato da 5 persone mentre si recava ad un Convegno presso l'Università di Milano (dovendo intervenire come relatore insieme al Segretario Generale dell'Autorità Garante per la protezione dei dati personali) e portato davanti al Pubblico Ministero con la forza (https://www.privacyassociation.org/index.php?option=com_content&task=view&id=1745&Itemid=228), tanto da ingenerare nella opinione pubblica l'idea che fosse stato addirittura arrestato (come riportato dal Guardian e da altre testate estere: http://www.guardian.co.uk/technology/2009/feb/03/google-trial-privacy). Come siano andati realmente i fatti lo indicano le annotazioni di PG del 22 e 23.1.2008 (che danno atto di averlo cercato invano nei giorni precedenti nei migliori hotels di Milano nonché nelle liste di attesa degli aerei per Milano: XI, 210 ss), e il fatto stesso che la convocazione notificatagli era ab origine fissata una ora dopo la fine del Convegno (convocazione peraltro spostata, su invito dei difensori, alla giornata successiva*: XI, 214)". Versione ribadita anche in seguito dalle pagine del suo autorevole *blog* (*http://peterfleischer.blogspot.com/2009/12/on-side walk-in-milan.html*), in perfetta sincronia con le udienze milanesi. Così il 23.11.2009 (due giorni prima della Requisitoria dei PM): *http://peterfleischer.blogspot.com/2009/11/on-trial-in-italy.html*. Allo stesso modo il giorno successivo, rappresentando altresì di aver ricevuto "*chiare istruzioni dal mio avvocato esterno di non mettere per nulla piede in Italia*": *http://peterfleischer.blogspot.com/2009/11/ciao-italia.html.*

[58] *http://troiano.org/?p=38.*

cui Google è presente. Anche se, è cosa nota, attraverso la profilazione degli indirizzi IP, un utente situato in Italia non può utilizzare *google.com*.

Che Google ce la metta tutta per rispettare la legge è fuori di dubbio; al tempo stesso è lecito chiedersi (come ha fatto un esimio avvocato milanese tra il pubblico): ma alla fine, Google che legge applica? Tutte e nessuna in particolare, sembra essere stata la risposta.

La realtà è che Google mostra una sua lungimirante visione quando spinge l'opinione pubblica all'adozione di una normativa globale sulla privacy (in seno ad organi istituzionali di pari portata), ma si è ancora molto, forse troppo, lontani da un tale sogno. In itinere, il diritto vigente in Italia resta senz'altro il c.d. codice della privacy che, armonizzato con le normative europee ed i pochi trattati internazionali in materia, Google deve necessariamente tenere in considerazione".

Alla fine, quindi, quali Leggi vengono applicate?

Di sicuro la sentenza del Tribunale di Milano è chiara nell'affermare che si applicano le leggi italiane, dal momento che quelle dello Stato della California hanno un ambito territoriale ben delimitato …

4. *Business* vs. persona: un doveroso bilanciamento di interessi (troppo spesso) contrapposti

In un articolo pubblicato su *Guida al Diritto*[59], apparso all'approssimarsi della prima udienza del processo Google Video, veniva autorevolmente sostenuto (al fine di escludere l'ipotesi di una responsabilità penale[60]) come

> "Il d.lgs. n. 70 del 2003 che trova applicazione anche in materia penale, stabilisce infatti che gli intermediari di internet sono responsabili solo se partecipano attivamente alla diffusione dell'informazione, selezionando i contenuti o i destinatari".

È tuttavia noto come il richiamato decreto legislativo, volto a dare "*attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico*", abbia un preciso campo di applicazione così come espressamente indicato dal combinato disposto dei due commi dell'art. 1:

> "1. Il presente decreto è diretto a promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico.
>
> 2. Non rientrano nel campo di applicazione del presente decreto:
>
> […]

[59] G.M. RICCIO, *Solo la neutralità degli internet provider può salvare la rete da un "effetto gelo"*, in *Guida dir.*, 2008, 48, p. 107.

[60] Allo stesso modo, ma in termini dubitativi, un articolo apparso all'inizio delle indagini: F. ABRUZZO, *Video choc girato ai danni di un giovane disabile. Una direttiva comunitaria potrebbe salvare Google* (28 novembre 2006), in *http://www.interlex.it/regole/abruzzo12.htm*, ove si legge: "*Quali sono le norme applicabili? La Procura di Milano sembra orientata ad attribuire una responsabilità a Google (inquadrato come un internet provider) per fatti commessi da terzi in base alle norme sulla responsabilità del direttore di una testata giornalistica ed in particolare all'art. 57 c.p., equiparando il gestore di un sito internet ad un direttore responsabile e attribuendogli l'obbligo di verificare la liceità del materiale pubblicato sul proprio server, compreso quello inviato da terzi ... Il Pm di Milano, però, dovrà valutare l'incidenza di una direttiva comunitaria, che sembra scagionare Google ... Google in questo caso svolge un'attività di semplice 'ospitalità' del filmato incriminato*".

b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675, e al decreto legislativo 13 maggio 1998, n. 171, e successive modificazioni; [...]".

Circostanza questa, in linea con l'art. 1 comma 5 lett. b della dir. 2000/31/CE[61], fin da subito messa in evidenza da autorevoli autori, tra i quali il Prof. Zeno-Zencovich in un noto scritto[62], ove si legge: "*La direttiva sul commercio elettronico fa espressamente salva la disciplina di tutela dei dati personali e, dunque, dobbiamo ritenere che essa non possa scalfire in alcun modo tutte quelle ipotesi di illeciti, sia civili che penali, contenuti nella direttiva 1995/46/CE, del 24 ottobre, e poi recepite dalla L. 31 dicembre 1996, n. 675, che sanzionano il trattamento non corretto dei dati*". Ed anzi, lo stesso Professore evidenzia "*una certa antinomia fra la direttiva sul commercio elettronico e la disciplina a tutela dei dati personali*", rappresentando correttamente – come del resto sostenuto dalla Procura di Milano nel caso Google Video – come "*nell'attività di commercio elettronico è immanente una attività di trattamento dei dati*".

Allo stesso modo, peraltro, tutti i commenti dottrinali sul punto[63], in linea con la Relazione Governativa[64]: "*... con il secondo comma ... vengono esclusi dal campo di applicazione della normativa in esame, determinate materie: ... le questioni relative alla tutela dei diritti e delle libertà fondamentali delle persone giuridiche e, in particolare, del diritto alla vita privata, con specifico riguardo al trattamento dei dati personali nel settore delle telecomunicazioni ...*".

Del resto il senso della disposizione che qui si commenta trova un diretto aggancio costituzionale nell'art. 41, ove si sancisce che la libertà di iniziativa economica "*non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana*"[65].

Quella dignità umana che è richiamata proprio dall'art. 17 Codice Privacy con una norma di chiusura che ben si attagliava al caso in esame, essendo evidente fin *ab origine* come il ser-

[61] Se ne riporta per facilità di lettura il testo: "*Articolo 1 – Obiettivi e campo di applicazione.*

1. La presente direttiva mira a contribuire al buon funzionamento del mercato garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri. […]

4. La presente direttiva non introduce norme supplementari di diritto internazionale privato, né tratta delle competenze degli organi giurisdizionali.5. La presente direttiva non si applica:

a) al settore tributario,

b) alle questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE […] ".

[62] *Profili attivi e passivi della responsabilità dell'utente in Internet*, in AA.VV., *La tutela del navigatore in Internet*, 2002, pp. 142-143.

[63] Cfr. tra gli altri C. ROSSELLO, *Commercio elettronico*, Milano, 2007, p. 73: "*il capoverso dell'art. 1 d.lgs. 70/2003 individua una serie di esclusioni, ovvero materie rispetto alle quali opera la disciplina di settore e non quella del commercio elettronico contenuta nel decreto*".

[64] In C. ROSSELLO-E. TOSI, *Commercio elettronico, documento informatico e firma digitale. La nuova disciplina*, Torino, 2003, p. 609 ss.

[65] Nello stesso senso L. PICOTTI, *Fondamento e limiti dela responsabilità penale dei Service-Providers in Internet*, in *Dir. pen. e proc.*, 1999, 3, p. 381: "*un atteggiamento così fortemente restrittivo, nel delineare e circoscrivere ab origine l'eventuale sfera di responsabilità penale dei Providers, non appare condivisibile, oltre che per le ragioni tecnico giuridiche che si esporranno, anche perché appare troppo sbilanciato, su di un piano di valutazione generale, a favore dell'esigenza di garantire le migliori e più libere condizioni d'esercizio della loro pur importante attività, unitamente ai fondamentali diritti di comunicazione e manifestazione del pensiero dei consociati: sacrificando, però, le contrapposte ed altrettanto esigenze di tutela di quei beni giuridici fondamentali, che ne costituiscono legittimo limite*".

vizio di Google Video – per come concepito, ovvero lasciato al libero accesso di chiunque [66] – presentava "*rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare*".

Ma ancora una volta i primi commentatori del caso Google Video [67] – forse distratti dal grido di allarme di quell'iniziale comunicato stampa di Google Italy [68] – si lanciarono in affrettate conclusioni:

> "Ciò che lascia perplessi, però, non è solo il modo in cui si vorrebbe applicare la normativa vigente. Il punto cruciale della questione è altro. Il caso di cui parliamo è gravissimo: un ragazzino disabile è stato malmenato, deriso, umiliato, da una banda di coetanei. È una vicenda che dovrebbe indurre a riflettere, e seriamente, perché è sintomatica dei disagi degli adolescenti.
>
> Invece, paradossalmente, sul banco degli imputati finisce il gestore di un servizio informatico. Viene provocatoriamente da domandarsi il perché non sia stato coinvolto anche il produttore del telefono cellulare con cui è stato girato il video. La situazione, però, non consente di cedere all'ironia: dopo oltre dieci anni di infinite discussioni sulle responsabilità in internet, si torna a parlare di applicabilità della disciplina prevista per gli editori o si cerca rifugio negli incerti confini della responsabilità oggettiva. Non si tratta di difendere Google, sia chiaro. Si tratta di difendere il principio della neutralità degli internet provider e di evitare che si ingeneri un *chilling effect*, un effetto raffreddamento che possa colpire tutti i soggetti che operano in rete".

4.1. Il fatto storico oggetto del processo, alla luce del quale far discendere il regime giuridico

Nella documentazione promozionale (ovvero rivolta agli inserzionisti più importanti) di Google Video ritrovata dalla Guardia di Finanza di Milano – Gruppo Pronto Impiego presso la sede di Google Italy s.r.l., era testualmente [69] previsto – fin dalla prima pagina – come "*la missione di Google video*" fosse quella di "*monetizzare ogni video presente nel nostro indice*" [70].

---

[66] Sul documento "*Google video: preliminary analysis of Italian market peculiarities*" nonché sugli elementi di prova ritrovati a seguito della ispezione dei sistemi informatici di Google Italy s.r.l. cfr. quanto richiamato nella sentenza del Tribunale di Milano, p. 18 ss.

[67] Cfr. l'autorevole saggio significativamente intitolato "Processo alla Rete" di G. SCORZA reperibile su *http://www.guidoscorza.it/wp-content/uploads/2009/01/processo-alla-rete-free-version-completo.pdf* e che si apre proprio con il paragrafo intitolato "*Non chiamiamolo il 'Caso Google'* " (in riferimento alla notizia della chiusura della indagine della Procura di Milano). In relazione alla nota di commento al decreto di citazione diretta in giudizio (a firma di G. CORRIAS LUCENTE ed anch'essa apparsa prima della celebrazione del dibattimento, in *Dir. inf. e informatica*, 2009, 1, p. 89 ss.) cfr. L. BONESCHI, *Nota del direttore responsabile. La Procura della Repubblica di Milano, un errore della Rivista e una discussione necessaria*, in *Dir. inf. e informatica*, 2009, 4-5, p. 735 ss.

[68] Cfr. nota 6.

[69] A fronte di simili evidenze documentali ritrovate presso gli uffici di Milano, corso Europa 2 (in uno con le dichiarazioni dei dipendenti di Google Italy raccolte durante le indagini), ancora di recente Stefano Maruzzi, nella sua qualità di "amministratore delegato di Google Italia", dichiarava ai *media*: "*Il punto è che il modello di business di Google Video era molto diverso da quello di YouTube. Sulla vecchia piattaforma non c'era monetizzazione, non c'era pubblicità … nel 2006 non c'era modo di guadagnare dai video. Crea imbarazzo sentire accuse del genere quando il prodotto aveva queste caratteristiche*": D. LEPIDO, *La crescita passa da You Tube*, in *Il Sole 24 Ore*, 26 marzo 2010, p. 30.

[70] Cfr. p. 62 ss della sentenza 24 febbraio 2010, n. 1972.

Da questo come da numerosi altri elementi raccolti durante le indagini era dunque emerso come la concreta operatività di Google video doveva necessariamente essere messa in relazione al servizio *Adwords* [71] (da *Advertising Words*, ossia letteralmente: parole pubblicitarie).

Le campagne pubblicitarie per i clienti più importanti, come ammesso dagli stessi dipendenti di Google Italy (che peraltro sono organizzati proprio per i diversi settori commerciali), erano effettuate proprio presso la sede di Milano, attraverso la progettazione della stesse ed il materiale inserimento delle parole chiave, per il tramite delle postazioni informatiche collegate mediante una VPN [72] con i *server* irlandesi, nel sistema *Adwords*.

Non è infatti più un mistero [73] che le sedi europee di Google nascono e giustificano il loro

[71] "*AdWords è il programma pubblicitario di Google. Esso consente di creare annunci semplici ed efficaci e visualizzarli per gli utenti che stanno già effettuando ricerche online delle informazioni correlate alla vostra attività. Come si fa quindi a visualizzare gli annunci solo per gli utenti più pertinenti? La risposta è data dalla pubblicità basata sulle parole chiave. Quando un utente visita Google e inserisce termini di ricerca — come ad esempio 'buone chitarre per principianti' – Google visualizza una serie di risultati di ricerca quali link ad articoli contenenti consigli per l'acquisto di chitarre o siti web dedicati ai musicisti novizi. Visualizza inoltre annunci AdWords collegati ad aziende online che vendono chitarre, lezioni di musica o altri prodotti e servizi correlati alla ricerca. Ad esempio, supponete di possedere un negozio di musica con una vasta selezione di chitarre. Potete effettuare l'iscrizione per un account AdWords e creare annunci relativi alle chitarre per principianti disponibili nel vostro magazzino. Per ognuno degli annunci, è possibile selezionare parole chiave (parole singole o frasi correlate al messaggio dell'annuncio) come 'chitarre di livello base' o 'chitarre per principianti'. Quando attivate l'account, gli annunci sono idonei ad essere visualizzati. Ciò significa che AdWords ricerca costantemente termini di ricerca correlati alle parole chiave selezionate, quindi visualizza gli annunci per utenti molto mirati. In breve, gli annunci sono rivolti direttamente a un pubblico che sta già cercando il prodotto o il servizio da voi offerto*": cfr. *http://www.google.com/intl/it/adwords/learningcenter/print-18910.html.*

[72] *Virtual Private Network*, ossia "Rete Virtuale Privata".

[73] Fece clamore, all'epoca della quotazione di Google Inc. in Borsa (agosto 2004), lo studio condotto dai *Pew Charitable Trusts* (una associazione indipendente non governativa americana) che mise in evidenza come "*la maggior parte degli utenti della rete non si rendevano neanche conto del fatto che i risultati delle ricerche di Google contenessero link pubblicitari*" e, più precisamente, "*il 62 per cento degli utenti di Google non compren-*

essere proprio per questo: è evidente come il grosso degli inserzionisti debba essere ricercato e "gestito" sul territorio**.** Per tali motivi, come peraltro ben espresso in una massima del *Tribunal de grande instance* di Parigi [74], non può dirsi irrilevante [75] il ruolo delle sedi territoriali di Google, proprio per l'intreccio di relazioni commerciali che queste determinano e le consulenze pubblicitarie che costituiscono la parte più rilevante della attività anche di Google Italy.

Alla luce di tali evidenze investigative, così concludeva sul punto la memoria dei Pubblici Ministeri depositata il 25 novembre 2009 (p. 115):

---

deva la differenza tra i risultati gratuiti delle ricerche e gli annunci pubblicitari mostrati alla loro destra. Se le persone si fossero rese conto che i piccoli riquadri testuali erano inserzioni pubblicitarie a pagamento, avrebbero cliccato su di essi con minor frequenza, a detta degli esperti di marketing". E in effetti si parla volontariamente di "*link sponsorizzati*" ed anche questa era "*la ragione principale per la quale persone anche molto intelligenti non riuscivano a capire come la società facesse soldi*": così D.VISE-M. MALSEED, *Google Story*, Milano, 2006, p. 159. Sul punto cfr. *The Economist, Gran Bretagna*, in *Internazionale*, 718, 9.11.2007: "*Il dilemma di Google. È l'azienda più importante della rete, ma sostiene che il suo obiettivo non è far soldi … l'azienda, che prima di entrare in borsa nel 2004 aveva come slogan* Don't be evil *(non essere malvagio), si considera una forza del bene in tutto il mondo, al punto di sfidare la logica commerciale. Più volte i suoi fondatori Larry Page e Sergej Brin e l'amministratore delegato Eric Schmidt hanno dichiarato esplicitamente che il loro scopo principale non è ottenere il massimo profitto, ma migliorare il mondo. Discorsi del genere fanno venire i brividi*".

[74] "*Nonostante la commercializzazione del sistema Adwords è localizzata in Irlanda per motivi economici o fiscali e nonostante il fatto che il nome del dominio, i marchi, i server e la gestione materiale del sito google.fr facciano capo alla società Google Inc, tale circostanza non può escludere la responsabilità della società Google France, che è l'unica società del gruppo ad intervenire legalmente in Francia e su questo territorio compare e si comporta come responsabile dell'attività pubblicitaria dell'omonimo sito internet Google France*": *Tribunal de grande instance de Paris 3ème chambre, 3ème section Jugement du 07 janvier 2009 (Voyageurs du Monde, Terres d'Aventure / Google et autres)*, in *http://www.legalis.net/jurisprudence-decision.php3?id_article=2532.*

[75] Se la Difesa aveva avuto modo di indicare al Tribunale di Milano diverse decisioni dell'Autorità Garante che, nel tempo, avevano attestato l'inapplicabilità del d.lgs. n. 196 del 2003 (essendo il trattamento operato presso i *server* americani), l'Accusa ha ribadito come le stesse, a parte la circostanza di riferirsi ad un diverso servizio (ossia al funzionamento del motore di ricerca), si siano sempre fondate su una ricostruzione dei fatti basata unicamente su autodichiarazioni provenienti da Google Italy. Si riportano quelle di Drummond e De Los Reyes, nella loro qualità di legali rappresentanti di Google Italy, nell'ambito del procedimento definito con decisione del 18. gennaio 2006:

"*… la società italiana Google Italy S.r.l. non ha il potere né la capacità di svolgere qualsiasi operazione tecnica sul motore di ricerca Internet denominato Google. … Google Italy S.r.l. non è fornitore di contenuti e/o servizi Internet e non impiega tecnici informatici presso i suoi uffici. In particolare …. Google Italy S.r.l.:*

1. non fornisce i servizi di ricerca internet disponibili tramite il motore di ricerca Google

2. non possiede e/o mantiene banche dati o siti web e non utilizza programmi allo scopo di collezionare informazioni, che è successivamente catalogato dal motore di ricerca denominato Google

3. non possiede e/o ha la capacità di accedere a qualsiasi equipaggiamento elettronico utilizzato per la fornitura di ricerca su internet tramite il motore di ricerca Google

4. non ha accesso all'indice del motore di ricerca denominato Google né ha il potere o la capacità per modificare e/o aggiornare tale indice

5. non ha il potere o la capacità per modificare, aggiornare e/o eliminare qualsiasi URL e/o astratto e/o copia nascosta delle pagine web alle quali il motore di ricerca Google connette".

Dichiarazioni peraltro, proprio in quel procedimento (all'esito del quale il Garante italiano aveva ritenuto di chiedere "*a Google america più tutele per gli utenti*": *http://www.garanteprivacy.it/garante/doc.jsp?ID=1267433*), introdotte nel giudizio di fronte all'Autorità a mezzo di procura alle liti falsa: ed infatti l'imputazione complessiva della Procura di Milano per il caso Google Video ricomprendeva (a carico di un diverso indagato) anche l'ipotesi di cui all'art. 168 d.lgs. 30 giugno 2003, n. 196 "*perché, in un atto successivamente esibito in un procedimento di fronte all'Autorità Garante per la protezione dei dati personali (procura speciale datata 14.11.2005 e depositata il 16.11.2005), dichiarava falsamente di essere – nel testo inglese – 'rappresentante debitamente autorizzato' e – nel testo in italiano – 'legale rappresentante' di Google Italy s.r.l., così radicando la legittimazione processuale della richiamata s.r.l. (resistente in giudizio) nella controversia Google Italy s.r.l. / C.O. (ricorso deciso con provvedimento del 18.1.2006)*" (fatti trasmessi per competenza territoriale a Roma, all'esito della decisione del Tribunale di Milano in data 21 aprile 2009).

"in relazione alla vicenda del video oggetto del presente procedimento, è stato effettuato un **trattamento illecito *ex* art. 167 d.lgs. 196/2003** (stante la violazione degli artt. 13 in relazione all'art. 23 comma 3, 26 e 17 Codice Privacy). Il dato personale (immagine) del soggetto raffigurato, con la sua immissione nel sistema di Google Video, è stato illecitamente *trattato* (sotto il profilo della violazione delle norme di legge contestate): è stato *raccolto* in tal modo (nonché *organizzato* **ai fini di sfruttamento economico tramite *messa a disposizione* in Internet e *diffusione* con relativa *comunicazione* a terzi)** perché così era stato deciso e voluto nell'ambito della logica di mercato di Google Italy s.r.l., e peraltro quanto successivamente accaduto era anche stato ragionevolmente previsto [76]. Come tutti i dati immessi nel sistema Google, quale effetto permanente della contestata condotta di illecito trattamento, fin dal primo giorno e nei due mesi di permanenza nel sistema Google Video lo stesso è stato altresì ***elaborato*** e ***utilizzato*** nell'ambito della attività economica relativa al servizio AdWords. E, alla fine, è diventato oggetto di dibattito pubblico, con relativa ulteriore diffusione (non solo prima della sua materiale rimozione ma anche dopo, con alcuni fotogrammi ripresi dalla stampa) ed enorme nocumento per le persona raffigurata (che, in relazione a quanto accaduto, ha presentato querela)".

5. Essere o non essere intermediari, questo è il problema

Per i motivi finora illustrati, nel caso Google Video la rilevanza di una Legge a protezione di diritti della persona appariva *ipso iure* prevalente rispetto a disposizioni dettate in materia di tutela del commercio elettronico.

Pur tuttavia, a fronte dell'impostazione difensiva contraria volta invece a sottolineare che "*la normativa sulla privacy e la normativa sul commercio elettronico, in realtà, costituiscono un quadro giuridico coerente e completo*" [77], è stato altresì affrontato dall'Accusa [78] – nelle due memorie depositate agli atti del processo – un ulteriore aspetto di non poca importanza, volto a verificare la pretesa applicabilità del regime giuridico di cui all'art. 16, comma 1 del già richiamato d.lgs. n. 70 del 2003 al caso in esame così come ricostruito alla fine del precedente paragrafo.

Per evitare confusioni concettuali, quando si parla di *Internet Service Provider* bisogna però fare alcune precisazioni terminologiche.

Se è vero che *Provider* (dal verbo inglese *to provide*) può essere definito in prima istanza come *colui che fornisce* (*un servizio attinente il Web*), è noto come nella realtà informatica (peraltro in continua evoluzione) si registrano diverse figure di *Provider*, tutte caratterizzate dalla natura del servizio fornito.

Anche se non esiste una classificazione "ufficiale", tradizionalmente si è soliti parlare di:

- ***Network provider*** = colui che si limita a fornire le infrastrutture di comunicazione;
- ***Access provider*** = colui che consente all'utente finale di collegarsi ad Internet;

[76] Cfr. p. 21 della sentenza n. 1972 del 2010, cit.

[77] Così il senso delle memorie difensive sul punto.

[78] Sicuramente poco informato sulle tesi dell'Accusa appare G. SCORZA che in data 28 febbraio 2010 così commenta in *http://www.youtube.com/watch?v=HQBOUP4CZvk*: "*Se c'è una certezza è che Google in relazione al servizio Google Video è un intermediario della comunicazione ... nel senso che diffonde contenuti creati e pubblicati dagli utenti ... in astratto si potrebbe discutere dell'applicabilità alla fattispecie della disciplina sul commercio elettronico o, piuttosto, della circostanza che Google sia uno degli specifici intermediari presi in considerazione da tale disciplina*". Per poi concludere, anche sul suo GBLOG: "*Ma nessuno di tali profili sembra aver affascinato l'accusa*": *http://www.guidoscorza.it/?p=1575*.

- ***Service provider*** = colui che offre all'utente di disporre di ulteriori servizi (es. *e-mail*) dopo che lo stesso abbia ottenuto la connessione;
- ***Host provider*** = colui che offre all'utente il mero spazio web del proprio *server* (affinché sia lo stesso utente a collocarvi i contenuti);
- ***Content provider*** = colui che è fornitore di contenuti.

A complicare notevolmente lo sforzo dell'interprete era ed è la circostanza che, come di fatto avviene, uno stesso *Provider* possa fornire più servizi: così comunemente si parla di *Internet Service Provider* laddove un soggetto fornisca all'utente non solo l'accesso ad Internet ma anche ulteriori servizi.

Sempre sotto il profilo terminologico, è stato ben osservato come la dir. 2000/31/CE [79] (recepita dal d.lgs. n. 70 del 2003) non faccia riferimento tanto agli *Internet Service Provider* quanto, più propriamente, ai c.d. *Information Society Service Providers* ossia, come precisato nel titolo della sezione IV della direttiva, agli "*intermediary service providers*" [80]. Il che ci fa meglio comprendere, già da una prima analisi letterale, come le norme ivi previste in punto di responsabilità non siano *de plano* applicabili a tutti gli *(Internet) Service Provider* ma solamente a coloro che, nel loro modo di *fornire servizi*, possano dirsi – come meglio preciseremo nel proseguo – *intermediari.*

Ebbene, già in un famoso scritto del Prof. Pasquale Costanzo [81] è possibile ritrovare illuminanti osservazioni circa alcuni servizi che possono essere erogati sulla Rete [82], trattandosi "*all'evidenza di situazioni nelle quali il motore di ricerca non si limita, per così dire, a fare il suo mestiere […] ciò costituisce, già di per sé, una condizione eccettuativa dal normale regime d'irresponsabilità fissato per gli intermediari tecnici dalla normativa europea recepita a livello nazionale*".

È davvero difficile pensare che la dir. 2000/31/CE avesse in mente anche il fenomeno del c.d. web 2.0 [83]: e questo per un dato prima logico e cronologico che giuridico.

Il famoso articolo di Tim O'Reilly "*What is Web 2.0*" [84] nel quale si ritrova, per la prima volta, una definizione del fenomeno (oltre che il suo nome di battesimo) è del settembre 2005.

Nel febbraio dello stesso anno nasceva *Youtube* [85], il cui omonimo sito diventò operativo due mesi dopo. L'avvento di Google Video, anche se di poco precedente [86], sarà tutto una rin-

[79] In *G.U.C.E.*, 17 luglio 2002, n. L 178/1. Il testo italiano della direttiva è reperibile anche su Internet: cfr. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001: 0016:IT:PDF.* Per il testo in lingua inglese: cfr. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: L:2000:178:0001:0016:EN:PDF.*

[80] L. EDWARDS, *The Fall and Rise of Intermediary Liability Online*, in L. EDWARDS-C. WAELDE, *Law and the Internet*, III ed., Oxford and Portland, 2009, p. 62.

[81] P. COSTANZO, *Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutela dei diritti?*, in *Dir. Internet*, 2006, 6, p. 548.

[82] Pur prendendo l'Autore in considerazione il servizio *Autolink* di Google, tali considerazioni – secondo l'interpretazione giuridica dell'Accusa – sono di fatto ben estendibili al servizio Google Video (stante il suo complessivo funzionamento accertato nelle indagini).

[83] Di tale evoluzione ne danno atto, senza tuttavia farne discendere conseguenze in diritto, anche G. SARTOR-M. VIOLA DE AZEVEDO CUNHA, *The Italian Google-Case*, cit., p. 12. Diversamente L. EDWARDS, *The Fall and Rise*, cit., p. 47 ss. (in particolare: p. 67 circa l'analisi in fatto, p. 87 sulle conseguenze in diritto).

[84] Cfr. *http://oreilly.com/web2/archive/what-is-web-20.html.* Per una traduzione in italiano cfr. *http://www.xyz.reply.it/web20.*

[85] Cfr. *http://www.youtube.com/t/about*. Sull'evoluzione dell'omonimo sito cfr. M. PESCE, *Le tappe storiche di YouTube: cinque anni di eventi che hanno creato un mito*, in *http://www.wired.it/news/archivio/2010-05/17/le-tappe-storiche-di-youtube-cinque-anni-di-eventi-che-hanno-creato-un-mito.aspx*.

[86] Cfr. *http://blog.searchenginewatch.com/050125-000100.*

corsa[87] verso l'acquisizione del suo maggiore *competitor*, che avverrà nell'ottobre 2006. E proprio alla fine di quell'anno la rivista americana *Time* sancirà l'affermarsi del Web 2.0 con quella famosa scritta sulla copertina: "*Time's Person of the Year: You*"[88].

Ebbene, come già messo in evidenza nell'introduzione giuridico-economica di uno dei primi Trattati italiani sulla materia, sebbene la Comunicazione della Commissione al Parlamento (COM)97 157 facesse riferimento a numerose attività di *e-commerce*[89], nella dir. 2000/31/CE "*il commercio elettronico viene circoscritto ai servizi della società dell'informazione, cioè a qualsiasi servizio normalmente prestato dietro retribuzione, a distanza, senza la presenza simultanea delle parti, per via elettronica, con riferimento esclusivo alla comunicazione e a richiesta individuale di un destinatario di servizi*"[90].

Alla fine degli anni '90 esistevano solo gestori di telecomunicazioni che era in grado fornire:

1. connettività (tra le parti);
2. spazio web (a mezzo del quale si potesse aprire "un negozio sulla Rete");
3. servizi di ricerca (a mezzo di appositi motori di ricerca);

con ciò rendendo (di fatto tecnicamente) possibile l'esistenza di tale *commercio elettronico*.

La natura di tali servizi offerti dal "*prestatore*"[91], di regola peraltro per la maggior parte gratuiti, anche ove fossero stati a pagamento per l'utente evidenziavano comunque un dato ben preciso: l'assoluta irrilevanza, per il prestatore, di quanto venisse "veicolato" per il tramite dei servizi da lui offerti.

Sulle questioni *sub* 2 e 3. lo stesso Tribunale di Milano era già intervenuto con alcune note pronunce, che nulla però avevano a che vedere con il caso attinente il diverso servizio di Google Video.

La fattispecie presa in considerazione dalla sentenza del Tribunale di Milano, Sez. V pen., 18 marzo 2004[92] era attinente all'ipotesi di mero *link* – ad opera del sito gestito dall'indagato[93] – ad un diverso sito (peraltro non apparentemente) pedopornografico. E, proprio a seguito di una corretta analisi della situazione di fatto portata alla Sua attenzione, il Tribunale milanese aveva avuto ben ragione di affermare che "*il sito dell'imputato aveva infatti rivestito solo la funzione di service provider rispetto al sito ospitato*": se infatti "*si potrebbe sostenere che anche il Serv(ice) Provider divulga o comunque agevola la divulgazione di dati illeciti … laddove l'attività del Provider sia stata solo quella di offrire uno spazio in rete od offrire un*

[87] Cfr. l'estratto del documento *Google video: preliminary analysis of Italian market peculiarities* richiamato nella sentenza del Trib. Milano, p. 21.

[88] Cfr. *http://www.time.com/time/magazine/article/0,9171,1569514,00.html.*

[89] "*il commercio elettronico consiste nello svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica; la distribuzione online di contenuti digitali, l'effettuazione per via elettronica di operazioni finanziarie e di borsa, gli appalti pubblici per vie elettronica ed altre procedure di tipo transattivo delle Pubbliche Amministrazioni*".

[90] G. COMMANDÈ-S. SICA, *Il commercio elettronico. Profili Giuridici*, Torino, 2001, pp. 5-6.

[91] Così come definito dall'art. 2, comma 1, lett. b), in relazione ai "*servizi della società dell'informazione*", ovvero – *ex* art. 2 comma 1, lett. a), "*le attività economiche svolte in linea* – on line – *nonché i servizi definiti dall'art. 1, comma 1, lett. b) della legge 21 giugno 1996, n. 317, e successive modificazioni*" (ovvero "*qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta di un destinatario di servizi*").

[92] Cfr. il testo in *http://www.penale.it/giuris/meri_159.htm.*

[93] Al quale, per tale motivo, veniva contestato il delitto di cui all'art. 600-*ter*, comma 3, c.p. per aver distribuito, divulgato e pubblicizzato a mezzo di tale sito web 5 filmati pedo-pornografici e 14 immagini pedo-pornografiche.

accesso al sito dove è pubblicato il contenuto illecito la sua responsabilità penale non appare configurabile innanzitutto sotto il profilo oggettivo".

Nello stesso modo concludeva la più recente sentenza del Tribunale di Milano, sez. VIII pen., 4 marzo 2008, attinente il "provider Aruba" ossia una delle più note società italiane che si limitano ad offrire pagine web a terzi, anche gratuitamente ma fornendo loro precise credenziali di accesso e *password* (che dunque lo rendono, in fatto, mero intermediario dei contenuti che ivi vengono allocati), allocandole presso i *server* in Arezzo [94].

Proprio alla luce di tale situazione fattuale e al fine di scongiurare scenari che si risolvessero, nei fatti, in una *assoluta immobilità del prestatore* (del tutto sottratto, anche sotto un profilo metagiuridico, a qualsiasi responsabilità attesa l'assenza di un qualsiasi interesse economico rispetto ad un contenuto da esso solamente veicolato), la dir. 2000/31/CE colse l'esigenza di prevedere in carico a tali soggetti (ISP) dei precisi obblighi, nonostante la riaffermazione per essi dell'inesistenza di un generale obbligo di sorveglianza di fatto inesigibile in quanto correlato con la loro natura di meri intermediari.

Si arriva quindi all'individuazione dei criteri di cui agli artt. 14 ss. del d.lgs. n. 70 del 2003, dove *l'host provider* (per quanto riguarda il caso che a noi interessa) viene necessariamente inteso nel senso già indicato, "*considerato che la sua prestazione non incide – anzi, non deve incidere – sul contenuto della comunicazione on line*" [95].

Su tale presupposto convergono tutti i più importanti commenti dottrinali in materia.

E la stesse definizioni di *host provider* sono in linea con quanto finora affermato, laddove autorevolmente è stato sostenuto come "*la finalità della prestazione di hosting è, dunque, quella di consentire alla clientela di pubblicare on line e gestire autonomamente brevi contenuti, ovvero un integrale sito web, senza, tuttavia, acquisire e gestire l'hardware e le infrastrutture di telecomunicazione occorrenti per la divulgazione in Rete, valendosi allo scopo di mezzi messi a disposizione dal provider*" [96].

Ed infatti "*la* guide line *è esplicitata nei considerando 42) e 43)*" della dir. 2000/31/CE*:* "*si può discorrere di esonero di responsabilità del* prestataire, *purché egli non sia 'in alcun modo coinvolto nell'informazione trasmessa' ed assolva ad un ruolo 'di ordine meramente tecnico, automatico e passivo'*" [97].

Questo principio emerge già fin dalla Proposta della Commissione Europa del 1998 [98] ove, a commento della sezione IV dedicata alla "*responsabilità degli intermediari*", si legge come "*soltanto le attività coinvolte nella prestazione di servizi di intermediazione online rientrano in tale fattispecie*".

---

[94] Cfr. *http://webfarm.aruba.it/*.

[95] Così efficacemente S. SICA, in G. COMMANDÈ-S. SICA, *op. cit.*, p. 223.

[96] I.P. CIMINO, *I contratti degli Internet Providers e per i data services on line*, in G. CASSANO-I.P. CIMINO (a cura di), *Diritto dell'internet e delle tecnologie telematiche*, Padova, 2009, p. 20.

[97] Così altrettanto efficacemente S. SICA, in G. COMMANDÈ-S. SICA, *op. cit.*, p. 229. Nello stesso senso, per le altre attività individuate nella Direttiva e nel d.lgs. n. 70 del 2003 si veda, tra gli altri, D. LUCARINI ORTOLANI, *L'Internet nell'intermediazione finanziaria*, in *Dir. inf. e informatica*, 2003, 1, p. 34, nota 50: "*Nella direttiva sul commercio elettronico si esclude la responsabilità del 'prestatore di servizi della società dell'informazione', qualora la sua attività si limiti al mero trasporto ('mere conduit') delle informazioni o alla loro memorizzazione temporanea ('caching'), quando non è in alcun modo coinvolto nell'informazione trasmessa. L'esenzione trova giustificazione nel fatto che in tal caso il prestatore non conosce né controlla le informazioni trasmesse o memorizzate (42° Considerando)*".

[98] Reperibile in *http://www.edis.sk/ekes/ecomm_legalen.pdf.*

5.1. La (ormai imprescindibile) necessità di distinguere caso per caso

Della *ratio* di una simile impostazione vi è una testuale conferma nell'art. 16, comma 2, d.lgs. n. 70 del 2003 [99] che prevede, in conformità con la previsione dell'art. 14, comma 2, dir. 2000/31/CE, come il regime di responsabilità indicato dall'art. 16, comma 1 [100] non si applichi "*se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore*". In questo caso "*il provider non agisce da mero intermediario, ma è il soggetto che volontariamente decide quali informazioni trasmette e attraverso quali modalità*", con consequenziale applicazione delle ordinarie norme sulla responsabilità [101].

Ebbene tale norma, proprio per quel discorso di cui sopra, era volta a distinguere nettamente la figura del *host provider* da quella del *content provider* e non poteva prendere espressamente in considerazione la diversa figura di colui che, nella memorizzazione dei contenuti, li sfrutta commercialmente ponendo in essere una condotta *attiva* su di essi (fin dalla loro immissione nella piattaforma informatica).

Tale ultima ipotesi, come vedremo nel proseguo, è già stata definita – dalla più attenta dottrina [102] e dalla giurisprudenza francese – come quella dell'*hoster attivo*, identificandola altresì come figura problematica (ai fini della individuazione del regime di responsabilità) in quanto si pone nel mezzo tra la posizione di (mero) *hosting provider* e quella di *content provider* (ovvero di produttore "in proprio" di contenuti).

Nello stesso senso e più recentemente il Tribunale di Roma [103], sia pure in una controversia di carattere civilistico, dà correttamente atto che "*la normativa – vedi d.lgs n. 70/2003 – e la giurisprudenza sta ormai orientandosi nel senso di una valutazione caso per caso della responsabilità del provider*". Nel percorso motivazionale, non si prende in considerazione l'applicabilità del d.lgs. n. 70 del 2003 laddove l'Autorità Giudiziaria si sofferma invece su una ricostruzione in fatto coincidente con quanto emerso nelle indagini sul caso Google Video:

> "ritenuto che, a fronte di una condotta così palesemente e reiteratamente lesiva dei diritti non è sostenibile la tesi delle resistenti su una presunta assoluta irresponsabilità del provider che si limiterebbe a svolgere l'unica funzione di mettere a disposizione gli spazi web sui quali gli utenti gestirebbero i contenuti dagli stessi caricati e sulla legittimità di avere un ritorno economico – escludendo il fine commerciale – connesso al proprio servizio in mancanza di un obbligo di controllare i contenuti illeciti e disabilitarne l'accesso; tali asserzioni infatti sono

[99] Cfr. l'approfondita analisi degli effetti di tale disposizione in D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet per i casi di diffamazione on line*, in *Riv. trim. dir. pen. ec*., 2009, 3, p. 562 ss.

[100] Si riporta, per facilità di lettura, il testo della richiamata disposizione: "*Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non e' responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:*

a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione e' illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;

b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso".

[101] Così G.M. RICCIO, *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e resp.*, 2003, 12, p. 1164.

[102] Il tema non sembra aver interessato il mondo accademico italiano (a parte il ricordato scritto del Prof. Costanzo): si rinvia alla attenta analisi di L. EDWARDS, *The Fall and Rise*, cit., p. 47 ss.

[103] Tribunale Civile di Roma, XI sezione civile, ordinanza 16 dicembre 2009 (ud. 24 novembre 2009), in *Guida dir.*, 2, 9 gennaio 2010, p. 56 ss.

smentite dagli stessi scritti difensivi delle convenute nonché dalla documentazione prodotta in giudizio relativa alle indicazioni desumibili sui siti YouTube e Google riguardanti "le regole" stabilite dal provider, che consentono la esclusione di contenuti pedopornografici, prevedono l'accettazione dell'utente di ogni aggiornamento deciso da YouTube, il diritto di controllare i contributi, la assoluta discrezionalità nell'interrompere in maniera temporanea o permanente la fornitura del servizio "in qualsiasi momento, senza previo avviso ed a sua esclusiva discrezione" nonché il diritto di risolvere il contratto con l'utente quando la fornitura non è più "vantaggiosa dal punto di vista commerciale" ... nella specie innegabile ed evidente è la responsabilità delle convenute che, oltre ad organizzare la gestione dei contenuti video, anche a fini di pubblicità (raccolta con le diverse modalità disponibili sulla Rete), nonostante le ripetute diffide e le azioni giudiziarie iniziate da Rti e la consapevolezza della sua titolarità dell'opera hanno continuato la trasmissione ... ad ulteriore, anche se non necessaria conferma, della consapevolezza della violazione dei diritti sicuramente inconciliabile con l'addotta semplice "messa a disposizione della piattaforma".

Anche la successiva pronuncia del Tribunale di Roma [104] (intervenuta a seguito di reclamo proposto avverso la precedente), seppure si sia sostenuto il contrario, non muta l'impostazione sul punto.

E infatti, lungi dall'aver statuito "*in modo inequivoco che Youtube è un web hosting*" [105], in essa testualmente si legge:

"occorre poi rilevare che la circostanza che YouTube e Google svolgano attività di Internet Service Provider cioè servizio di "hosting", consistente nell'offrire ai propri utenti una piattaforma attraverso la quale conservare e rendere disponibili al pubblico contenuti audio e video e quindi memorizzazione di informazioni fornite da un destinatario del servizio (circostanza peraltro contestata da RTI la quale afferma che YouTube e Google svolgono al contrario attività imprenditoriale a fini di lucro e cioè "una articolata attività di impresa finalizzata a fornire una complessa serie di servizi aggiuntivi al fine di offrire agli utenti dei siti internet un palinsesto di video, fonte di utili milionari per gli spazi pubblicitari correlati ai video") non esclude l'illiceità della condotta lamentata".

In linea con quella ricordata necessità di "*valutazione caso per caso*", è stato autorevolmente ricordato [106] come nel 2009 il Comitato per l'informazione, computer e politiche della comunicazione (CSISAC [107]) abbia suggerito una classificazione dei c.d. intermediari del mondo digitale non più secondo una "visione statica" ma in rapporto alle funzioni da essi svolte, proprio in quanto "*nel corso degli anni, gli intermediari su internet sono passati dall'offerta di servizi di base per l'accesso a internet e le e-mail, a un'ampia gamma di strumenti sul Web che consentono agli utenti di pubblicare qualsiasi cosa in formato elettronico*".

Coerentemente con una simile impostazione, secondo tale Autore il problema – in punto di responsabilità – non si porrebbe né per i tradizionali fornitori di servizi in Internet qualificabili come *Access Provider* (ovvero coloro che forniscono il mero accesso alla Rete) né per "*gli intermediari del commercio elettronico*", stante la loro pacifica riconducibilità alle norme

[104] Trib. civ. Roma, sez. specializzata in materia di proprietà industriale ed intellettuale, ord. 11 febbraio 2010.

[105] G. SCORZA, *Ma-si-ma-no la "sorveglianza" è un tiro alla fune ...* (13 febbraio 2010), in *http://www.guidoscorza.it/?p=1521*: "*I giudici, questa volta, scrivono in modo inequivoco che Youtube è un web hosting e che ad esso sarebbe, quindi, applicabile la disciplina sul commercio elettronico in materia di assenza di obbligo generale di sorveglianza*".

[106] U. PAGALLO, *Sul principio di responsabilità giuridica in rete*, in *Dir. inf. e informatica*, 2009, p. 705 ss.

[107] Cfr. *http://csisac.org/*.

del d.lgs. n. 70 del 2003, ma per i "*prestatori di servizi in rete volti alla distribuzione e reperimento delle informazioni, nonché alla messa a disposizione di piattaforme e applicazioni digitali. Si tratta di quel variegato insieme d'imprese e soggetti che comprende motori di ricerca, mondi virtuali, siti di social network, piattaforme video e vendite all'asta, blog, hosting provider, etc*.".

Orbene, occorre subito far presente come tale ultimo elenco ricomprenda fenomeni e funzioni di per sé non sovrapponibili [108].

Si pensi solo, ai fini del nostro discorso, che un *social network* – a differenza di una situazione fattuale identificabile quale *hoster attivo* – si caratterizza per una "indifferenza piena" rispetto ai contenuti ad opera del creatore/fornitore della piattaforma informatica, la quale viene concepita proprio per essere lasciata in tutto e per tutto ad uso esclusivo degli utenti (peraltro in gruppi tendenzialmente ad accesso limitato): non sarà quindi possibile applicare agli *hoster attivi* argomentazioni che, anche di recente, sono state sostenute in diritto [109] relativamente ai *social networks.*

Affermare poi che il divieto generale di sorveglianza valga "*per* tutti *'i prestatori di servizi della società dell'informazione' come individuati dall'art. 2 del D.L. 70/2003 che recepisce la citata D-2000/31/CE*" [110] (ed indipendentemente da una loro classificazione a seconda del servizio concretamente svolto) significa non solo dimenticarsi dell'ambito di applicazione soggettiva delle regole di responsabilità (riferibili ai soli *intermediari*, come già ricordato) ma anche non tener adeguatamente conto, oltre che dell'*incipit* dell'art. 17 [111], del fatto che è lo stesso art. 16 comma 2 a dirci come il d.lgs. n. 70 del 2003 non trovi spazio per i *content provider* (soggetti che, a buon ragione, rientrano comunque nella definizione normativa di *Information Society Service Providers).*

L'interpretazione che qui si critica peraltro porterebbe paradossalmente con sé la contraddizione di dover ritenere il *content provider* (che ovviamente non potrà proclamarsi ignaro dei contenuti, avendoli lui stesso realizzati) responsabile non già per la diffusione del contenuto illecito (come sarebbe logicamente e giuridicamente corretto aspettarsi) ma, eventualmente, solo nei casi di cui all'art. 17, comma 3, d.lgs. n. 70 del 2003.

Alla luce di simili premesse ed al fine di coglierne i riflessi giuridici nel caso concreto posto all'attenzione del Tribunale di Milano, interessanti sono alcune pronunce giurisprudenziali francesi.

Già nel giugno 2007 il *Tribunal de Grande Instance de Paris* [112] – in conformità con decisioni precedenti [113] – aveva negato la qualifica di *hosting service* (*hébergeur*), e per essa l'applicabilità del regime dettato dalla normativa sul commercio elettronico, al servizio MySpace:

[108] Analogamente fenomeni non sovrapponibili vengono trattati in maniera identica in G. SARTOR-M. VIOLA DE AZEVEDO CUNHA, *The Italian Google-Case*, cit., p. 12.

[109] A solo titolo di esempio, viene spesso citato il parere 5/2009 – WP 163 sui *social network online* adottato dal Wp29 il 12 giugno 2009, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.*

[110] Così U. PAGALLO, *Sul principio*, cit., p. 715.

[111] "*Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza …*".

[112] Cfr. *Jean Yves L. dit Lafesse* v *Myspace*, *Tribunal de Grande Instance de Paris, Ordonnance de référé, 22 June 2007*, in *http://www.legalis.net/jurisprudence-decision.php3?id_article=1965*. Per un commento si veda A. STROWEL, *Google et les nouveaux services en ligne: quels effets sur l'économie des contenus, quels défis pour la propriété intellectuelle* in A. STROWEL-J.TRIALLE, *Google et les nouveaux services en ligne: impact sur l'économie du contenu et questions de propriété intellectuelle*, Bruxelles, 2008, pp. 44-45 (citato da G. SARTOR-M. VIOLA DE AZEVEDO CUNHA, *The Italian Google-Case*, cit., p. 5*).*

[113] *Tiscali Media* v *Dargaud Lombard, Lucky Comics, Cour d'appel de Paris (4ème chambre, section A) decision of 7 June 2006*, in *http://www.legalis.net/jurisprudence-decision.php3?id_article=1638.*

secondo il Tribunale, elementi rilevanti al fine di affermare la diversa qualifica di *publisher of content* (*éditeur*) erano l'imposizione di una pagina predefinita per gli utenti e la presenza di pubblicità (che generava ricavi) mostrata ad ogni visita [114].

Quanto al servizio Google Video [115], sempre in una decisione del *Tribunal de Grande Instance de Paris* – 24 giugno 2009 [116] significativamente si legge che, seppur "*nella propria attività di stoccaggio di video, la società Google Inc. beneficia della statuto di 'ospitante'*", anche all'interno del servizio Google Video e proprio per quel *quid pluris* che lo caratterizza "*per quanto concerne il funzionamento del motore di ricerca Google, che offre un sistema di indicizzazione dei video sulla 'rete', il tribunale ritiene che la società Google non può beneficiare dello statuto di 'ospitante' per questa attività*".

Ed infatti, secondo il Tribunale di Parigi, "*il regime 'alternativo' di ospitante, che è un regime di eccezione, non può andare a beneficio delle società che assicurano la diffusione di contenuti mediante l'accesso a siti di ospitamento*", anche se non siano esse stesse ad assicurarlo materialmente ("*poiché non sono esse ad assicurarlo materialmente*"). E dunque, sia per le società terze (ossia quelle sui cui *server* di fatto sono stoccati i video) che per Google (nel suo servizio volto ad indicizzare gli stessi ed a permettere agli utenti di visionarli per intero o per estratti) si applicheranno i normali principi di responsabilità, fissati "*dal diritto comune*" [117].

Alla luce di quanto finora complessivamente affermato, si potrà comprendere come l'impostazione dell'Accusa sia stata quella di sostenere che dietro la (auto)dichiarazione di essere "mero intermediario" si nascondesse, per il servizio di Google Video, una vera e propria *frode delle etichette.*

Invero di fronte ad un servizio che, per le sue caratteristiche operative, si poneva nel mezzo tra la posizione di (mero) *hosting provider* e quella di *content provider* (ovvero di produttore "in proprio" di contenuti), si trattava di verificare – in un'ottica costituzionalmente orientata e lontana da qualsiasi pericolo di applicazione analogica in *malam partem* – quale potesse essere il regime di responsabilità in concreto applicabile.

[114] Cfr. C. ANGELOPOULOS, *Filtering the Internet for Copyrighted Content in Europe*, 2009, p. 3, in *http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2009.pdf.en.*

[115] È opportuno qui ricordare che, a seguito dell'acquisizione di Youtube ad opera di Google, l'originario servizio di Google Video si è evoluto nel ricomprendere anche una indicizzazione/visualizzazione di video presenti sulla rete (e dunque non solo di quelli ospitati sui server di Google).

[116] *Jean-Yves Lafesse et autres* v *Google et autres*, *Tribunal de grande instance de Paris (3ème chambre, 3ème section) Jugement du 24 juin 2009*, in *http://legalis.net/spip.php?page=breves-article&id_article=2682* (sentenza prodotta in giudizio dai difensori degli imputati).

[117] Si legge infatti nella motivazione: "*Ora, nella fattispecie, la società Google permette all'utente internet, a partire da una ricerca sul suo motore di ricerca, di prendere visione di tutto, o parte, di un video ospitato su un sito ch non è quello di Google. Se effettivamente l'attività di indicizzazione in se non permette di coinvolgere la responsabilità di Google sui video indicizzati, ciò non vale per il servizio che essa offre agli utenti interni, permettendo loro di visionare suddetti video per intero o estratti di questi. Questo servizio di diffusione dipende dal diritto comune e spetta a Google Inc. contrarre con le società terze delle garanzie contrattuali nelle ipotesi di video non autorizzati dai titolari di diritto … Se effettivamente la responsabilità della società Google Inc. potrebbe essere coinvolta in ragione della diffusione integrale dei video ospitati su siti terzi a partire dai risultati del suo motore di ricerca, il tribunale non può far altro che constatare la carenza dei richiedenti per quanto concerne la prova di una diffusione illecita delle loro opere a partire dal motore di ricerca Google*".

5.2. L'impostazione della Cassazione in materia di responsabilità degli *Internet Service Providers*

In una simile prospettiva, è ultimamente intervenuta la nostra Suprema Corte, sez. III pen., con la sentenza n. 49437/09 del 23 dicembre 2009 [118] proprio in tema di responsabilità penale degli *Internet Service Providers*.

Si tratta, a ben vedere, di una pronuncia che si pone nel filone già segnato (nelle sue premesse giuridiche) da Cass. pen., sez. III, 4 luglio 2006, n. 33945 [119] in relazione ad un caso nato proprio da un'indagine della Procura di Milano [120], attinente ad una ipotesi ben diversa da quella precedentemente analizzata dal Tribunale di Milano nel 2004.

Qui si trattava, infatti, non già di meri *link* – ad opera del sito gestito dagli indagati – a materiali illeciti, dal momento che tale sito offriva altresì istruzioni utili all'accesso (con collaterale visualizzazione e diffusione dei relativi contenuti) a siti esteri riproducenti materiali lesivi del diritto d'autore. Così sul punto la Cassazione:

> "Il problema ora da affrontare concerne il perfezionamento della contestata fattispecie di reato sotto il profilo della abusiva "immissione" nella rete internet; come correttamente evidenziato dai Giudici di merito, "fra più condotte generiche suscettibili di integrare la messa a disposizione di una serie indeterminata di soggetti, il legislatore ha inteso sanzionare penalmente soltanto la condotta specifica di immissione nella rete internet dell'opera protetta". Ora è pacifico, in punto di fatto, che gli indagati avevano messo a disposizione degli utenti le informazioni ed i mezzi tecnici attraverso i quali era possibile installare sul proprio personal computer tutto il software necessario alla visione delle partite di calcio sulle quali la Sky vantava un diritto di esclusiva; tale condotta è stata ritenuta dai Giudici come posteriore alla immissione in rete delle opere protette e, di conseguenza, inserendosi in un momento successivo al perfezionamento del reato, è stata considerata irrilevante ai fini penali. Tale conclusione merita un approfondimento. È innegabile che gli attuali indagati hanno agevolato, attraverso un sistema di guida on line, la connessione e facilitato la sincronizzazione con l'evento sportivo; senza la attività degli indagati, non ci sarebbe stata, o si sarebbe verificata in misura minore, la diffusione delle opere tutelate. Le informazioni sul link e sulle modalità per la visione delle partite in Italia, per raggiungere il loro obiettivo, devono essere state inoltrate agli utenti in epoca antecedente alla immissione delle trasmissioni in via telematica; tale rilievo, se puntuale in fatto, comporta come conseguenza che, in base alle generali norme sul concorso nel reato, gli indagati, pur non avendo compiuto l'azione tipica, hanno posto in essere una condotta consapevole avente efficienza causale sulla lesione del bene tutelato. È appena il caso di ricordare come l'attività costitutiva del concorso può essere individuata in qualsiasi comportamento che fornisca un apprezzabile contributo alla ideazione, organizzazione ed esecuzione del reato; non è necessario un previo accordo diretto alla causazione dell'evento, ben potendo il concorso esplicarsi in una condotta estemporanea, sopravvenuta a sostegno della azione di terzi anche alla insaputa degli altri agenti".

[118] In *CED*, rv. 245936.

[119] In Internet su *http://www.penale.it/public/docs/Cass_III_Pen_4_07_2006_N33945_Calciolibero.pdf.* Cfr. A. NATALINI, *Diritti tv, quell'esclusiva aggirata in Rete. Calcio e streaming: se linkare è reato. Punito chi agevola on line la visione delle gare. Con tanti dubbi*, in *Dir. e giust.*, 2006, 40, p. 37 ss. e L. SCOPINATO, *Rilevanza penale della divulgazione via web di programmi tv*, in *Dir. pen. e proc.*, 2007, 5, p. 651 ss.

[120] Per un commento all'intera vicenda (in fatto ed in diritto), nata da una impugnazione in Cassazione, ad opera del Pubblico Ministero Gianluca Braghò, di un provvedimento di sequestro preventivo negato sia dal GIP che dal Tribunale del Riesame di Milano: G. DALIA, *Sky vs. Cina: terzo, e non ultimo, atto* (nota a Cass. pen., sez. III, 10 ottobre 2006), in *Dir. Internet*, 2007, 2, p. 157.

La recente sentenza della Cassazione appare importante perché essa fa espressamente discendere un diverso trattamento giuridico a soggetti che operano in fatto diversamente, nonostante entrambi si fossero dichiarati soggetti alla normativa sul commercio elettronico in quanto meri intermediari [121] per sfuggire a responsabilità penali (il primo) e all'applicazione dell'inibitoria ad opera dell'Autorità Giudiziaria (il secondo).

E forse si capisce perché Google Italy, proprio nel corso del processo milanese, dalle pagine del suo *blog* si fosse sentita "*in dovere di fare alcune precisazioni*" [122] sul punto.

Ma le motivazioni della Suprema Corte non sembrano lasciare spazio a diverse interpretazioni:

> "Se il sito web si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello peer to peer) per consentire la condivisione di file contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato.
>
> Però se il titolare del sito non si limita a ciò ma fa qualcosa di più – ossia indicizza le informazioni che gli vengono dagli utenti, che sono tutti potenziali autori di uploading, sicché queste informazioni (i.e. chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), anche se ridotte a minimo, ma pur sempre essenziali perché gli utenti possano orientarsi chiedendo il downloading di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito, ad es. a mezzo di un motore di ricerca o con delle liste indicizzate – il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. C'è un *quid pluris* in quanto viene resa disponibile all'utenza del sito anche un'indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto l'attività di trasporto dei file non è più agnostica; ma si caratterizza come attività di trasporto di dati contenente materiale coperto da diritto d'autore. Ed allora è vero che lo scambio di file avviene da utente ad utente (*peer to peer*) ma l'attività del sito web (al quale è riferibile il protocollo di trasferimento e l'indicizzazione dei dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone *ex* art. 110 c.p.".

È dunque "quel fare qualcosa di più", già efficacemente segnalato dal Prof. Costanzo nel suo scritto e accertato nei fatti dell'indagine sul caso Google Video, che fa la differenza e che conseguenzialmente rende non applicabile la disciplina sul commercio elettronico (perché non siamo in presenza di un mero intermediario, *agnostico* rispetto ai dati memorizzati, ma invece di soggetti che surrettiziamente pretendono di fatto di avvalersi di un regime di irresponsabilità).

Di contro, la stessa Cassazione correttamente applica il regime di cui al d.lgs. n. 70 del 2003 a soggetti la cui attività a ragione rientra nella nozione giuridica di "*prestatore di un servizio della società dell'informazione*" (nel caso i soggetti che, in quanto qualificabili come

[121] Tesi peraltro sostenuta anche nel processo presso il Tribunale di Stoccolma a carico dei 4 gestori del sito *thepiratebay.org* (conclusosi con sentenza di condanna in primo grado, emessa in data 17 aprile 2009).

[122] Così M. PANCINI (Google Italy – *European Policy Counsel*) in data 27 aprile 2009: "*In questi giorni, a seguito della sentenza di condanna emessa in Svezia contro i titolari di The Pirate Bay, circolano alcuni paragoni tra The Pirate Bay e Google. Ci sentiamo in dovere di fare alcune precisazioni. La missione di Google è indicizzare e rendere disponibili tutte le informazioni presenti online, questo indipendentemente dai formati in cui questi file sono messi online. I formati dei file non sono di per sé illeciti, ma è l'uso che se ne fa che li qualifica come tali. Per fare un esempio Google è come un'autostrada sulla quali circolano molte autovetture (i contenuti); Google non può essere considerato responsabile se con una di queste automobili viene commesso un crimine e nemmeno lo è l'automobile di per sé*": *http://googleitalia.blogspot.com/2009/04/perche-google-e-diverso-da-pirate-bay.html.*

Access Provider, possono correttamente in fatto dichiararsi meri intermediari), così argomentando:

> "tale normativa speciale, nel prevedere in generale la libera circolazione – nei limiti però del rispetto del diritto d'autore: art. 4, comma 1, lett. a) – di tali servizi, quali quelli prestati dal provider per l'accesso alla rete informatica Internet, contempla anche, come deroga a tale principio, che la libera circolazione di un determinato servizio possa essere limitata con provvedimento dell'autorità giudiziaria per motivi attinenti all'opera di prevenzione, investigazione, individuazione e perseguimento dei reati".

Anche sotto questo profilo apparivano illuminanti alcune indicazioni riconducibili alla sentenza del 6 maggio 2009 della Corte di Appello di Parigi [123] e nelle quali si ritrova esplicitata la figura dell'*hoster attivo* quale figura diversa dal *hoster* tradizionalmente inteso dalla direttiva sul commercio elettronico (ossia, come già indicato, un *hoster passivo* ed indifferente quindi ai contenuti che tramite esso vengono veicolati dall'utente, destinatario del servizio di *hosting*).

In tale pronuncia infatti si legge che gli appellanti contestavano alla società Dailymotion (che sostanzialmente fornisce lo stesso servizio di Google Video) "*di avvalersi indebitamente della qualità di fornitore di servizi tecnici in quanto svolge un'attività che in realtà configura quella di editore di contenuti; ... gli stessi intendono sostenere a questo riguardo: – che la classificazione binaria hoster/editore prevista dalla LCEN* [124] *non è adattata allo scenario internet così come si delinea con la nascita dei siti 'partecipativi' o 'collaborativi' del 'web. 2.0' che impone l'esclusione dello status di hoster per gli 'hoster attivi', cioè le persone che assicurano mediante un servizio da esse sfruttato la memorizzazione e la diffusione dei contenuti memorizzati, e il mantenimento di tale status per gli 'hoster passivi', cioè solo le persone che si limitano a proporre una fornitura di spazi per la memorizzazione dei contenuti*".

Il Giudicante tuttavia sul punto, rilevando che "*non è comprovata nel caso in questione l'esistenza di una relazione tra le modalità del compenso derivante dalla pubblicità e la determinazione dei contenuti messi in linea*", ritiene che "*la società Dailymotion rivendica a buon diritto lo status di intermediario tecnico*".

Circostanza invece provata dalle indagini attinenti al caso Google Video dal momento che l'operatività dell'attività pubblicitaria *AdWords*, come emerso dalle complessive indagini, appariva strettamente correlata ai dati (anche personali) immessi nel sistema Google Video.

E dunque non già un mero "*sfruttamento del sito mediante la commercializzazione di spazi pubblicitari*" (dal momento che è la stessa Corte d'Appello francese a rilevare che "*ciò non fa dedurre una capacità di intervento del servizio sui contenuti messi in linea*") ma un qualcosa di più, che è tale da collocarsi nel mezzo della (ormai superata, seppur troppo spesso recuperata a livello accademico) distinzione tra "*colui che fornisce il contenuto*" e "*colui che fornisce il servizio*" e che caratterizza proprio la figura dell'*hoster attivo,* non indifferente ai contenuti in quanto da lui stesso sfruttati commercialmente all'atto della fornitura del servizio.

---

[123] *S.A. Dailymotion v.Societè Nord-Ouest Production et autres, Cour d'appel de Paris (4ème chambre, section A) Arrêt du 06 mai 2009*, in *http://legalis.net/spip.php?page=breves-article&id_article=2634* (sentenza prodotta in giudizio dai difensori degli imputati).

[124] *Loi sur la Confiance dans l'Economie Numérique*: trattasi della legge francese sul commercio elettronico.

5.3. Il percorso motivazionale della sentenza della Corte Europea del 23 marzo 2010 in materia di *keyword advertising*

Allo stesso modo l'impostazione sostenuta dalla Procura di Milano appare coincidere con quella indicata nella recente sentenza della Corte Europea del 23 marzo 2010 che, sebbene affrettatamente commentata come favorevole a Google [125], ad un più attento lettore indica che "*l'art. 14 della direttiva 2000/31 deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati*" [126].

Si riporta il percorso motivazionale, che significativamente lascia al Giudice nazionale – che "*meglio può conoscere le modalità concrete della fornitura del servizio*" nel caso sottoposto alla attenzione della Corte Europea ("*keyword advertising*" ossia pubblicità a partire da parole chiave) – verificare se "*il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza*":

> "110. Come indicato ai punti 14 e 15 della presente sentenza, il legislatore ha definito la nozione di "servizio della società dell'informazione" come comprendente i servizi prestati a distanza mediante attrezzature elettroniche di trattamento e di memorizzazione di dati, a richiesta individuale di un destinatario di servizi e, normalmente, dietro retribuzione. Tenuto conto delle caratteristiche del servizio di posizionamento di cui trattasi nelle cause principali, riassunte al punto 23 della presente sentenza, si deve concludere che tale servizio presenta tutti gli elementi di tale definizione.
>
> 111. Non si può contestare, inoltre, il fatto che il prestatore di un servizio di posizionamento trasmette informazioni del destinatario di detto servizio, vale a dire l'inserzionista, su una rete di comunicazione accessibile agli utenti di Internet e memorizza, vale a dire salva sul proprio server, taluni dati, quali le parole chiave selezionate dall'inserzionista, il link pubblicitario e il messaggio commerciale che lo accompagna, nonché l'indirizzo del sito dell'inserzionista.
>
> 112. È necessario inoltre, affinché la memorizzazione effettuata dal prestatore di un servizio di posizionamento possa rientrare nella previsione dell'art. 14 della direttiva 2000/31, che il comportamento di tale prestatore si limiti a quello di un "prestatore intermediario" nel senso voluto dal legislatore nell'ambito della sezione 4 di tale direttiva.
>
> 113. Dal quarantaduesimo 'considerando' della direttiva 2000/31 risulta, a tal proposito, che le deroghe alla responsabilità previste da tale direttiva riguardano esclusivamente i casi in cui l'attività di prestatore di servizi della società dell'informazione sia di ordine "meramente tecnico, automatico e passivo", con la conseguenza che detto prestatore "non conosce né controlla le informazioni trasmesse o memorizzate".
>
> 114. Pertanto, al fine di verificare se la responsabilità del prestatore del servizio di posizionamento possa essere limitata ai sensi dell'art. 14 della direttiva 2000/31, occorre esaminare se il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza.
>
> 115. Per quanto attiene al servizio di posizionamento di cui trattasi nelle cause principali,

[125] Cfr. *La decisione della Corte di Giustizia Europea a favore di Google*, in *http://googleitalia.blogspot.com/2010/03/la-decisione-della-corte-di-giustizia.html*; G. SCORZA, *La rivincita degli intermediari*, in *http://www. guidoscorza.it/?p=1654*.

[126] Cfr. punto 120. Il testo della sentenza è reperibile su *http://curia.europa.eu/*.

dal fascicolo e dalla descrizione di cui ai punti 23 e seguenti della presente sentenza si evince che la Google, tramite software da essa sviluppati, effettua un trattamento dei dati inseriti dagli inserzionisti ottenendo la visualizzazione di annunci a condizioni stabilite dalla stessa Google. Quest'ultima stabilisce quindi l'ordine di visualizzazione in funzione, in particolare, del pagamento degli inserzionisti.

116. Occorre osservare che la semplice circostanza che il servizio di posizionamento sia a pagamento, che la Google stabilisca le modalità di pagamento, o ancora che essa dia informazioni di ordine generale ai suoi clienti, non può avere come effetto di privare la Google delle deroghe in materia di responsabilità previste dalla direttiva 2000/31.

117. Del pari, il fatto che la parola chiave selezionata e il termine di ricerca inserito da un utente di Internet coincidano non è di per sé sufficiente a ritenere che la Google conosca o controlli i dati inseriti dagli inserzionisti nel suo sistema e memorizzati sul suo server.

118. Nell'ambito dell'esame di cui al punto 114 della presente sentenza, è invece rilevante il ruolo svolto dalla Google nella redazione del messaggio commerciale che accompagna il link pubblicitario o nella determinazione o selezione di tali parole chiave.

119. Proprio alla luce delle suesposte considerazioni spetta al giudice nazionale, che meglio può conoscere le modalità concrete della fornitura del servizio nelle cause principali, valutare se il ruolo svolto dalla Google corrisponda a quello descritto al punto 114 della presente sentenza".

5.4. Il consenso dell'interessato ai dati personali trattati nell'ambito di servizi di *hosting* attivo: chi, come e quando

Di fronte all'evolversi della tecnologia ed al moltiplicarsi dei casi portati all'attenzione dei giuristi, rimangono le norme di legge tra le quali quella degli artt. 13, 23 commi 3 e 4, 26 Codice Privacy.

Nel corso del processo milanese è stato sostenuto dai difensori degli imputati che, quanto ai "*dati del soggetto disabile ripreso nel video …, avrebbe dovuto essere lo stesso uploader, quale titolare al trattamento dei dati, a dover informare l'interessato ed a raccogliere il suo espresso consenso alla pubblicazione del video su internet*" e che dunque, più sinteticamente, "*qualsiasi violazione della privacy del ragazzo, dovuta al mancato ottenimento del suo consenso, deriva dalla condotta dell'uploader, e non da quella degli imputati*".

Nell'impostazione accusatoria invece, sgomberato il campo dall'invocato principio *ad impossibilia nemo tenetur* dal momento che in realtà nessuna iniziativa era stata pensata [127] né in concreto adottata nella vicenda in esame (il video peraltro era rimasto *online* per quasi 2 mesi nella categoria dei "video più divertenti", arrivando fino al 29° posto dei video più visti – per la precisazione: 5.500 volte – prima di essere stato rimosso), si è portato all'attenzione del Tribunale come una simile interpretazione del complessivo dato normativo sembrerebbe non solo paradossale ed incoerente rispetto ad analoghe condotte poste in essere dalle società del gruppo Google ma soprattutto non conforme al diritto vigente.

La portata *paradossale* emergeva proprio dai fatti oggetto del procedimento penale: si vorrebbe ragionevolmente sostenere che i bulli, dopo aver vergognosamente vessato il minore disabile, avrebbero dovuto acquisire il suo consenso per la successiva diffusione *online* della loro riprovevole azione.

L'*incoerenza* di tale affermazione rispecchia invece una dicotomia dell'agire economico

[127] Il servizio era stato lanciato in Italia nel luglio 2006 senza neppure la presenza del meccanismo di *flagging*, introdotto successivamente.

di Google: perché, laddove invece era stata la società ad acquisire *ab origine* i dati da immettere nella propria piattaforma informativa, i principi [128] (anche in diritto) sembravano ribaltarsi. Significativo il fatto che, nella controversia con l'Autorità Garante svizzera, la stessa società avesse "*rifiutato di attuare la maggior parte*" delle misure raccomandategli "*per migliorare la protezione della sfera privata nel suo servizio on line Street View*", annunciando peraltro di voler "*fotografare principalmente il centro della città*" ma mettendo invece in rete "*zone molto più estese*" [129]. O, ancora più di recente, che la stessa sia stata condannata in data 18 dicembre 2009 dal *Tribunal de grande instance de Paris* [130] dal momento che – come si legge nelle

[128] Cfr. da ultimo l'iniziativa dell'Associazione Italiana Editori (in *www.aie.it*) nei confronti dell'ipotesi di accordo transattivo per il servizio Book Search (la prima udienza della Corte di New York era prevista il 18 febbraio 2010), allo stesso modo di analoghe iniziative delle associazioni degli editori tedeschi, austriaci, svizzeri, francesi e spagnoli. "*Noi non siamo contro a priori – ci dice Marco Polillo, presidente dell'Associazione Italiana Editori – ma Google Books ha accelerato le sue operazioni seguendo il principio: cominciamo a fare il più possibile, poi vediamo che tipo di problemi possono sorgere*" (in T. CAPPELLINI, *La biblioteca universale resterà un sogno, 30.1.2010, www.ilgiornale.it*). Riporta sul punto APCOM (*www.apcom.net*, 5.2.10) "*Questo accordo è una versione modificata di quello che Google e gli editori avevano concluso lo scorso anno e mira a rispondere alle obiezioni formulate a settembre dal ministero della Giustizia Usa e da altre istanze sulla tutela dei diritti d'autore e sulle leggi contro il monopolio. Pur notando un 'progresso sostanziale', il ministero della Giustizia ha ritenuto che la nuova versione dell'accordo 'soffre dello stesso problema centrale dell'accordo originario'* ".

[129] Cfr. comunicato stampa dell'Incaricato federale della protezione dei dati e della trasparenza, (*http://www.edoeb.admin.ch/aktuell/index.html?lang=it*): "*Street View: L'IFPDT porta Google dinanzi al Tribunale amministrativo federale. Berna, 13.11.2009 – L'11 settembre 2009 Hanspeter Thür, Incaricato federale della protezione dei dati e della trasparenza, ha raccomandato a Google diverse misure per migliorare la protezione della sfera privata nel suo servizio on line Street View. Google ha rifiutato di attuare la maggior parte di queste misure. L'IFDPT intenta pertanto un'azione dinanzi al Tribunale amministrativo federale. Nel servizio Street View, messo on line da metà agosto 2009, numerosi volti e targhe di veicoli non sono sufficientemente mascherati dal punto di vista della protezione dei dati o le persone sono mostrate nei dintorni di luoghi sensibili quali ospedali, carceri o scuole. Per questo motivo l'11 settembre 2009 l'IFPDT ha emanato una raccomandazione nella quale invitava Google a tenere maggiormente conto della protezione dei dati personali e della sfera privata. Nella sua lettera del 14 ottobre 2009 Google ha respinto la maggior parte dei punti della raccomandazione. Già la comunicazione preliminare fornita da Google all'IFPDT era incompleta: Google aveva ad esempio annunciato di voler fotografare principalmente il centro delle città, ma ha invece messo in rete zone molto più estese. Nei quartieri periferici in cui la densità della popolazione sulle strade diminuisce rapidamente, il mascheramento dei volti (blurring) non è più sufficiente, soprattutto considerando la funzione di ingrandimento. Questa permette infatti agli utenti di Street View di isolare le persone sullo schermo e di ingrandirle. È inadeguata anche l'altezza della fotocamera montata sui veicoli di Google, già criticata nella raccomandazione, poiché supera recinzioni, siepi e muri e permette così di vedere in Street View molto più di quanto possono vedere solitamente i passanti sulle strade. La sfera privata in luoghi recintati (giardini, cortili) non è in tal modo più garantita. Per questi motivi, l'IFPDT ha deciso di agire intentando un'azione dinanzi al Tribunale amministrativo federale*". In attesa della decisione del Tribunale, nel dicembre 2009 è stato successivamente raggiunto un accordo in base al quale Google continuerà ad effettuare le riprese in Svizzera ma senza immetterle in Rete (utilizzandole eventualmente all'interno del Gruppo soltanto a scopi e per prodotti che non coinvolgono le persone). All'esito di tale accordo, le parti hanno così dichiarato: "*Peter Fleischer, Incaricato della protezione dei dati per Google: 'Siamo soddisfatti di avere raggiunto con il signor Thür un accordo che ci permette di proseguire le nostre riprese fotografiche per Street View. Fino alla decisione del Tribunale amministrativo federale, tuttavia, non inseriremo più nessuna nuova immagine in Street View'. Hanspeter Thür, Incaricato federale della protezione dei dati: Questo accordo consente di conseguire tutti gli obiettivi da noi perseguiti con le misure cautelari: durante la procedura dibattimentale non verranno inserite altre immagini. In caso di riprese, le persone eventualmente interessate saranno tempestivamente informate. Google si impegna inoltre ad accettare una sentenza definitiva di un tribunale svizzero e ad applicarla anche alle immagini scattate in Svizzera già presenti all'estero*". Con sentenza del 30 marzo 20011 il Tribunale amministrativo federale ha statuito come *Google Street View* violi ingiustificatamente la sfera privata delle persone e contravviene così al diritto svizzero.

[130] Il testo delle motivazioni della sentenza è disponibile sul sito *http://www.legalis.net/jurisprudence-decision.php3?id_article=2812*. Per un riassunto della vicenda: *http://www.legalis.net/actualite.php3*.

motivazioni – sono state inserite nel sistema di *Google Books* ben 23.900 pagine senza autorizzazione dei relativi titolari del diritto d'autore [131].

La *non conformità al diritto vigente* emerge dalla semplice lettura dell'art. 13, comma 4, d.lgs. n. 196 del 2003, laddove si prevede – in perfetta aderenza agli artt. 10 e 11 dir. 46/1997/CE – che "*se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie dei dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione*".

La dottrina concordemente sottolinea che, per mezzo dell'informativa che "*il titolare del trattamento*" è tenuto a fornire ai sensi dell'art. 13, "*l'interessato*" (ovvero titolare dei dati che lo riguardano, e quindi – nel caso in esame – la persona raffigurata nel video [132]) è così messo nella condizione di esprimere un consenso consapevole [133] e di esercitare i propri poteri di autodeterminazione [134].

Ed è chiaro che "*ove l'interessato non venisse informato, e fosse prevista unicamente l'informativa ad un soggetto terzo di cui all'art. 13 comma 1, molto probabilmente egli non verrebbe mai a conoscenza dell'esistenza di un trattamento dei dati che lo riguardano, realizzando così un'ipotesi di trattamento illecito. Se infatti non fosse previsto un obbligo di informativa anche all'interessato, per le ipotesi di dati raccolti presso terzi, la previsione della sola informativa ai sensi del comma 1° potrebbe generare fattispecie di trattamento illecito. Già la raccolta può, infatti, considerarsi trattamento dei dati personali (ancorché in una fase solo iniziale dello stesso) ed ove non si procedesse ad informare l'interessato potrebbe configu-*

[131] "*Si tratta di una decisione che, nella visione di chi l'ha applaudita, potrebbe costituire un freno alla corsa di Google nella creazione di un monopolio sull'universo dei libri digitalizzati. Una corte di Parigi ha recentemente stabilito che BigG dovrà risarcire con la cifra di 300mila euro la casa editrice francese La Martiniere, dopo aver scansionato alcuni suoi testi all'interno del progetto Book Search. Un'operazione di digitalizzazione che Mountain View avrebbe effettuato senza ottenere un consenso esplicito da parte dell'editore transalpino.* La *Martiniere aveva citato in giudizio Google tre anni fa, insieme a SNE, associazione francese degli editori, e alla Société des Gens De Lettres (SGDL) che riunisce invece gli scrittori. All'interno del progetto Book Search, la Grande G era stata accusata di una ripetuta violazione del copyright, dal momento che aveva reso disponibili online un nutrito gruppo di volumi in formato elettronico (peraltro non soltanto appartenenti al catalogo di La Martiniere) ... stando a dati riportati dalla stessa SNE, sono state circa 100mila le opere francesi digitalizzate da Google senza alcun consenso esplicito da parte dei detentori dei diritti*": (*http://punto-informatico.it/2774917/PI/News/francia-google-paghera-book-search.aspx*).

[132] Di diverso avviso sembra essere il Garante Privacy, intervenuto sul merito della sentenza alcuni giorni dopo il deposito delle motivazioni: cfr. A. LONGO, *Regole globali per disciplinare privacy e internet,* in *http://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2010/04/sentenza-google-pizzetti.shtml* ("*Presidente, che cosa non la convince in questa sentenza? – Il giudice basa la sentenza sull'articolo 13 del Codice, il quale però contiene obblighi diversi da quelli che, secondo la sentenza, Google avrebbe violato. L'articolo dice che il titolare del servizio (Google, in questo caso) ha il dovere di informare sul trattamento dei dati dell'interessato (ossia dell'utente che invia il video). Deve dire cioè come usare i dati del proprio utente*"). Analogamente V. ZAMBARDINO, *Il Garante Privacy sulla sentenza di Milano: "È sbagliata, ma ora bisogna fare regole non censorie"*, in *http://zambardino.blogautore.repubblica.it/2010/04/16/il-garante-privacy-sulla-sentenza-di-milano-e-sbagliata-ma-ora-bisogna-fare-regole-non-censorie/.*

[133] L'ipotesi in questione fa riferimento a dati sensibili in relazione ai quali si rimanda alle lucide considerazioni in G. COMMANDÈ-S. SICA, *op. cit.*, p. 92: "*la differenza tra il consenso 'documentato per iscritto' e quello 'scritto' non è una sfumatura lessicale. Essa rimanda al differente peso degli interessi in gioco: nell'un caso si tratta di dati a tutela ordinaria, nell'altro, rafforzata. Nella seconda ipotesi il consenso è requisito legale procedimentale, in assenza del quale il trattamento – e non solo il consenso – è invalido ed al contempo illecito*".

[134] E. BASSOLI, *Art. 13*, in *Codice in materia di protezione dei dati personali, commento articolo 'per articolo' al testo sulla privacy. D.Lgs. 30 giugno 2003, n. 196*, Milano, 2004, pp. 106, 344; P. CECCOLI, *Art. 13, Informativa*, in *Codice della Privacy, Commento al decreto legislativo 30 giugno 2003, n. 196*, I, Milano, 2004, p. 181.

rarsi un trattamento illecito ai sensi dell'art. 23, comma 3°, che impone l'obbligo di informazione quale condizione ai fini di validità del trattamento" [135].

Se dunque l'intera normativa in materia di protezione dei dati personali, come già ampiamente illustrato, è quello volto alla "*difesa dell'individuo nei confronti del potere informatico*", si comprende il valore fondamentale di tali disposizioni al fine di un'effettiva tutela, soprattutto a fronte di dati sensibili.

E allora, se da un lato si sosteneva l'impossibilità di essere ritenuti "*titolari del trattamento*" in quanto "*le modalità e le finalità del trattamento*" erano state determinate esclusivamente dall'*uploader*, dall'altro si osservava come è proprio la nozione stessa di "*titolare del trattamento*" *ex* art. 4, comma 1, lett. f), Codice Privacy ad essere incentrata sulle finalità del trattamento (ed in questo presuppone che i titolari possano essere anche più di uno, a seconda delle rispettive finalità [136]).

E quindi anche sotto tale profilo occorreva controbattere che Google Video assumesse la natura di mero servizio di *hosting* (passivo): solo così si sarebbe giustificata l'insussistenza di una (propria) finalità di trattamento del dato, immesso dall'utente destinatario del servizio unicamente per la diffusione a terzi.

Ma la ricostruzione dei fatti, come abbiamo più volte affermato, offriva una realtà diversa: se tale dato risultava immesso dall'utente in Google Video per la sua diffusione, esso veniva contestualmente sfruttato a livello commerciale dal gestore della piattaforma informatica per il tramite del sistema *Adwords*. E dunque, non essendo il servizio di Google Video "agnostico" (per usare l'efficace espressione della Suprema Corte di Cassazione) o "neutro" (per usare invece quella della Corte Europea di Giustizia) rispetto al dato che di volta in volta inserito, è evidente che in relazione alla sua materiale operatività si connotano operazioni di trattamento la cui titolarità non può essere "accollata" *sic et simpliciter* al solo *uploader*.

In ultima istanza – a fronte di un'attività di trattamento difficilmente confutabile [137] nei fatti ed in diritto, data l'ampia nozione di cui all'art. 4, comma 1, lett. a), Codice Privacy [138] – veniva altresì contrapposta la circostanza che il contenuto immesso dall'*uploader* sarebbe stato comunque da lui stesso "autorizzato" nel momento in cui lo stesso accetta "*le condizioni di servizio – Termini del contratto*" al momento della registrazione al servizio.

A fronte di tale ultimo rilievo, la posizione della Procura di Milano è stata quella di indicare al Tribunale che le pattuizioni contrattuali del servizio Google Video (di tenore discutibile, atteso non solo il contenuto a tratti incomprensibile delle stesse ma anche le modalità con le quali vengono sottoposte all'accettazione dell'utente [139]) non potessero derogare norme di legge imperative.

---

[135] F. GRELBO, *Commento all'art. 13*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, I, Padova, 2007, p. 321.

[136] Ed infatti la stessa fattispecie di cui all'art. 167, d.lgs. n. 196 del 2003 è costruita con la previsione di una duplice tipologia di dolo specifico, caratterizzato dal fine di danno (teorizzabile in capo all'*uploader*) o di profitto (teorizzabile in capo a soggetti diversi, ove gli stessi realizzino operazioni di trattamento).

[137] Cfr. *retro*, par. 4.1.

[138] Si riporta il testo della norma per facilità di lettura: "*Art. 4. Definizioni – 1. Ai fini del presente codice si intende per: a) 'trattamento', qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*".

[139] "*Un cenno ... merita l'aspetto delle clausole di esonero da responsabilità presenti in molti contratti d'accesso a Internet; nella modulistica più diffusa nel settore, infatti, vengono spesse incluse clausole che limitano o escludono la responsabilità dei providers per alcune ipotesi. Nella materia trova applicazione, senza ra-*

Concludendo con il rilevare come, con tre semplici passaggi logici ma in un sillogismo viziato nei suoi presupposti, si potesse abilmente vanificare (a favore del proprio *business*) il senso di disposizioni di legge precise.

Ed infatti gli artt. 13, 23, commi 3 e 4, 26, d.lgs. n. 196 del 2003, espressioni della stessa *ratio* della legge in materia di trattamento dei dati personali, non paiono possano essere tacitati a bella posa – proprio per la prevalenza del bene interesse tutelato (diritti fondamentali della persona) e conformemente con la previsione dell'art. 1, comma 2, lett. b), d.lgs. n. 70 del 2003 – da disposizioni emanate per "*contribuire al buon funzionamento del mercato garantendo la libera circolazione dei servizi della società dell'informazione*" [140].

Anche perché, come è stato già rilevato in precedenza, il trattamento dei dati personali è definito dallo stesso d.lgs. n. 196 del 2003 come attività pericolosa (con il testuale rinvio al criterio civilistico di responsabilità *ex* art. 2050 c.c., con la correlata inversione dell'onere probatorio) che impone, anche a livello penalistico attesa la previsione di cui all'art. 17 Codice Privacy, la predisposizione di "*misure ed accorgimenti a garanzia dell'interessato*".

Orbene, sebbene il servizio Google Video *ipso facto* presentasse "*rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare*", tali "*misure ed accorgimenti*" (come richiamati dall'art. 17 Codice Privacy per i dati non sensibili, ma *a fortiori* necessari per quelli sensibili e comunque desumibili dalla complessiva normativa in materia) non furono previsti, seppure fosse già evidente – dall'analisi di mercato – come i filmati immessi in Google Video avrebbero sicuramente avuto ad oggetto "dati sensibili" (idonei a rivelare lo stato di salute, come quelli relativi al minore inquadrato) o comunque "personali".

6. L'evoluzione dei servizi offerti dagli *Internet Service Providers* americani: le radici del problema

È già stato accennato come la posizione complessivamente sostenuta dall'Accusa nel caso Google Video abbia radici lontane: ed infatti proprio l'esperienza delle indagini svolte dal *pool* reati informatici della Procura di Milano dal 2004 [141] ha fornito un contributo – sia pur

gioni di deroga, l'ordinaria disciplina invocabile in argomento; sicché, se il rapporto è tra provider e consumatore, l'efficacia di tali clausole andrà verificata" ai sensi della disciplina sulle clausole c.d. abusive: così S. SICA, in G. COMMANDÈ-S. SICA, *op. cit.,* p. 224. Così anche A. MAIETTA, *Il sistema delle responsabilità nelle comunicazioni via internet*, in G. CASSANO-I.P. CIMINO (a cura di), *Diritto dell'internet*, cit., p. 515.

[140] Così l'art. 1, comma 1, dir. 2000/31/CE.

[141] All'interno della grandi Procure, l'idea di un *pool* di magistrati dediti alla criminalità informatica era sicuramente da consigliare fin da prima della Legge 48/2008. Nell'esperienza milanese (con il *pool* costituitosi di fatto nell'ottobre del 2004 con l'affiancamento del sottoscritto all'allora unico Pubblico Ministero che si occupava sistematicamente della materia, Gianluca Braghò), devo altresì rimarcare la professionalità delle Forze dell'ordine in materia di accertamenti informatici (Polizia Postale di Milano nonché due diverse realtà della Guardia di Finanza di Milano che, al loro interno, si sono "*cyberspecializzate*" quasi per passione: intendo qui riferirmi al vecchio Gruppo Repressione Frodi e al Gruppo Pronto Impiego) e contestualmente esserne grato. Nonché dare atto, dal momento che i reati informatici sono in costante aumento, che dal maggio 2007 la Procura della Repubblica presso il Tribunale di Milano – grazie al personale interessamento del Procuratore Manlio Minale e l'appoggio del Procuratore Aggiunto Alberto Nobili – si è altresì dotata di un'apposita "Squadra di PG reati informatici" (attualmente costituita da 6 persone, provenienti da tutte le forze di polizia presenti sul territorio – Polizia di Stato, Carabinieri, Guardia di Finanza, Polizia locale – di supporto al *pool* reati informatici ma anche ad accertamenti informatici in indagini in carico ad altri colleghi, ove riservatezza o complessità degli stessi lo rendano opportuno). Sul punto cfr. M. CARDUCCI, *Il pool reati informatici nella Procura di Milano: i*

minimo – alle riflessioni in materia svoltesi negli ultimi anni presso gli organismi comunitari (Eurojust e Consiglio d'Europa *in primis*) [142].

Il punto di partenza, come già più diffusamente sostenuto [143], è dato dal fatto le tre più importanti società che forniscono i servizi di comunicazione elettronica (Google, Microsoft e Yahoo!) e che hanno i *server* negli USA, "in teoria" sarebbero anche disposte a una collaborazione più celere con le Autorità Giudiziarie europee salvo poi attestare che ciò non sarebbe possibile per la "loro" legge.

6.1. "*No server no law opinion*" vs "*No server but law opinion*"

In questo come in altri casi similari, ci troviamo sempre più spesso di fronte a due impostazioni contrapposte.

Da un lato quella che privilegia il luogo di allocazione dei *server* interessati, spesso al di fuori degli Stati Membri dell'Unione Europea. Questa opinione dogmatica arriva a sostenere che, non essendoci *server* sul territorio nazionale o comunque europeo, non potrebbero trovare applicazione le rispettive leggi nazionali (e comunitarie).

Di contro registriamo l'impostazione volta a ribadire – in linea con la giurisprudenza non solo comunitaria ma anche, come vedremo, americana – che ciò che conta è il luogo dove il servizio Web viene offerto, anche ai fini dell'applicazione della relativa legge.

6.2. L'intercettazione di caselle di posta elettronica *@.com*

Tramite i più diffusi sistemi di posta elettronica offerti dalle richiamate società americane, viene generato un flusso di comunicazioni tra persone che, spesso, sono entrambe presenti nel nostro Stato.

È in questo ambito che si verifica, sempre più spesso, quanto già prima indicato in relazione alla teoria da noi definita come quella del "*no server no law*".

È noto agli addetti ai lavori come, per le società di telecomunicazione nazionali, sia possibile richiedere – in esecuzione del provvedimento del Giudice che dispone l'intercettazione telematica – che la posta elettronica indirizzata alla *e-mail* intercettata venga reindirizzata ad un *account* appositamente creato dalla Polizia Giudiziaria: questo consente non solo un risparmio dei costi delle complessive operazioni di intercettazione ma anche soprattutto la pos-

rapporti con la Polizia Giudiziaria e la Magistratura estera, *Atti del Convegno OLAF "Nuove prospettive dell'attività investigativa nella lotta antifrode in Europa"*, Milano, 24-25 gennaio 2008, Bruxelles, 2008.

[142] Il primo "*Strategic meeting on Cybercrime*" è stato organizzato da Eurojust e si è tenuto ad Atene il 23-24 ottobre 2008: cfr. *http://www.eurojust.europa.eu/press_releases/2008/30-10-2008.htm*; La "*2009 Octopus Interface Conference – Cooperation against Cybercrime*", organizzata dal Consiglio d'Europa, si è tenuta a Strasburgo il 10-11 marzo 2009: cfr. *http://www.coe.int/cybercrime.*

Tra questi due importanti appuntamenti, si è tenuto nel novembre 2008 l'altrettanto significativo incontro tra magistrati europei dediti alla lotta al *cybercrime* organizzato a Durbuy dal Consiglio Superiore della Giustizia del Belgio dal titolo: "*Investigation, Prosecution and Judgment of Information Technology Crime: legal framework and criminal policy in the European Union*".

[143] F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono …,* in *Ciberspazio e Diritto*, vol. 11, n. 1, 2010, pp. 185-210. Si consenta altresì il rinvio a F. CAJANI, *Interception of communications: Skype, Google, Yahoo! and Microsoft tools and electronic data retention on foreign servers: A legal perspective from a prosecutor conducting an investigation,* in *Digital Evidence and Electronic Signature Law Review*, vol. 6, 2009, pp. 158-180.

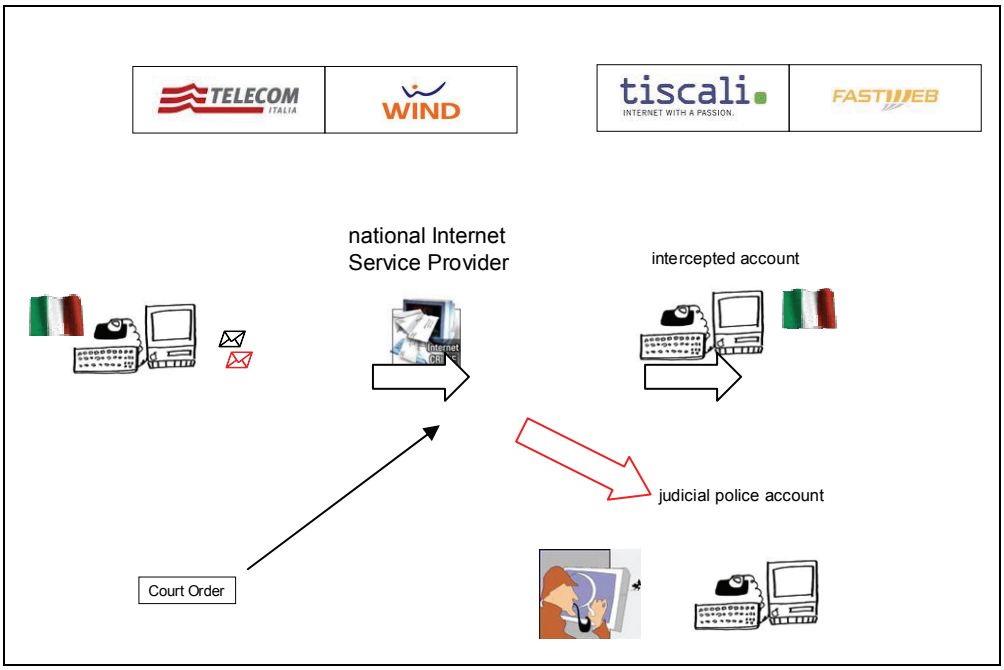
sibilità di iniziarle in tempi ragionevolmente brevi [144] (questione non di poco momento laddove si addirittura in pericolo una vita umana) [145].

[144] Diversamente, occorrerebbe dapprima richiedere i tabulati telefonici del numero utilizzato per la connessione ad Internet (per verificare quale sia il gestore che la fornisce) e successivamente pianificare, d'intesa con il gestore, l'azione di collocamento delle c.d. sonde (tecnicamente necessarie per intercettare il traffico utile): nel complesso tali operazioni ragionevolmente possono anche durare un'intera settimana!

[145] Ormai è tristemente risaputo che, durante il sequestro dell'imprenditore Roveraro, proprio l'utilizzo di Skype aveva inizialmente comportato un non indifferente ostacolo per gli investigatori del Raggruppamento Operativo Speciale (ROS) Carabinieri – Sezione Anticrime di Milano guidati dai Pubblici Ministeri milanesi Alberto Nobili e Mario Venditti. Così l'efficace ricostruzione di L. GRIMALDI, *Due giorni di misteri, poi l'esecuzione*, in *Corriere della Sera*, 6 aprile 2008: "*Pure la storia dell'omicidio di Gianmario Roveraro, dopo la confessione dell'assassino, sembra estremamente lineare, tanto che in apparenza la sua cronaca può scorrere veloce e consequenziale: davanti al magistrato, Filippo Botteri sostiene di aver rapito Roveraro perché, ritenendolo responsabile della perdita di una grossa somma di denaro, intendeva chiedergli di essere risarcito. E allora, sbarcato a Milano da Parma, l'ha aspettato all'uscita della metropolitana insieme a un complice. Voleva coglierlo di sorpresa, pensando che così quello non reagisse. Ma Roveraro, alto e aitante com'era malgrado i settant'anni, si è messo a menare colpi con la ventiquattrore, e ce n'è voluto, prima di riuscire a immobilizzarlo e a caricarlo sulla macchina e poi a legargli i polsi e mettergli una mascherina sugli occhi. 'Dopo, solo noi due, signor giudice. Io e il dottor Roveraro ...' lo chiamava ancora così. 'Lui sul sedile di dietro, io alla guida. Abbiamo girato per la campagna attorno a Fornovo per ore e ore'. Intanto Roveraro telefona alla moglie per dirle di non preoccuparsi, che lui è in Austria e tornerà presto. Manda anche un fax alla sua segretaria per ordinarle di 'movimentare' un milione di euro e tenerlo a disposizione. Entrambi i messaggi vengono resi irrintracciabili da Emilio Toscani, quel mago del computer che è uno dei complici del rapitore. Due giorni di vita zingara, con Roveraro sempre immobilizzato e con la mascherina sugli occhi*".

A rileggere gli atti di indagine che hanno portato alla condanna degli imputati (in particolare l'annotazione riepilogativa dei ROS sui profili tecnici emersi, datata 1 febbraio 2007 e a firma del Ten. Col. Mario Mettifogo) e nonostante l'impossibilità di sottoporre ad immediata intercettazione tali comunicazioni Skype (42 in totale, dalle ore 1.25 del 6 luglio 2006 alle ore 17.53 del 7 luglio 2006), tuttavia gli investigatori furono in grado di ricostruire *ex post* un complesso "*sistema di comunicazioni ... finalizzato a garantire anonimato e riservatezza*", con l'utilizzo di "*strumenti telefonici classici, impiegati con opportuni accorgimenti (intestatari fittizi e rose di contatti chiuse) e strumenti telematici di ultima generazione come servizi di VoIP e di Electronic Fax, nonché mezzi informatici di occultamento di indirizzi IP e di account di posta elettronica. Tale sistema, a dimostrazione della premeditazione del reato, è stato ideato, concretizzato e testato ben prima di porre in essere la condotta criminale, al fine di garantirne il perfetto funzionamento allorquando si fosse reso necessario*".

In particolare, l'utilizzo di un sistema di Electronic Fax (denominato *Efax Plus Service*) comportò necessariamente il pagamento del relativo traffico tramite addebito su due carte di credito prepagate, non ricaricabili, emesse dall'Istituto IMI San Paolo senza identificazione degli intestatari. Acquisito il riepilogo delle operazioni su tali carte, emerse che una delle due era stata "*utilizzata anche per effettuare una ricarica al servizio Skype da 11.50 euro in data 5 giugno 2006*", ovvero un mese prima del rapimento (avvenuto nei giorni del 6 e 7 luglio 2006). Alla luce di questi primi riscontri, gli investigatori riuscirono – con forti pressioni, data la gravità della vicenda, sui responsabili italiani di eBay Inc., società anch'essa con filiale a Milano nonché, all'epoca dei fatti, controllante Skype – a verificare "*se l'utenza domestica della famiglia Roveraro ... fosse mai stata contattata da account Skype*" (dal momento che dai primi esiti dei tabulati telefonici non risultava alcuna traccia delle telefonate indicate dalla moglie nella denuncia di scomparsa), con esito positivo dal momento che furono forniti due diversi *account* ("rov1987" e "bitorzolo77") e il relativo traffico complessivamente generato. "*I dati di registrazione dei due account Skype*" apparvero subito "*facilmente riconducibili a quelli dell'account dell'Efax Plus Service, in quanto 'rov1987' e(ra) stato registrato con casella di posta elettronica d'appoggio marlon87 @SoftHome.net*" simile all'indirizzo *marlon87@email.it* utilizzato invece per il servizio di E-Fax. Così "*giunti a conoscenza del mezzo telefonico mediante il quale di Dr. Roveraro ha comunicato per l'ultima volta con la propria famiglia in data 7 luglio 2006, si è tentato di risalire alle utenze fisiche utilizzatrici dei singoli indirizzi IP relativi alle connessioni Skype*": se tale attività ha permesso agli investigatori di evidenziare "*l'utilizzo di proxy-server che garantiscono l'occultamento dell'identità del punto di connessione*", in alcuni casi sono stati individuati contatti effettuati tramite due diverse utenze cellulare (Vodafone e TIM), entrambe intestate a tale Svitlana Didenko. L'individuazione di tali utenze mobili "*è stata immediatamente seguita da accertamenti tesi all'acquisizione del relativo traffico telefonico, all'intercettazione ed alla richiesta a tutti i gestori di telefonia nazionale dell'esistenza nei rispettivi database di ulteriori utenze intestate al nominativo o al codice fiscale di Didenko*



Tuttavia, con riferimento a caselle di posta elettronica *@.com*, questo meccanismo diventa spesso impossibile ... infatti quando la Polizia Giudiziaria va a notificare a Google o a Microsoft (entrambe aventi, quali filiali, una società di diritto italiano con sede in Milano) il decreto del Giudice che autorizza l'intercettazione, quale è la tipica risposta che viene loro fornita?

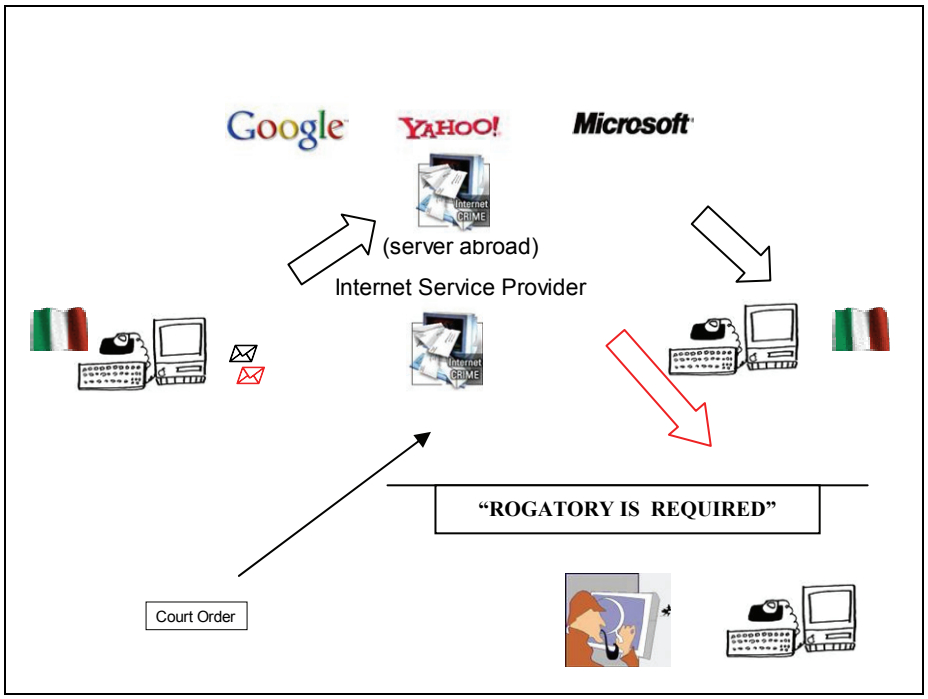
"*Spiacenti, i nostri server stanno in America ... quindi chiedete l'intercettazione con una rogatoria!*".

Svitlana", con individuazione di una terza utenza (TIM) ad essa intestata. L'analisi del traffico storico di tale ultima utenza ha evidenziato "*un utilizzo anomalo, avendo generato contatti unicamente con altre due utenze TIM con numeri sequenziali immediatamente precedenti*" a questa. Tutte queste tre utenze TIM erano state attivate presso lo stesso esercizio commerciale in Modena, un anno prima del rapimento.

Nonostante questa accurata ricostruzione tecnica (grazie anche all'ausilio del Reparto Tecnico dei ROS) circa i sistemi di comunicazione complessivamente utilizzati, un diverso elemento mise gli investigatori sulla pista giusta: infatti la moglie riferì subito che Roveraro "*da almeno 5 o 6 anni non si recava più all'estero per lavoro ... L'unica cosa che la portava a collegare all'Austria le attività di suo marito era un investimento da lui effettuato, su consiglio e tramite il dott. Botteri Filippo di Parma, su una società austriaca ... Investimento che è risultato in totale perdita*".

Tali complessivi elementi, insieme ad altri, consentirono di richiedere al GIP l'emissione di un'ordinanza di misura cautelare, eseguita all'alba del 21 luglio 2006 con l'arresto dei tre indagati e culminata, "*nella stessa giornata, con il rinvenimento nel comune di Fornovo di Taro (PR) dei poveri resti della vittima del sequestro*".

Sul recente annuncio di Sean O'Neil, esperto di *reverse engineering*, di essere in possesso del codice in grado di decifrare le comunicazioni che viaggiano su Skpe cfr. A. MARUCCIA, *Skype, una crepa nel VoIP cifrato?,* in *http://punto-informatico.it/2938992/PI/News/skype-una-crepa-nel-voip-cifrato.aspx;* G. ZICCARDI, *Rotto il codice di cifratura delle comunicazioni via Skype. Intercettiamo? E cade un grande tema della computer forensics?*, in *http://zik.typepad.com/resistenza/2010/07/rotto-il-codice-di-cifratura-delle-comunicazioni-via-skype-intercettiamo-e-cade-un-grande-tema-della-computer-forensics.html*.



Solo Yahoo (anch'essa avente, quale filiale, una società di diritto italiano, sempre sede a Milano) dispone di un *software* – denominato '*Yahoo! Account Management Tool*' – che consente l'intercettazione delle caselle di posta elettronica in tal modo, ma con alcuni limiti (e con alcuni problemi, come verificatosi in una nota indagine milanese [146]).

Più precisamente, sulla base del principio della *Net Citinzenship* (Cittadinanza di Rete), l'utente può scegliere – al momento della registrazione di una *e-mail @yahoo* – a quale legislazione sottoporre la sua casella di posta elettronica.

Solamente ove abbia scelto quella italiana, il richiamato *software* ne consente l'intercettazione immediata ove necessaria ai fini investigativi ed autorizzata con provvedimento dell'Autorità Giudiziaria.

6.2.1. Le richieste relative alla c.d. "posta in giacenza"

Nonostante nei moderni ordinamenti processual-penalistici sembrerebbe essere patrimonio comune la distinzione netta tra intercettazione di comunicazioni e richiesta al gestore della

[146] Il caso è nato da una casella *@yahoo.it* sottoposta ad intercettazione – con le modalità consentite dal '*Yahoo! Account Management Tool'*– senza alcun risultato (ovvero la Polizia Giudiziaria non riceveva nulla sul proprio *account* predisposto *ad hoc*). Dopo aver arrestato l'indagato (un *phisher* della Romania), lo stesso durante un interrogatorio e alla presenza del difensore ci fornì le credenziali di accesso alla sua casella (ovvero a quella che era stata intercettata senza successo). Scoprimmo allora con sorpresa, tramite accesso c.d. *webmail*, che invece vi erano molti messaggi ancora giacenti, ricevuti nel periodo nel quale la casella era stata sottoposta ad intercettazione. Le successive indagini della Guardia di Finanza – Gruppo Pronto Impiego di Milano hanno consentito di accertare che al richiamato *Tool* potevano accedere davvero in tanti all'interno delle varie filiali europee di Yahoo!, con pregiudizio alla riservatezza degli utenti (e non solo alle indagini di Polizia Giudiziaria).

Gli atti sono stati trasmettessi al Garante per la protezione dei dati personali, che ha confermato gli accertamenti tecnici e l'impostazione giuridica della Procura di Milano: cfr. *infra*, nota 156.

c.d. posta in giacenza[147], la posizione di Microsoft è quella di equiparare le due situazioni, negando di fatto anche richieste di acquisizione di posta giacente ove non sorrette da una richiesta di assistenza giudiziaria.

La procedura richiesta all'Autorità Giudiziaria è dunque la medesima:

> "*Procedura per l'intercettazione/duplicazione delle caselle di posta elettronica ai sensi dei vigenti trattati internazioni tra Italia e Stati Uniti.*
>
> Affinché una richiesta di intercettazione proveniente da una *law enforcement agency* straniera (nel caso specifico, l'Autorità Giudiziaria italiana) sia accolta, è necessario che la stessa venga presentata attraverso una rogatoria internazionale o attraverso le modalità stabilite dai Trattati internazionali in materia di assistenza giudiziaria reciproca in ambito penale (*Mutual Legal Assistance In Criminal Matters Treaties – MLATs*). Una volta che la procedura è stata avviata, il Dipartimento di Giustizia degli Stati Uniti d'America dovrà richiedere alla Corte competente per il caso specifico di emettere un ordine nei confronti del soggetto che fornisce il servizio di posta elettronica (nel caso specifico Microsoft Corporation) al fine di monitorare i contenuti delle comunicazioni effettuate da un determinato utente a beneficio della *law enforcement agency* straniera richiedente.
>
> Per legge, il Dipartimento di Giustizia può ottenere un ordine di intercettazione solo se le indagini sono connesse ad un reato per il quale l'*Electronic Communications Privacy Act* (*E-CPA*) autorizza specificamente l'intercettazione".

Se anche Google si conforma agli stessi principi, per Yahoo! invece valgono i medesimi presupposti già analizzati al precedente paragrafo (e dunque in alcuni casi il richiamato '*Yahoo! Account Management Tool*' consentirà di ottenere copia della posta in giacenza, ove necessaria ai fini investigativi ed autorizzata con provvedimento del Pubblico Ministero).

6.3. La conservazione dei dati relativi al traffico telematico

Un discorso in parte diverso vale relativamente ai dati relativi al traffico telematico, i c.d. *log files*.

Qui, quanto all'esperienza italiana, Microsoft è stata la prima a fornire – senza rogatoria ma solo con una richiesta della Autorità giudiziaria[148] – tali dati non solo con riferimento a caselle *@hotmail.it* ma anche a caselle *@hotmail.com*.

Google, in un primo momento, ha ribadito la necessità di una rogatoria per qualsiasi ri-

[147] "*Se non vi è dubbio che la trasmissione di sms o di e-mail si sostanzia in una comunicazione telematica di flussi informatici, come tale soggetta alla disciplina delle intercettazioni telematiche, è possibile rilevare come tali operazioni dovrebbero riguardare solamente l'attività di captazione di comunicazioni contestuali: sicché non dovrebbe rientrare in tale categoria l'attività di acquisizione di dati informatici oggetto di comunicazioni non contestuali perché già avvenute*": E. APRILE, *La disciplina delle intercettazioni telefoniche e delle videoriprese di comportamenti comunicativi*, in *http://appinter.csm.it/incontri/relaz/17233.pdf*, 2009, p. 12.

[148] Come formalmente comunicato alla Procura di Milano nell'ambito di una indagine, sulla base di una "politica adottata da Microsoft Corporation" volta ad "*accettare richieste relative alle generalità degli intestatari di indirizzi Hotmail ed agli accessi dagli stessi effettuati (IP log file – no password di accesso) anche nel caso in cui tali richieste provengano da autorità giudiziarie diverse da quella statunitense, purché l'atto di richiesta sia classificabile come 'court order' per la legge dello Stato di Washington e sia indirizzato direttamente a Microsoft Corporation [...] In casi simili, in passato, sono state ritenute valide le richieste di informazioni provenienti dall'Ufficio del Pubblico Ministero nell'ambito di indagini di polizia giudiziaria*". Si noti come la stessa Microsoft s.r.l. cura la traduzione in inglese dell'atto emesso dalla Autorità giudiziaria italiana e il suo successivo invio a Microsoft Corporation.

chiesta in tal senso: tuttavia, proprio a partire dall'indagine milanese sul caso di Google Video, la società americana pare abbia cambiato decisamente *policy*, fornendo i dati richiesti a fronte del solo provvedimento della Autorità Giudiziaria Italiana ed anche per il tramite di Google Italy.

E tuttavia, con una *policy* di difficile comprensione circa il fondamento giuridico, vengono forniti i dati richiesti solamente laddove l'IP interessato rientri nel *range* assegnato a Paesi Membri UE (laddove, diversamente, viene indicato la sola localizzazione dell'IP richiesto e l'impossibilità di comunicare i relativi dati ad Autorità Giudiziarie diverse da quelle dello Stato interessato).

Con l'originale risultato verificatosi di recente in una indagine sul *phishing* relativa al fenomeno dei c.d. *financial manager*[149], laddove per il reclutamento di tali soggetti venivano utilizzate caselle di posta elettronica *@gmail.com*: interesse investigativo era, ovviamente, quello di verificare i dati relativi alla loro attivazione e utilizzo.

Sulla base della risposta ricevuta da Google Inc. per il tramite di Google Italy, è stato necessario – nell'ambito di una corposa richiesta di assistenza giudiziaria relativa ad un ingente flusso di denaro (provento dei reati di *phishing* a danno di correntisti italiani) trasferito dall'Italia in Russia tramite *Western Union* – sollecitare l'Autorità giudiziaria della Federazione russa a richiedere essa stessa tali dati a Google.

Con un evidente dispendio di tempo ed energie, dal momento che, in casi analoghi verificatisi a seguito di risposte di altri gestori (anche americani), la richiesta alla Autorità Giudiziaria della Federazione russa era stata invece limitata solamente al passo successivo, ovvero a quello di identificare compiutamente i soggetti che risultavano abbinati all'IP interessato (ed in relazione al quale il gestore aveva precedentemente fornito tutti i dati in suo possesso).

Yahoo! invece richiede ancora la rogatoria solo laddove la casella di posta elettronica non possa essere gestita per il tramite del richiamato *Tool*.

7. La giurisprudenza americana sulla legge applicabile al mondo Internet

Ma, anche a voler aderire all'impostazione del "*no server no law*", cosa potrebbe succedere di fronte ad una Corte Americana?

Più precisamente, potrebbe in ipotesi un ISP con *server* in Italia (laddove offra servizi a cittadini americani) argomentare alla stessa maniera? O ancora, rimanendo sempre all'interno degli Stati Uniti d'America, potrebbe così giustificarsi un ISP americano con *server* in uno Stato (es. California) chiamato in causa di fronte ad una Corte Federale di un altro Stato (es. Arizona)?

Ebbene, sono stati altrove[150] già indicati alcuni validi motivi per ritenere che la teoria del "*no server no law*", tanto invocata al di fuori dei confini americani, non reggerebbe in madrepatria.

Dal momento che non è un caso che tali società rivolgano servizi anche a cittadini europei, ed anzi in Europa abbiano costituito delle società di diritto europeo, la fattispecie da noi considerata rientra pienamente nei criteri interpretativi cristallizzati dalla giurisprudenza americana[151].

[149] Sul punto si consenta il rinvio a F. CAJANI-G. COSTABILE-G. MAZZARACO, *Phishing e furto d'identità digitale*, cit., p. 51 ss.

[150] Cfr. nota 143.

[151] Cfr. G.J.H. SMITH, *Internet law and regulation*, III ed., London, 2002, pp. 347-349; J. HORNLE, *The Jurisdictional Challenge of the Internet*, in L. EDWARDS-C. WAELDE, *Law and the Internet*, cit., p. 143 ss.

È infatti evidente come anche una mera attività di *marketing* sia essenziale per la diffusione di un servizio (quale, per quanto possa qui rilevare, quello di posta elettronica) e, quindi, fondamentale in un'ottica di realizzazione di profitti economici. In relazione ai servizi *e-mail* forniti da Google, Yahoo! e Microsoft emerge – in ultima analisi – un sistema complesso di società di diritto europeo la cui attività economica "sul territorio", assolutamente essenziale per la controllante americana al fine di massimizzarne i complessivi profitti economici, sfugge tuttavia – sotto il profilo rilevante in questa analisi – alla applicazione delle normative statali ed europee.

Ebbene, con il conforto della giurisprudenza americana e nel silenzio della Convenzione di Budapest sul *Cybercrime* [152], l'elaborazione dogmatica del *pool* reati informatici della Procura di Milano ha suggerito soluzioni che indicavano come doverosa l'applicazione di norme già esistenti in Italia, e per di più tutte di derivazione comunitaria.

Del resto, che rilevante sia – ai fini dell'applicabilità di una norma di legge al mondo Internet – non già il luogo ove i dati sono allocati ma quello ove i relativi servizi vengono offerti (con contestuale profitto economico) si può anche ricavare dalla stessa direttiva n. 31 del 2000 che, al considerando 19, così prevede:

> "(19) Il luogo di stabilimento del prestatore va determinato in base alla giurisprudenza della Corte di giustizia delle Comunità europee, secondo la quale la nozione di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata mediante l'insediamento in pianta stabile. Tale condizione è soddisfatta anche nel caso in cui una società sia costituita a tempo determinato. Il luogo di stabilimento, per le società che forniscono servizi tramite Internet, non è là dove si trova la tecnologia del supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica. Se uno stesso prestatore ha più luoghi di stabilimento, è importante determinare da quale luogo di stabilimento è prestato il servizio in questione. Nel caso in cui sia difficile determinare da quale dei vari luoghi di stabilimento un determinato servizio è prestato, tale luogo è quello in cui il prestatore ha il centro delle sue attività per quanto concerne tale servizio specifico".

8. La normativa in materia di conservazione dei dati (*data retention*)

È noto come il d.lgs. 30 maggio 2008, n. 109 abbia finalmente introdotto in Italia [153] la disciplina europea in materia di *data retention* prevista dalla direttiva n. 24 del 2006 (la quale, con il combinato disposto degli artt. 3 e 6, prevede per gli Stati Membri un obbligo di conservazione dei dati attinenti il traffico telematico per un periodo di tempo non inferiore a 6 mesi e tuttavia non superiore ai 2 anni).

E dunque, ai fini del nostro discorso e sulla base dell'impostazione dogmatica qui sostenuta, questo significherebbe che gli obblighi di conservazione normativamente previsti dalla richiamata legge varrebbero anche per Google, Yahoo! e Microsoft.

Peraltro, che qualunque normativa comunitaria possa trovare applicazione a coloro che rivolgono i loro servizi ai cittadini europei emerge chiaramente dalla già richiamata illustre opinione di Peter Schaar in relazione al trattamento dei dati personali operato da Google.

---

[152] Cfr. il testo su *http://conventions.coe.int/* (*Convention on Cybercrime – CETS No. 185*).

[153] Cfr. S. ATERNO-A. CISTERNA, *Il legislatore interviene ancora sul data retention, ma non è finita*, in *Dir. pen. e proc.*, 2009, 3, p. 279 ss.

Con buona pace della legge americana, che non prevede sul punto – a differenza della diversa ipotesi di intercettazione delle comunicazioni – prescrizioni specifiche.

Quanto al periodo di conservazione dei dati relativi alle caselle di posta elettronica fornite dalle tre richiamate società, la *ratio* dunque risiede unicamente in precise *policies* aziendali (e dunque in semplici valutazioni economiche).

Microsoft attualmente conserva tali dati per un periodo di 60 giorni.

Google, da quanto formalmente comunicato alla Procura di Milano, conserva per "circa 30 giorni le informazioni di *login*" in relazione agli *account @gmail.com.*

All'epoca della ricordata indagine sui sistemi informatici di Yahoo!, essa era in grado di fornire i dati degli ultimi 30/45 giorni [154].

Chiunque abbia una minima esperienza in tema di contrasto del *cybercrime* è consapevole di quanto brevi siano tali periodi di conservazione! E, quantomeno per Microsoft (visti anche i rapporti collaborativi con la Polizia delle Comunicazioni [155]), la scelta finora operata (e ribadita anche recentemente in una indagine della Procura di Milano) appare onestamente di difficile comprensione.

E tuttavia un importante precedente in materia si è verificato proprio in relazione all'indagine relativa ai sistemi informatici di Yahoo! Italia: e, infatti, all'esito dell'istruttoria del Garante per la protezione dei dati personali (che ha confermato gli accertamenti tecnici e l'impostazione giuridica della Procura di Milano, comminando la relativa prescrizione alla luce della contestazione mossa ai sensi dell'art. 169, d.lgs. n. 196 del 2003) [156] e contestualmente all'adempimento delle prescrizioni imposte, i legali della società in data 9 settembre 2008 avevano comunicato all'Autorità che Yahoo! Italia, "*anche ai sensi del recente Decreto Legislativo n. 109 del 30/05/2008, si è adoperata per approntare le misure tecniche necessarie a garantire il tracciamento e la conservazione dei dati del traffico telematico (c.d. files di log,*

[154] Il procedimento penale che aveva originato il richiamato invio degli atti all'Autorità Garante (trattandosi di violazione di misure minime di sicurezza in relazione ai sistemi informatici della società Yahoo! Italia, anch'essa con sede legale a Milano e avente i *server* negli USA presso la casa madre), era scaturito dall'impossibilità di fatto di concludere gli accertamenti di Polizia Giudiziaria alla luce di quanto denunciato dalla persona offesa in data 12.9.2005: in particolare si trattava di invio di immagini pornografiche alla ragazza del denunciante, tramite utilizzo abusivo – ad opera di soggetti terzi non identificati (attesa la risposta negativa di Yahoo! Italia s.r.l. ai Carabinieri di Bresso datata 10 febbraio 2006, considerato il periodo di conservazione dei file di log riguardante "*solamente gli ultimi 30 giorni dalla data dell'accertamento*") della casella di posta elettronica *@yahoo.it* in uso alla persona offesa. Successivamente il periodo di conservazione era stato aumentato a 45 giorni.

[155] "*Non faccio assolutamente fatica a riconoscere il livello di affidabilità dei sistemi Microsoft*", ci dice Antonio Apruzzese, il direttore della Polizia Postale e delle Comunicazioni, "*anche in ragione della pluriennale esperienza di lavoro congiunto a livello di attività e progetti. Si tratta di un'azienda che ci supporta in tantissime iniziative professionali legate ai settori della lotta alla pedopornografia e dei crimini connessi all'accesso abusivo ai sistemi informatici e alla propagazione dei virus, per i quali ci fornisce fondamentali strumenti di lavoro a livello di software specializzati estremamente complessi, testati appositamente sulle nostre esigenze e di grandissima utilità per i nostri riscontri operativi*": A. MILANESI, *Ecco perché io invece tifo per il concorrente*, in *Corriere della Sera* – Sette, 28 giugno 2010, p. 30.

[156] Il Dirigente del dipartimento attività ispettive e sanzioni presso l'Autorità Garante, all'esito della relativa istruttoria, così conclude: "*L'indagine della Procura di Milano [...] fa emergere alcuni elementi sulla liceità dei trattamenti che, seppur non compiutamente definibili nell'ambito della procedura di cui all'art. 169, comma 2, del Codice, appaiono, in ogni caso meritevoli di approfondimento da parte dell'Autorità. […] Nondimeno, un approfondimento appare opportuno al fine di chiarire anche l'eventuale ambito di applicazione di altre disposizioni del Codice (ad es. l'art. 132) alle quali fa riferimento l'indagine della Procura di Milano, ancorché non inerenti alla materia delle misure minime di sicurezza, alla luce del provvedimento sulla sicurezza dei dati di traffico telefonico e telematico adottato il 17 gennaio 2008*".

dati relativi agli accessi effettuati dagli utenti alle Proprietà Yahoo![157] *per un periodo pari a 12 mesi; allo stato risultano già disponibili i file di log decorrenti dalla data del 21 novembre 2007*". Precisando ulteriormente – con comunicazione alla Procura di Milano del 10 settembre 2008 – che "*le suddette misure tecniche sono state adottate anche per le altre società europee del Gruppo le quali, a seconda delle diverse discipline locali, ne hanno dato specifica attuazione*".

E non potrebbe essere diversamente, a mio[158] modesto modo di vedere: siamo in presenza di società che trattano dati personali[159] connessi alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (cfr. art. 3 dir. 2002/58/CE) e dunque, per tali motivi ed indipendentemente dall'allocazione dei relativi *server*, destinatarie degli obblighi precettivi della normativa (italiana e comunque comunitaria) in materia di *data retention*.

8.1. Le contraddizioni degli *Internet Service Providers* americani in tema di *data retention*: quando non si vuole conservare …

La recente iniziativa del Wp29 (Gruppo per la tutela dei dati personali – articolo 29)[160] di sollecitare per iscritto[161] i tre *Internet Service Providers* circa la necessità di una maggiore sensibilizzazione in tema di cancellazione degli IP degli utenti ha posto alla ribalta un ulteriore aspetto, significativo per il nostro discorso.

E infatti, se da un lato tali società assumono *policy* restrittive nella conservazione dei dati utili per l'Autorità Giudiziaria, dall'altro sono invece prodighe nel conservare i dati utili per il proprio *business*.

Le tre lettere del 26 maggio 2010 sono un'ottima sintesi della situazione verificatasi dopo il documento adottato dal richiamato organismo comunitario nell'aprile 2008[162]: ed infatti Google aveva pubblicamente annunciato che avrebbe "anonimizzato" gli IP degli utenti conservati sui propri *server* dopo 9 mesi[163]; allo stesso modo Microsoft aveva annunciato pubblicamente l'intenzione di ridurre il periodo di conservazione dei *cookies* e degli *IP address* a 6 mesi[164]; Yahoo! si disse intenzionata, dopo aver deciso di anonimizzare i dati raccolti dopo 13 mesi, a ridurre tale periodo a 90 giorni (salvo alcune eccezioni).

---

[157] Intendendo con tale definizione "*i servizi web-based offerti da Yahoo! per il cui utilizzo sia necessaria la preventiva registrazione degli utenti al sito istituzionale ... www.yahoo.it, tramite apposito modulo di iscrizione, ovvero la successiva identificazione mediante inserimento di username e password*".

[158] Sul punto cfr. anche la posizione del Prof. Emilio Tosi in *ItaliaOggi*, 24 novembre 2009, p. 8: *http://www.tosilex.com/img/ITALIA%20OGGI%2024_11_09.pdf.*

[159] Tale situazione di fatto è stata peraltro formalmente comunicata dalla Procura di Milano al Garante per la protezione dei dati personali, anche nell'ambito della consultazione pubblica avviata con la deliberazione del 19 settembre 2007.

[160] Cfr. nota 54.

[161] *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010-others_en.htm*.

[162] *Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP148, adopted 4 April 2008*: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.*

[163] Cfr. il *post* "*Another step to protect user privacy*" (8 settembre 2008) firmato da Peter Fleischer (Global Privacy Counsel), Jane Horvath (Senior Privacy Counsel) e Alma Whitten (Software Engineer), in *http://google-blog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html.*

[164] Cfr. il *Microsoft press statement 'Microsoft Supports Strong Industry Search Data Anonymisation Standards'* (8 dicembre 2008), in *http://www.microsoft.com/emea/presscentre/pressreleases/TrustworthyComputingPR_081208.mspx.*

Periodi temporali ritenuti tuttavia ancora eccesivi dal Wp29 … ma la differenza rispetto agli attuali periodi di conservazione dei dati ai soli fini di indagine appare, sotto questo profilo, davvero imbarazzante.

Ma come biasimarli: conservare per le esigenze della collettività non è certo economicamente conveniente ...

9. Gli obblighi di mutua assistenza con gli Stati Uniti derivanti dalla Convenzione sul *Cybercrime*

Diversamente dalla ipotesi relativa alla conservazione dei dati attinenti al traffico, Microsoft e Google hanno osservato come la legislazione americana imponga invece precisi divieti in punto di trasmissione del contenuto delle relative comunicazioni a soggetti terzi, in assenza di un provvedimento (di intercettazione) ad opera dalla competente Autorità Giudiziaria. La *ratio* di tale previsione è di agevole comprensione: si tratta di garantire i diritti degli utenti e di sottoporre le relative richieste al vaglio della Autorità Giudiziaria che abbia giurisdizione in relazione al territorio ove si svolgono i fatti (e ove, verosimilmente, abbiano cittadinanza le persone che di tali fatti sono i protagonisti). E dunque, tradizionalmente, alla Autorità Giudiziaria statunitense.

Ma il mondo rapidamente è cambiato e una situazione di fatto impensabile fino a 15 anni fa adesso è all'ordine del giorno: ovvero che persone non fisicamente presenti sul territorio di uno Stato possano utilizzare sistemi di comunicazione fisicamente localizzati in quello Stato. E, ancor di più, che tali persone non abbiamo neppure cittadinanza in quello Stato!

E proprio per questo si impone, nello specifico tema oggetto della nostra analisi, una riflessione in punto di giurisdizione: laddove il Giudice italiano attesti (come peraltro avviene anche oggi nelle motivazioni delle richieste di intercettazione formulate dai Pubblici Ministeri) che tali sistemi di comunicazione (fisicamente allocati negli Stati Uniti, quantomeno in relazione ai *server* interessati [165]) siano utilizzati da cittadini italiani o comunque da persone presenti sul territorio dello Stato italiano, quali ulteriori ostacoli normativi residuerebbero?

Non potrebbe invece lo Stato italiano ragionevolmente affermare in questi casi la propria giurisdizione in materia, essendo solo un *accidente* quello relativo alla diversa localizzazione del servizio di comunicazione utilizzato da propri cittadini o comunque da persone che operano peraltro sul territorio italiano? Io credo proprio di sì.

Da un punto di vista strettamente giuridico, è peraltro noto come la Suprema Corte di Cassazione abbia da lungo tempo chiarito come non costituiscano violazione delle norme sulle rogatorie internazionali le prassi operative – quali quelle del c.d. instradamento, aventi ad oggetto anche comunicazioni verso utenze estere o provenienti dall'estero – per il tramite delle quali tutta l'attività di intercettazione, ricezione e registrazione delle telefonate venga compiuta completamente sul territorio italiano, senza alcuna lesione delle prerogative degli Stati esteri [166].

Proprio una simile situazione [167] si verificherebbe ove si rendesse possibile l'immediato

[165] Tale dato di fatto comunque spesso non è del tutto vero: si pensi, per esempio, all'utilizzo sempre più esteso delle c.d. *Akamai Technologies*, che consentono di ottimizzare servizi di comunicazione elettronica per gli utenti attraverso l'utilizzo di server collocati anche sul territorio italiano (dai quali vengono prelevati, in particolare, le immagini che vanno a comporre le pagine web strumentali alla visualizzazione dei relativi contenuti).

[166] Cfr. Cass., sez. IV, 29 luglio 2004, n. 32924, Belforte, in *CED*, rv. 229103; Cass., sez. V, sent. 21 ottobre 1998, n. 4401, Assisi, in *CED*, rv. 211520.

[167] "*Da tale indicazione si può quindi dedurre un principio generale in base al quale ad incardinare la*

re-indirizzamento delle comunicazioni giacenti su una casella *@.com* su una casella di posta elettronica comunicata dalla Polizia Giudiziaria, a fronte di un flusso di comunicazioni *e-mail* intercorrenti tra due soggetti (ed almeno uno dei quali, ossia il destinatario, utilizzatore di una casella *@.com*) presenti sul territorio dello Stato e che verrebbero intercettate in Italia.

Peraltro non bisogna dimenticare come ogni soggetto italiano (o comunque situato sul territorio dello Stato) che utilizza un qualsiasi sistema di posta elettronica, allo stesso modo di qualsiasi altro servizio su Internet, "*di norma svolge tali attività transitando dal server di un provider il cui nodo di trasmissione (c.d. pop) si trova fisicamente nei pressi del luogo da cui chiede la connessione*" [168].

Del resto, proprio analizzando la risposta tipo di Microsoft sul punto emerge come essi stessi riconoscano rilevante il luogo ove il servizio viene offerto e utilizzato (e solo residuale, ma di fatto prevalente in mancanza di prova contraria, il luogo di ubicazione dei *server*):

> "I servizi di posta elettronica identificati dai domini msn e hotmail sono forniti da Microsoft Corporation, società di diritto statunitense, indipendentemente dall'eventuale indicazione .it, la quale si riferisce esclusivamente all'area geografica di appartenenza dell'utente al momento della propria registrazione [169]. Tale indicazione geografica può comunque essere sempre modificata dall'utente indipendentemente dal luogo in cui si registra. Pertanto, non è da considerarsi indicativa del fatto che il servizio venga fornito nel territorio italiano.
>
> Per effettuare un'intercettazione deve quindi essere preso in considerazione il luogo in cui i dati richiesti risiedono e conseguentemente il luogo in cui i server sono ubicati. Nel caso dei servizi offerti da Microsoft Corporation tali server risiedono negli Stati Uniti e l'eventuale intercettazione/duplicazione deve necessariamente essere rivolte a Microsoft Corporation, tramite rogatoria, come disposto dal Dipartimento di Giustizia degli Stati Uniti d'America ed in forza dei vigenti trattati di diritto internazionale in materia, come se si trattasse di acquisizione di documentazione residente all'estero".

Inoltre all'attento lettore non sfuggirà un ulteriore curioso aspetto della questione: evidentemente Yahoo! ritiene di potersi conformare ad un'altra soluzione operativa (nel momento che consente, sia pure in alcuni casi, l'intercettazione e la comunicazione di contenuti comunicativi materialmente allocati su *server* americani).

---

competenza territoriale italiana è sufficiente che almeno uno dei 'capi' della comunicazione sia fisicamente situato in Italia. È quindi intercettazione 'italiana' quella che ha per oggetto tutte le comunicazioni dirette ad una utenza presente sul territorio nazionale, così come quelle che, partendo da una simile utenza, sono dirette all'estero": C. PARODI, *Criminalità informatica ed indagini telematiche: profili tecnici, normativi ed investigativi*, in *http://appinter.csm.it/incontri/relaz/12010.pdf*, 2005, p. 54.

[168] F. TESTA, *Cybercrime, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, in *http://appinter.csm.it/incontri/relaz/11794.pdf*, 2005, p. 19.

[169] A seguito di alcuni accertamenti di Polizia Giudiziaria sui servizi *hotmail.it*, si era avuto modo di osservare la seguente situazione fattuale: "*Peraltro, proprio dall'analisi del contratto relativo al servizio di posta elettronica (cfr. annotazione di PG del 4.3.2009), emergono alcuni dati significativi. In primis, l'articolo 1 precisa come 'il contratto intercorre tra l'utente e la società identificata dall'articolo 29' ovvero, in relazione all'utente italiano, Microsoft Luxemburg S.a.r.l.. Inoltre è prevista una clausola derogatoria della giurisdizione italiana che si pone in netto contrasto non solo con la previsione di cui all'art. 4 Legge 31.5.1995 n. 218 (difettando la forma scritta nella conclusione di un simile contratto on line) ma anche con quella di cui all'originario art. 1469bis c.c. ed oggi art. 33 lett. u) D.Lvo 6.9.2005 n. 206 (Codice del consumo), trattandosi di clausola vessatoria.*

Anche a voler ritenere valide le ricordate pattuizioni, emerge dunque che non sia la società americana ma tale società di diritto europeo a fornire il relativo servizio, anche se in ogni caso l'utente digitando l'indirizzo internet www.hotmail.it (sito registrato da Microsoft s.r.l.) viene di fatto messo nella condizione di ottenere, dopo aver ricevuto tutte le dovute informazioni in lingua italiana, una casella di posta elettronica @hotmail.it".

Una posizione peraltro che pare invece essere in linea con i principi sanciti nella Convenzione sul *Cybercrime* del Consiglio d'Europa, aperta alla firma il 23 novembre 2001 a Budapest.

Ebbene, gli Stati Uniti già da tempo avevano ratificato tale Convenzione, che prevede – proprio nelle due materie oggetto di trattazione – questi due precisi obblighi di collaborazione "in tempo reale" (art. 33 in materia di raccolta dei dati del traffico; art. 34 in materia di intercettazione dei contenuti):

> "**Article 33 – Mutual assistance in the real-time collection of traffic data**
>
> The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
>
> Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.
>
> **Article 34 – Mutual assistance regarding the interception of content data**
>
> The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws".

E dunque, dal momento che anche l'Italia nel 2008 ha finalmente ratificato tale Convenzione, tali obblighi oggi acquistano una loro effettiva valenza giuridica bilaterale (*pacta sunt servanda*).

9.1. Intercettazioni ed indagini penali

"*Le intercettazioni sono uno strumento essenziale per le indagini*"*:* in tali termini si è recentemente espresso Lanny Breuer, sottosegretario al Dipartimento di Giustizia con delega alla criminalità organizzata internazionale, nel corso di un incontro con la stampa presso l'ambasciata degli Stati Uniti a Roma[170].

A fronte del sempre più ampio utilizzo di caselle di posta elettronica *@.com* da parte della criminalità organizzata (proprio per la consapevolezza delle difficoltà, per le forze dell'ordine nazionali, in punto di tracciamento/intercettazione), tali condivisibili affermazioni indicano la necessità della revisione del Trattato di mutua assistenza in materia penale tra il Governo della Repubblica Italiana e il Governo degli Stati Uniti d'America, sottoscritto a Roma il 9 settembre 1982.

Nelle more, è evidente che le Autorità Giudiziarie continueranno ad applicare le norme di legge nazionali e quelle di derivazione europea nei confronti di tali società americane[171].

[170] Cfr. *http://www.rainews24.it/it/news.php?newsid=141187* (21 maggio 2010).

[171] L'ultimo episodio è quello relativo alla condanna di 55.000 euro, oltre a 10.000 euro per ogni giorno successivo di inadempimento, inflitta dal Tribunale belga di Dendermonde a Yahoo! Inc. (che peraltro non ha neppure una filiale in Belgio) per non aver fornito informazioni sul titolare di una casella di posta elettronica. Cfr. in Internet: *http://www.techcrunch.com/2009/03/02/yahoo-fined-by-belgian-court-for-refusing-to-give-up-e-mail-account-info* (2 marzo 2009). La Corte di Appello di Ghent, con sentenza del 30 giugno 2010, aveva dato ragione alla società americana (cfr. F. VAN LEEUW, *Cybercrime vs. law enforcement: the urgent need for new ways in the International cooperation. Some pratical exemples*, in F. CAJANI-G. COSTABILE (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Forlì, 2011, p. 51) ma di recente la

10. Libertà e Responsabilità

La Rete è sicuramente una risorsa fondamentale per la società.

Ebbene, è la storia della nostra civiltà a dirci che qualsiasi risorsa fondamentale è stata fatta *naturalmente* oggetto di regolamentazione dagli uomini … dal fuoco all'acqua all'elettricità.

La tesi della anarchia di Internet, sia pure positivamente sostenuta sotto le diverse e più accattivanti espressioni di libertà, non è più sostenibile [172].

Scomodare, quale agognato rifugio nella Prateria, il pericolo di una censura è stato l'ultimo tentativo per sfuggire ad un'analisi della realtà aderente ai fatti, dalla quale emerge come per i più importanti *Internet Service Providers* – modificandosi nel tempo la natura dei servizi da loro offerti e divenendo sempre meno indifferenti ai contenuti (che, se pur generati dagli utenti, sono sempre da loro organizzati e sfruttati secondo modelli di *business* ormai noti [173]) che veicolano – necessariamente si pongono problemi nuovi [174] di responsabilità civili ed anche penali.

Un discorso dunque che si pone in termini generali, senza tanti *se* e *ma* di facciata [175], e

Suprema Corte belga – con provvedimento del 18 gennaio 2011 – ha accolto il ricorso del Procuratore Generale della Corte di Appello, restituendo gli atti alla Corte d'Appello di Bruxelles.

[172] "*Bisogna essere sinceri: non servivano certo le parole di un magistrato, di un giudice e di un gruppetto di avvocati indemoniati per capire che dietro i pasticci del caso Google si nascondono problemini mica da poco. Ovvero: che diavolo si vuole dire quando si parla di libertà nella rete? E soprattutto: che razza di stravagante teoria è quella di chi ci vuole convincere che essere liberi sul Web significa davvero avere la possibilità di fare tutto il cavolo che ci pare? A meno che non si voglia ammettere che la libertà della rete significa semplicemente avere la possibilità di utilizzare il Web come se fosse una cassetta delle lettere in cui l'unico vero vincolo per la pubblicazione di un post, di un video, di una foto è la semplice capienza della mail box, beh, dovrebbe essere chiaro che chi in queste ore sostiene che sul Web non sia un illecito pubblicare sempre e comunque tutto quanto quello di cui si dispone commette un grosso errore. Il filosofo inglese John Locke, lo ricorderete, ripeteva spesso che laddove non c'è legge non c'è libertà e in questo senso sostenere che Google sia giustificata a comportarsi come se fosse un postino – 'che non può essere ritenuto responsabile del contenuto delle lettere' – è un modo molto ingenuo per nascondere il problema centrale di questa storia*": C. CERASA, *Che cosa vogliamo dire quando parliamo di libertà del Web?* (26 febbraio 2010), in *http://www.ilfoglio.it/soloqui/4525*.

[173] Così efficacemente S. QUINTARELLI, *Iniziativa diplomatica di Google,* in *http://blog.quintarelli.it/blog/2010/06/iniziativa-diplomatica-di-google.html:* "*e forse la cosa piu' importante ... per google, facebook, ecc. gli utenti non sono il cliente, gli utenti sono il prodotto che viene venduto ai loro clienti*".

[174] "*È peraltro significativo che con riguardo a Internet si sia deciso di percorrere – a livello europeo, ma sulla spinta di precisi orientamenti statunitensi – una strada per certi versi differente rispetto a quella della stampa e della radiotelevisione. Lì l'editore sceglie e confeziona i prodotti informativi-comunicativi e li diffonde, rispondendo per il loro contenuto, perché senza il mezzo da esso controllato la diffusione non sarebbe avvenuta. Per attenuare la sua responsabilità l'editore invoca – ma, come si è detto, erroneamente – la libertà di manifestazione del pensiero, sostenendo di aver esercitato un diritto. Nel mondo di Internet, seguendo una suddivisione tipica del mondo delle telecomunicazioni, colui il qual si limita a veicolare un dato, una notizia, una manifestazione del pensiero, senza averlo scelto o predisposto, e senza aver individuato il destinatario del messaggio, è esente da responsabilità. Il che costituisce una deviazione dai principi di contribuzione materiale alla produzione dell'evento dannoso*": V. ZENO-ZENCOVICH, *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, Bologna, 2004, pp. 138-139.

[175] A solo titolo di esempio, si riportano queste due recenti dichiarazioni (significativamente concordanti non tanto nella data di rilascio quanto nel contenuto): "*Ma guardiamo anche di cosa stiamo parlando: la privacy. Va certamente protetta, ma cos'è? È un concetto in piena evoluzione. Per me che ho 44 anni è una cosa importante, per mio padre ancora di più; mia figlia, che di anni ne ha 20, se ne cura molto meno*" (C. D'ASARO BIONDO, *"Il nuovo vicepresidente del gruppo" Google*, in M. GAGGI, *Google, nuovo monopolista rapace? No, crescendo impariamo a cooperare*, *Corriere della Sera*, 23 giugno 2010, p. 29); "*Il tema della privacy rivestirà un'importanza sempre maggiore.* "*Certamente. Ma bisogna capire che le cose sono molto cambiate negli ultimi*

che oggi deve essere ulteriormente rivisitato alla luce di piattaforme (sempre meno attente alla *privacy* dei loro utenti) quali *Facebook*[176] o di sistemi di comunicazione sempre più utilizzati e potenzialmente non tracciabili[177] quali *Skype*[178] e *Twitter*.

L'impressione tuttavia è che, dietro la tesi della necessità di (auto)regolamentazione del Web, non si vogliano appositamente vedere le Leggi che già oggi ci sono, nascondendosi dietro una "virtualità del *cyberspazio*" che è solo di facciata.

E, in effetti, *policy* più attente alla tutela della *privacy*, la conservazione dei dati ai fini di giustizia ed un più veloce metodo per consentire l'intercettazione di caselle di posta elettronica *@.com* impongono dei costi, ma possiamo affermare che ragioni economiche possano prevalere sulla difesa dei diritti delle persone che sono danneggiate dai crimini (anche informatici)?

---

sei anni. E che il concetto di privacy che ho io non è lo stesso che ha mio padre ed è diverso anche da quello di un ragazzo di quattordici anni. Sei anni fa nessuno voleva che le proprie informazioni personali fossero sul web, oggi il numero delle persone che rende disponibile il proprio cellulare su Facebook è impressionante. Per i miei genitori la privacy era un valore, per i miei coetanei condividere è un valore." (*Mark Zuckerberg, "il fondatore di Facebook"*, in E. ASSANTE, *Per la mia generazione la privacy non è un valore* (23 giugno 2010), *http://www.repubblica.it/tecnologia/2010/06/23/news/intervista_a_zuckerberg-5098864/*). Tale ultima dichiarazione così è commentata da G. SCORZA (*Zuckerberg: la privacy c'est moi!*, in *http://www.guidoscorza.it/?p=1912*): "*Facebook è, per milioni di italiani, il 'nuovo focolare' e si ritrova, nel 2010, a svolgere un ruolo che, per taluni aspetti – nonostante Zuckerberg ai microfoni di Assante si sforzi, senza peraltro, troppa convinzione, di negarlo – è analogo a quello svolto per anni dalla TV. Questo significa che Facebook e la filosofia che traspare e trasparirà dalla più grande piattaforma di socialnetwork al mondo è irrimediabilmente destinata ad influenzare in maniera quasi osmotica le convinzioni di milioni di utenti, proprio come hanno fatto – ed in buona misura continuano a fare – i media tradizionali. È per questo che sentir dire al patron di Facebook che la privacy per le nuove generazioni vale di meno di quanto non valesse per le precedenti, mi spaventa almeno quanto mi hanno sin qui spaventato le affermazioni di certi divi del piccolo schermo che, nel passato e nel presente, si sono eretti e ancor si ergono a tenutari del Sapere ed a Maestri di vita e di pensiero*".

[176] Cfr. A. ZAMPIGLIONE, *Facebook sacrifica la privacy sull'altare della pubblicità*, in *La Repubblica*, 12 aprile 2010, *Affari e Finanza*, p. 1: *http://ricerca.repubblica.it/repubblica/archivio/repubblica/2010/04/12/facebook-sacrifica-la-privacy-sullaltare-della-pubblicita.html.*

[177] Cfr. C. PARODI, *VoIP, Skype e tecnologie di intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Dir. pen. e proc.*, 2008, 10, p. 1309 ss.; C. MAIOLI-R. CUGNASCO, *Profili normativi e tecnici delle intercettazioni: dai sistemi analogici al voice over IP*, Bologna, 2008.

[178] Cfr. sul tema D. MCCULLAGH, *Skype: We can't comply with police wiretap requests*, in *http://news.cnet.com* (9 giugno 2008). Per la situazione italiana si rimanda a M. MENSURATI-F. TONACCI, *Boss e intercettazioni, Skype sotto accusa*, in *Repubblica*, 15 febbraio 2009: "*Tutto comincia nel 2006 a Milano. Il pm antimafia Margherita Taddei si accorge che alcuni indagati hanno trovato un modo sicuro per parlare tra di loro. Via Skype. Il pm incarica due consulenti di risolvere il problema, questi chiamano Skype che fissa loro un bizzarro appuntamento: a Londra, in una saletta riservata dell'aeroporto. La società è estone con sede in Lussemburgo. Non c'è motivo di incontrarsi a Londra. Ma i due accettano. La riunione, però, si dimostra inutile: 'Non c'è niente da fare'. Il pm decide allora di rivolgersi ad Eurojust (unità di cooperazione giudiziaria europea). Viene fissato un secondo incontro, stavolta a Milano. Da una parte gli investigatori e la rappresentanza italiana di Eurojust, dall'altra due uomini Skype: Kurt Sauer (security manager) e Stephen Collins (legale). Gli italiani propongono una serie di soluzioni, sia legali sia tecniche. I delegati della società estone, però, non battono ciglio, ripetendo quella che di qui in avanti diventerà la 'Versione di Skype': 'Non possiamo per problemi tecnici e non possiamo per problemi giuridici. La normativa del Lussemburgo non ce lo permette'. La rappresentanza italiana di Eurojust non si rassegna. E organizza un terzo incontro. Stavolta all'Aja. Da una parte investigatori italiani (magistrati delle Dda di Milano e Napoli, guidati dal procuratore nazionale antimafia Pietro Grasso), francesi, tedeschi, inglesi e greci, dall'altra i rappresentanti di Skype. Chi era presente a quella riunione racconta di un clima strano. 'Gli investigatori continuavano a proporre soluzioni, quelli di Skype ascoltavano in silenzio'. Poi il colpo di scena. 'I lavori erano programmati fino alle 19, ma alle 15 quelli di Skype spariscono nel nulla. Qualcuno sostiene usciti dal retro'. Fine dell'incontro. Lo scontro si arroventa, con i magistrati che continuano a chiedere una mano per le loro indagini e Skype a opporre le solite 'questioni tecniche e giuridiche', qualche volta utilizzando anche insistenti incomprensioni linguistiche per fare ostruzione*".

Ragionando in termine di bilancio, possiamo ragionevolmente affermare che i costi di impresa non supportati dalle relative società di telecomunicazione si stanno trasformando in più alti costi sociali. E dove stanno i profitti? Nelle tasche delle organizzazioni criminali!

Massimo Mucchetti, dalle pagine del *Corriere della Sera* del 28 febbraio 2010 [179], così chiosava circa "*La libertà della Rete e quella di fare affari*":

> "[…] la dichiarazione dell'ambasciata Usa [180] stupisce per quanto appaia ricalcata sulla propaganda di Google, che identifica se stessa con la Rete e presenta il processo di Milano come una minaccia contro tutti i grandi siti. […] Quando venne fondata Google, nel 1998, la Rete esisteva già da decenni. La libertà di Google, dunque, non può essere scambiata con la libertà della Rete. Sono cose diverse. […]
>
> Meglio lasciar perdere le false sacralità sulla Rete e, rispettati i diritti individuali, discutere di quell'argomento profano che sono gli affari in modo laico e leggibile".

Tale affermazione costituisce un invito a chiamare le cose con il loro nome, anche nel dibattito accademico scaturito da quell'efficace parallelismo con le *scritte sui muri* evocate dal Tribunale di Milano nella sentenza del caso Google Video [181]: come ha fatto chi, sull'edificio a fianco della bellissima Cattedrale di San Michele a Pavia, ha recentemente scritto senza timore di vergogna che "*IL VANDALISMO VA RIVALUTATO!*".

[179] Cfr. *http://archiviostorico.corriere.it/2010/febbraio/28/liberta_della_Rete_quella_fare_co_9_ 100228050.shtml.*

[180] Il riferimento è alle dichiarazioni dell'ambasciatore americano a Roma, David Thorne: cfr. *http://blog.quintarelli.it/blog/2010/02/lambasciatore-usa-difende-google-parlando-senza-conoscere-i-contenuti.html.* Lo stesso Thorne, alcuni giorni dopo, sembra essere ritornato sui suoi passi precisando come quello sui modi e limiti dell'utilizzo di Google "*è un dibattito importante*" perché l'attuale "*è un momento in cui tutti stiamo imparando*" come affrontare i problemi giuridici che sorgono dalle nuove tecnologie: *http://www.wallstreetitalia.com articolo.asp?art_id=878339*.

[181] Cfr. p. 98: "*In parole semplici: non è la scritta sul muro che costituisce reato per il proprietario del muro, ma il suo sfruttamento commerciale può esserlo, in determinati casi ed in presenza di determinate circostanze*".

Ebbene, l'impostazione fin qui sostenuta è stata dichiarata fin dalle origini del *pool* reati informatici di Milano e credo che questo sia ulteriore motivo di serenità nell'adempimento della nostra funzione istituzionale volta alla tutela dei diritti della persona, ovunque essi vengano messi in pericolo e calpestati.

E a chi va invocando una libertà messa irrimediabilmente a tacere dall'azione di una Procura italiana, i Pubblici Ministeri nella loro requisitoria per il caso Google Video hanno già risposto con le famose parole di Victor E. Frankl:

> "Se sulla costa dell'Oceano Atlantico, in arrivo al porto di New York, i passeggeri incontrano la statua della Libertà, sarebbe meraviglioso poter edificare sulla costa opposta la statua della Responsabilità".

€ 12,00 (IVA inclusa)

ISBN/EAN
9 788834 818770